

X S T A C K

CLI Manual

Product Model: **xStack**[™] DGS-3600 Series

Layer 3 Gigabit Ethernet Managed Switch

Release 2.4



Table of Contents

INTRODUCTION	1
USING THE CONSOLE CLI.....	3
COMMAND SYNTAX	7
BASIC SWITCH COMMANDS.....	9
SWITCH PORT COMMANDS	22
PORT SECURITY COMMANDS.....	25
STACKING COMMANDS	28
NETWORK MANAGEMENT (SNMP) COMMANDS	32
SWITCH UTILITY COMMANDS (INCLUDING FILE SYSTEM COMMANDS)	55
NETWORK MONITORING COMMANDS	71
MULTIPLE SPANNING TREE PROTOCOL (MSTP) COMMANDS	86
FORWARDING DATABASE COMMANDS.....	98
BROADCAST STORM CONTROL COMMANDS	105
QOS COMMANDS	109
PORT MIRRORING COMMANDS	118
VLAN COMMANDS	121
PROTOCOL VLAN GROUP COMMANDS.....	132
LINK AGGREGATION COMMANDS.....	137
IP-MAC-PORT BINDING (IMPB)	142
IP COMMANDS (INCLUDING IP MULTINETTING).....	150
IPV6 NEIGHBOR DETECTION COMMANDS	156
IGMP COMMANDS (INCLUDING IGMP V3).....	162
IGMP SNOOPING COMMANDS.....	165
MLD SNOOPING COMMANDS.....	176
DHCP RELAY.....	184
DHCP SERVER COMMANDS	190
LIMITED IP MULTICAST ADDRESS.....	204
802.1X COMMANDS.....	210
ACCESS CONTROL LIST (ACL) COMMANDS.....	227
TIME RANGE COMMANDS.....	246
ACL FLOW METERING COMMANDS	248
SFLOW	252
TIME AND SNTP COMMANDS	262
POLICY ROUTE COMMANDS	268
SAFEGUARD ENGINE COMMANDS.....	271
TRAFFIC SEGMENTATION COMMANDS.....	274
ARP AND GRATUITOUS ARP COMMANDS	276

VRRP COMMANDS	284
ROUTING TABLE COMMANDS.....	291
ROUTE REDISTRIBUTION COMMANDS	296
DNS COMMANDS.....	301
RIP COMMANDS	305
DVMRP COMMANDS	308
PIM COMMANDS.....	313
IP MULTICASTING COMMANDS.....	328
MD5 COMMANDS.....	330
OSPF CONFIGURATION COMMANDS.....	332
ROUTE PREFERENCE COMMANDS.....	349
MAC NOTIFICATION COMMANDS	352
WEB-BASED ACCESS CONTROL (WAC) COMMANDS	356
ACCESS AUTHENTICATION CONTROL COMMANDS	363
SSH COMMANDS.....	383
SSL COMMANDS	390
JUMBO FRAME COMMANDS	395
LLDP COMMANDS.....	397
D-LINK SINGLE IP MANAGEMENT COMMANDS.....	413
COMMAND HISTORY LIST.....	423
TECHNICAL SPECIFICATIONS.....	426

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 Manual.

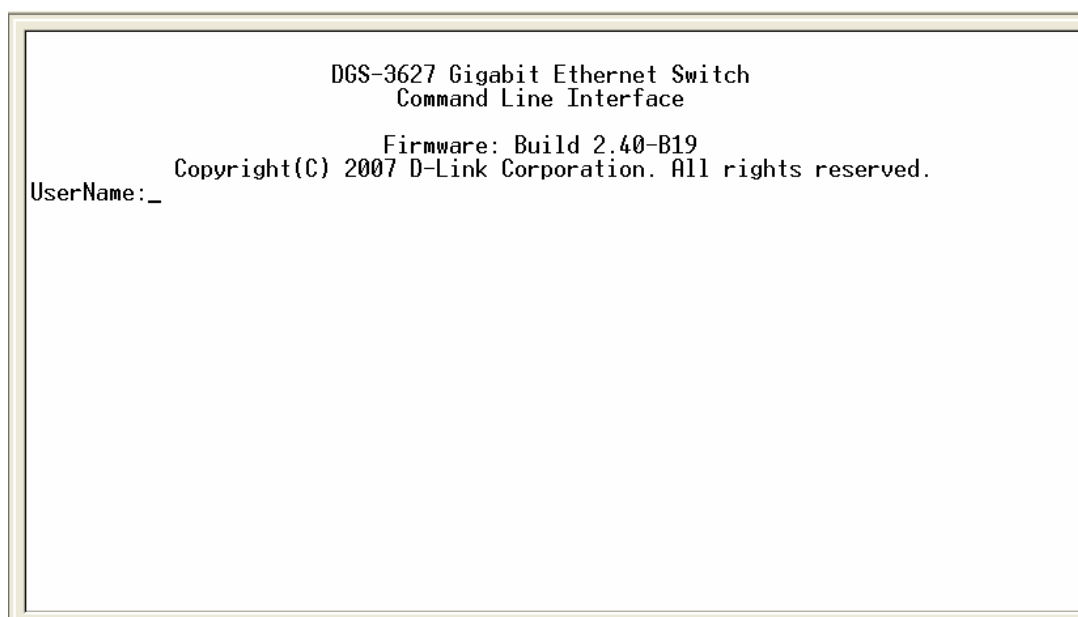
Accessing the Switch via the Serial Port

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-3627 Gigabit Ethernet Switch
Command Line Interface

Firmware: Build 2.40-B19
Copyright(C) 2007 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-3627:5#**. 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. You can change the default Switch IP address to meet the specification of your networking address scheme.

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

```
Boot Procedure 1.10-B09
-----
Power On Self Test ..... 100 %
MAC Address   : 00-19-5B-F1-CA-80
H/W Version   : 2A1G

Please wait, loading V2.40-B19 Runtime image ..... 100 %
UART init    ..... 100 %
Device Discovery ..... 100 %
Configuration init ..... 100 %
```

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, you can enter **config ipif System ipaddress xxx.xxx.xxx.xxx/z**. Where the **x**'s represent the IP address to be assigned to the IP interface named **System** and the **z** represents the corresponding number of subnets in CIDR notation.

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

```
DGS-3627:5#config ipif System ipaddress 10.24.22.200/255.0.0.0
Command: config ipif System ipaddress 10.24.22.200/8

Success.

DGS-3627:5#
```

Figure 1-3. Assigning an IP Address

In the above example, the Switch was assigned an IP address of 10.24.22.200 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.

USING THE CONSOLE CLI

The Switch 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 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 an IP address has been set for the 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 you have logged in, the console looks like this:

```
DGS-3627 Gigabit Ethernet Switch
Command Line Interface

Firmware: Build 2.40-B19
Copyright(C) 2007 D-Link Corporation. All rights reserved.
UserName:
Password:
DGS-3627:5#_
```

Figure 2- 1. Initial Console Screen after logging in

Commands are entered at the command prompt, **DGS-3627:5#**.

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.

```
?.
?  
cd  
clear  
clear arptable  
clear attack_log  
clear counters  
clear dhcp_binding  
clear fdb  
clear log  
clear port_security_entry port  
config 802.1p default_priority  
config 802.1p user_priority  
config 802.1x auth_mode  
config 802.1x auth_parameter ports  
config 802.1x auth_protocol  
config 802.1x capability ports  
config 802.1x guest_vlan ports  
config 802.1x init  
config 802.1x reauth  
config access_profile profile_id  
config account  
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 a **Next possible completions:** message.

```
DGS-3627:5#config account  
Command: config account  
Next possible completions:  
<username>  
  
DGS-3627:5#
```

Figure 2- 3. Example Command Parameter Help

In this case, the command **config account** was entered with the parameter **<username>**. The CLI will then prompt to enter the **<username>** with the message, **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, all of the next possible sub-commands can be seen, 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-3627:5#config account
Command: config account
Next possible completions:
<username>

DGS-3627:5#config account

```

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-3627:5#the
Available commands:
..                ?
config            copy                cd                clear
dir              disable             create            delete
erase            login              download          enable
ping6            reboot            logout            ping
reset            save              reconfig         rename
upload           traceroute
DGS-3627:5#_

```

Figure 2-5. Available Commands

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

For example, if you enter the **create** command with no additional parameters, the CLI will then display all of the possible next parameters.


```
DGS-3627:5#create
Command: create
Next possible completions:
802.1x          access_profile    account           address_binding
arpentry        authen            authen_enable    authen_login
cpu            dhcp              dot1v_protocol_group
double_vlan    fdb               igmp_snooping    ipif
iproute        ipv6              ipv6route        link_aggregation
md5            multicast_fdb     multicast_range   ospf
pim            policy_route     route            sflow
snmp           stp               syslog           trusted_host
vlan           vrrp              wac

DGS-3627:5#_
```

Figure 2- 6. Next possible completions: Create command

In the above example, all of the possible next parameters for the **create** command are displayed.

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	create ipif <ipif_name 12> <network_address> (<ip_addr/netmask>) <vlan_name 32> {secondary state [enable disable]}
Description	In the above syntax example, users must supply an IP interface name in the <ipif_name> space, a VLAN name in the <vlan_name 32> space, and the network address, including the netmask, in the <network_address> (<ip_addr/netmask>) space. Do not type the angle brackets.
Example Command	create ipif Engineering 10.24.22.5/255.0.0.0 Design

[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 the admin , operator , or user level account to be created. Do not type the square brackets.
Example Command	create account admin ctsnow

 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, you must specify the admin , operator , or user level account to be created. Do not type the backslash.
Example Command	create account admin ctsnow

{braces}

Purpose	Encloses an optional value or set of optional arguments.
Syntax	reset {[config system]}
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.
Example command	reset config

Line Editing Key Usage

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

BASIC SWITCH COMMANDS

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

Command	Parameters
create account	[admin operator user] <username 15>
config account	<username>
show account	
delete account	<username> {<string>}
show session	
show switch	
show serial_port	
config serial_port	{baud_rate [9600 19200 38400 115200] auto_logout [never 2_minutes 5_minutes 10_minutes 15_minutes]}
enable clipaging	
disable clipaging	
enable telnet	<tcp_port_number 1-65535>
disable telnet	
enable web	<tcp_port_number 1-65535>
disable web	
save	{[config {<drive_id> <pathname 64> log all]}
reboot	{<string>}
reset	{[config system]} {<string>}
login	
logout	
show device_status	
config command_prompt	
config greeting_message	{default}
show greeting_message	

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	The create account 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 eight user accounts can be created.
Parameters	<p><i>admin</i> <username 15> - Enter a name between 1 and 15 alphanumeric characters to define the administrator account created here.</p> <p><i>operator</i> <username 15>- Enter a name between 1 and 15 alphanumeric characters to define the operator account created here.</p> <p><i>user</i> <username 15>- Enter a name between 1 and 15 alphanumeric characters</p>

create account

to define the user account created here.

Restrictions Only Administrator-level users can issue this command.

Example usage:

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

```
DGS-3627:5#create account admin dlink
Command: create account admin dlink

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

Success.

DGS-3627:5#
```

To create an operator-level user account with the username “frazier”.

```
DGS-3627:5#create account operator frazier
Command: create account operator frazier

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

Success.

DGS-3627:5#
```

To create a user-level user account with the username “reed”.

```
DGS-3627:5#create account user reed
Command: create account user reed

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

Success.

DGS-3627:5#
```

config account

Purpose	Used to configure user accounts.
Syntax	config account <username>
Description	The config account command configures a user account that has been created using the create account command.
Parameters	<username>- Enter a name between 1 and 15 alphanumeric characters to define the administrator account to configure here.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the user password of “dlink” account:

```
DGS-3627:5#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-3627:5#
```

show account

Purpose	Used to display user accounts
Syntax	show account
Description	Displays all user accounts created on the Switch. Up to eight 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-3627:5#show account
Command: show account

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

DGS-3627:5#
```

delete account

Purpose	Used to delete an existing user account.
Syntax	delete account <username> {<string>}
Description	The delete account command deletes a user account that has been created using the create account command.
Parameters	<username> - <string> - Enter an alphanumeric string of up to 15 characters to define the username.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete the user account “System”:

```
DGS-3627:5#delete account System
Command: delete account System

Are you sure to delete the last administrator account?(y/n)y
Success.
```

DGS-3627:5#

show session

Purpose	Used to display a list of currently logged-in users.
Syntax	show session
Description	This command displays a list of all the users that are logged-in at the time the command is issued.
Parameters	None
Restrictions	None.

Example usage:

To display the way that the users logged in:

```
DGS-3627:5#show session
Command: show session

ID   Live Time   From           Level  Name
--   -
8    03:36:27   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 displays information about the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display the Switch's information:

```
DGS-3627:5#show switch
Command: show switch

Device Type       : DGS-3627 Gigabit Ethernet Switch
MAC Address       : 00-10-20-33-45-00
IP Address        : 10.24.22.200 (Manual)
VLAN Name         : default
Subnet Mask       : 255.0.0.0
Default Gateway   : 0.0.0.0
Boot PROM Version : Build 1.10-B06
Firmware Version  : Build 2.40-B19
Hardware Version  : 2A1G
System Name       :
System Location   :
System Contact    :
Spanning Tree     : Disabled
GVRP              : Disabled
```

```

IGMP Snooping      : Disabled
MLD Snooping       : Disabled
RIP                 : Disabled
DVMRP              : Disabled
PIM                : Disabled
OSPF               : Disabled
TELNET             : Enabled (TCP 23)
WEB                : Enabled (TCP 80)
RMON               : Disabled
SSL status         : Disabled
SSH status         : Disabled
802.1x             : Disabled
Jumbo Frame        : Off
Clipaging          : Disabled
MAC Notification   : Disabled
Port Mirror        : Disabled
SNTP               : Disabled
DHCP Relay         : Disabled
DNSR Status        : Disabled
VRRP               : Disabled
HOL Prevention State : Disabled
Syslog Global State : Disabled
Single IP Management: Disabled
    
```

DGS-3627:5#

show serial_port

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

Example usage:

To display the serial port setting:

```

DGS-3627:5#show serial_port
Command: show serial_port

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

DGS-3627:5#
    
```

config serial_port

Purpose	Used to configure the serial port.
Syntax	config serial_port {baud_rate [9600 19200 38400 115200] auto_logout [never 2_minutes 5_minutes 10_minutes 15_minutes]}
Description	This command is used to configure the serial port's baud rate and auto logout settings.

config serial_port

Parameters	<p><i>baud_rate</i> [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, and 115200.</p> <p><i>never</i> – No time limit on the length of time the console can be open with no user input.</p> <p><i>2_minutes</i> – The console will log out the current user if there is no user input for 2 minutes.</p> <p><i>5_minutes</i> – The console will log out the current user if there is no user input for 5 minutes.</p> <p><i>10_minutes</i> – The console will log out the current user if there is no user input for 10 minutes.</p> <p><i>15_minutes</i> – The console will log out the current user if there is no user input for 15 minutes.</p>
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To configure baud rate:

```
DGS-3627:5#config serial_port baud_rate 115200
Command: config serial_port baud_rate 115200

Success.

DGS-3627:5#
```

enable clipaging

Purpose	Used to pause the scrolling of the console screen when the show command displays more than one page.
Syntax	enable clipaging
Description	This command is used when issuing the show 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-level 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-3627:5#enable clipaging
Command: enable clipaging

Success.

DGS-3627:5#
```

disable clipaging

Purpose	Used to disable the pausing of the console screen scrolling at the
----------------	--

disable clipaging

	end of each page when the show 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 the show command would display more than one screen of information.
Parameters	None.
Restrictions	Only administrator-level 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-3627:5#disable clipaging
Command: disable clipaging

Success.

DGS-3627:5#
```

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-level and operator-level users can issue this command.

Example usage:

To enable Telnet and configure port number:

```
DGS-3627:5#enable telnet 23
Command: enable telnet 23

Success.

DGS-3627:5#
```

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.

disable telnet

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

Example usage:

To disable the Telnet protocol on the Switch:

```
DGS-3627:5#disable telnet
Command: disable telnet

Success.

DGS-3627:5#
```

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-level and operator-level users can issue this command.

Example usage:

To enable HTTP and configure port number:

```
DGS-3627:5#enable web 80
Command: enable web 80

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

DGS-3627:5#
```

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-level and operator-level users can issue this command.

Example usage:

To disable HTTP:

```
DGS-3627:5#disable web
Command: disable web
```

Success.

DGS-3627:5#

save

Purpose	Used to save changes in the Switch's configuration to non-volatile RAM.
Syntax	save {[config <drive_id> <pathname 64> log all]}
Description	This command is used to enter the current switch configuration or log file into non-volatile RAM. The saved switch configuration will be loaded into the Switch's memory each time the Switch is restarted.
Parameters	<p><i>config <drive_id></i> – Specify to save current settings to the Flash memory of the switch.</p> <p><i><drive_id></i> - Specify the ID of the drive where the log or configuration file will be placed.</p> <p><i><pathname 64></i> - Enter a name of up to 64 characters to define the file to be saved on the flash drive.</p> <p><i>log</i> – Specify to save current Switch log to NV-RAM.</p> <p><i>all</i> – Use to save the configuration and log file to NV-RAM.</p>
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

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

```
DGS-3627:5#save
Command: save

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

DGS-3627:5#
```

reboot

Purpose	Used to restart the Switch.
Syntax	reboot {<string>}
Description	This command is used to restart the Switch.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To restart the Switch:

```
DGS-3627:5#reboot
Command: reboot
Are you sure 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]} {<string>}
Description	This command is used to restore the Switch's configuration to the default settings assigned from the factory.
Parameters	<p><i>config</i> – 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.</p> <p><i>system</i> – 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.</p> <p>If no parameter is specified, the Switch's current IP address, user accounts, and the switch history log are not changed. All other parameters are restored to the factory default settings. The Switch will not save or reboot.</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

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

```
DGS-3627:5#reset config
Command: reset config

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

Success.

DGS-3627:5#
```

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-3627:5#login
Command: login

UserName:
```

logout

Purpose	Used to log out a user from the Switch's console.
Syntax	logout

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-3627:5#logout
```

show device_status

Purpose	Used to display the current status of the hardware of the Switch.
Syntax	show device_status
Description	This command displays the current status of the Switch's physical elements.
Parameters	None.
Restrictions	None.

Example usage:

To show the current hardware status of the Switch:

```
DGS-3627:5#show device_status
Command: show device_status

Internal Power   External power   Side Fan   Back Fan
-----
      Active           Fail           OK           ---
DGS-3627:5#
```

config command_prompt

Purpose	Used to configure the command prompt for the Command Line Interface.
Syntax	config command_prompt [<string 16> username default]
Description	This command is used to configure the command prompt for the CLI interface of the Switch. The current command prompt consists of "product name + : + user level + product name" (ex. DGS-3627:5#). The user may replace all parts of the command prompt, except the # by entering a string of 16 alphanumeric characters with no spaces, or the user may enter the current login username configured on the Switch.
Parameters	<p><i><string 16></i> - Enter an alphanumeric string of no more than 16 characters to define the command prompt for the CLI interface.</p> <p><i>username</i> - Entering this parameter will replace the current CLI command prompt with the login username configured on the Switch.</p> <p><i>default</i> - Entering this parameter will return the command prompt to its original factory default setting.</p>
Restrictions	<p>The reset command will not alter the configured command prompt, yet the reset system command will return the command prompt to its original factory default setting.</p> <p>Only administrator-level and operator-level users can issue this</p>

config command_prompt

command.

Example usage:

To configure the command prompt:

```
DGS-3627:5#config command_prompt Tiberius
Command: config command_prompt Tiberius

Success.

Tiberius#
```

config greeting_message

Purpose	Used to configure the greeting message or banner for the opening screen of the Command Line Interface.
Syntax	config greeting_message {default}
Description	This command is used to configure the greeting message or login banner for the opening screen of the CLI.
Parameters	<i>default</i> – Adding this parameter will return the greeting command to its original factory default configuration.
Restrictions	The reset command will not alter the configured greeting message, yet the reset system command will return the greeting message to its original factory default setting. The maximum character capacity for the greeting banner is 6 lines and 80 characters per line. Entering Ctrl+W will save the current configured banner to the DRAM only. To save it into the FLASH memory, the user must enter the save command. Only administrator-level and operator-level users can issue this command.

Example usage:

To configure the greeting message:

```
DGS-3627:5#config greeting_message
Command: config greeting_message
```

Greeting Messages Editor

```
=====
                        DGS-3627 Gigabit Ethernet Switch
                        Command Line Interface

                        Firmware: Build 2.40-B19
                        Copyright(C) 2008 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	Only administrator-level and operator-level users can issue this command.

Example usage:

To view the currently configured greeting message:

```
DGS-3627:5#show greeting_message
```

```
Command: show greeting_message
```

```
=====
```

```
DGS-3627 Gigabit Ethernet Switch
```

```
Command Line Interface
```

```
Firmware: Build 2.40-B19
```

```
Copyright(C) 2008 D-Link Corporation. All rights reserved.
```

```
=====
```

```
DGS-3627:5#
```


SWITCH PORT COMMANDS

The switch port commands in the Command Line Interface (CLI) are listed (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 32> clear_description]}
show ports	{<portlist>} { [description err_disabled] }

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

config ports

Purpose	Used to configure the Switch's Ethernet port settings.
Syntax	[<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]}
Description	This command allows for the configuration of the Switch's Ethernet ports. Only the ports listed in the <portlist> will be affected.
Parameters	<p><i>all</i> – Configure all ports on the Switch.</p> <p><i><portlist></i> – Specifies a port or range of ports to be configured. The beginning and end of the port list range are separated by a dash.</p> <p><i>medium_type [fiber copper]</i> – This applies only to the Combo ports. If configuring the Combo ports this defines the type of transport medium used.</p> <p><i>speed</i> – Allows the user to adjust the speed for a port or range of ports. The user has a choice of the following:</p> <ul style="list-style-type: none"> • <i>auto</i> – Enables auto-negotiation for the specified range of ports. • <i>[10 100 1000]</i> – 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. • <i>[half full]</i> – Configures the specified range of ports as either full-duplex or half-duplex. • <i>[master slave]</i> - The master setting (1000M/Full_M) will allow the port to advertise capabilities related to duplex, speed and physical layer type. The master setting will also determine the master and slave relationship between the two connected physical layers. This relationship is necessary for establishing the timing control between the two physical layers. The timing control is set on a master physical layer by a local source. The slave setting (1000M/Full_S) uses loop timing, where the timing comes from a data stream received from the master. If one connection is set for 1000M/Full_M, the other side of the connection must be set for 1000M/Full_S. Any other configuration will result in a link down status for both ports. <p><i>flow_control [enable disable]</i> – Enable or disable flow control for the specified ports.</p> <p><i>learning [enable disable]</i> – Enables or disables the MAC address learning on the specified range of ports.</p> <p><i>state [enable disable]</i> – Enables or disables the specified range of ports.</p> <p><i>description <desc 1-32></i> - Enter an alphanumeric string of no more than 32 characters to describe a selected port interface.</p> <p><i>clear_description</i> - Enter this command to clear the port description of the selected port(s).</p>

config ports

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

Example usage:

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

```
DGS-3627:5#config ports 1-3 speed 10_full learning enable state enable
Command: config ports 1-3 speed 10_full learning enable state enable

Success.

DGS-3627:5#
```

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. The beginning and end of the port list range are separated by a dash.
- {description} – Adding this parameter to the **show ports** command indicates that a previously entered port description will be included in the display.
- err_disabled – Choosing this parameter will display ports that have been disconnected due to an error on the port, such as a Loopback Detection.

Restrictions None.

Example usage:

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

```
DGS-3627:5#show ports
Command: show ports
```

Port	Port State	Settings Speed/Duplex/FlowCtrl	Connection Speed/Duplex/FlowCtrl	Address Learning
1	Enabled	Auto/Enabled	Link Down	Enabled
2	Enabled	Auto/Enabled	Link Down	Enabled
3	Enabled	Auto/Enabled	Link Down	Enabled
4	Enabled	Auto/Enabled	Link Down	Enabled
5	Enabled	Auto/Enabled	Link Down	Enabled
6	Enabled	Auto/Enabled	Link Down	Enabled
7	Enabled	Auto/Enabled	Link Down	Enabled
8	Enabled	Auto/Enabled	Link Down	Enabled
9	Enabled	Auto/Enabled	Link Down	Enabled
10	Enabled	Auto/Enabled	Link Down	Enabled
11	Enabled	Auto/Enabled	100M/Full/None	Enabled
12	Enabled	Auto/Enabled	Link Down	Enabled
13	Enabled	Auto/Enabled	Link Down	Enabled
14	Enabled	Auto/Enabled	Link Down	Enabled
15	Enabled	Auto/Enabled	Link Down	Enabled
16	Enabled	Auto/Enabled	Link Down	Enabled
17	Enabled	Auto/Enabled	Link Down	Enabled
18	Enabled	Auto/Enabled	Link Down	Enabled
19	Enabled	Auto/Enabled	Link Down	Enabled

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

Example usage:

To display the configuration of all ports on the Switch, with description:

```
DGS-3627:5#show ports description
Command: show ports description
```

Port	Port State	Settings Speed/Duplex/FlowCtrl	Connection Speed/Duplex/FlowCtrl	Address Learning
1	Enabled	Auto/Disabled Description: dads1	Link Down	Enabled
2	Enabled	Auto/Disabled Description:	Link Down	Enabled
3	Enabled	Auto/Disabled Description:	Link Down	Enabled
4	Enabled	Auto/Disabled Description:	Link Down	Enabled
5	Enabled	Auto/Disabled Description:	Link Down	Enabled
6	Enabled	Auto/Disabled Description:	Link Down	Enabled
7	Enabled	Auto/Disabled Description:	Link Down	Enabled
8	Enabled	Auto/Disabled Description:	Link Down	Enabled

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

To display the Error Disabled ports:

```
DGS-3627:5#show ports err_disabled
Command : show ports err_disabled
```

Port	Port State	Connection status	Reason
2	Enabled Desc: Port 2	Err-disabled	Storm control
8	Enabled Desc: Port 8	Err-disabled	Storm control

```
DGS-3627:5#
```

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 0-16> lock_address_mode [Permanent DeleteOnTimeout DeleteOnReset]}
delete port_security_entry vlan_name	<vlan_name 32> port <port> mac_address <macaddr>
clear port_security_entry port	<portlist>
show port_security	{ports <portlist>}

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 0-16> lock_address_mode [Permanent DeleteOnTimeout DeleteOnReset]}
Description	This command allows for the configuration of the port security feature. Only the ports listed in the <i><portlist></i> are affected.
Parameters	<p><i>portlist</i> – Specifies a port or range of ports to be configured. The beginning and end of the port list range are separated by a dash.</p> <p><i>all</i> – Configure port security for all ports on the Switch.</p> <p><i>admin_state [enable disable]</i> – Enable or disable port security for the listed ports.</p> <p><i>max_learning_addr <max_lock_no 0-16></i> - Use this to limit the number of MAC addresses dynamically listed in the FDB for the ports.</p> <p><i>lock_address_mode [Permanent DeleteOnTimeout DeleteOnReset]</i> – Indicates the method of locking addresses. The user has three choices:</p> <ul style="list-style-type: none"> ▪ <i>Permanent</i> – The locked addresses will not age out after the aging timer expires. ▪ <i>DeleteOnTimeout</i> – The locked addresses will age out after the aging timer expires. ▪ <i>DeleteOnReset</i> – The locked addresses will not age out until the Switch has been reset.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To configure the port security:

```
DGS-3627:5#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-3627:5#
```

delete port_security_entry vlan_name

Purpose	Used to delete a port security entry by MAC address, port number and VLAN ID.
Syntax	delete port_security_entry vlan_name <vlan_name 32> port <port> mac_address <macaddr>
Description	This command is used to delete a single, previously learned port security entry by port, VLAN name, and MAC address.
Parameters	<p><i>vlan name <vlan_name 32></i> - Enter the corresponding vlan name of the port to delete.</p> <p><i>mac_address <macaddr></i> - Enter the corresponding MAC address, previously learned by the port, which the user wishes to delete.</p> <p><i>port <port></i> - Enter the port number which has learned the previously entered MAC address.</p>
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To delete a port security entry:

```
DGS-3627:5#delete port_security_entry vlan_name default port 6
mac_address 00-01-30-10-2C-C7
Command: delete port_security_entry vlan_name default port 6
mac_address 00-01-30-10-2C-C7

Success.

DGS-3627:5#
```

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 port <portlist>
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	<i><portlist></i> – Specifies a port or port range to clear. The beginning and end of the port list range are separated by a dash.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To clear a port security entry by port:

```
DGS-3627:5# clear port_security_entry port 6
Command: clear port_security_entry port 6

Success.

DGS-3627:5#
```

show port_security

Purpose	Used to display the current port security configuration.
Syntax	show port_security {ports <portlist>}
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. The beginning and end of the port list range are separated by a dash.
Restrictions	None.

Example usage:

To display the port security configuration:

```
DGS-3627:5#show port_security ports 1-5
Command: show port_security ports 1-5

Port Admin State Max. Learning Addr. Lock Address Mode
-----
1 Disabled 1 DeleteOnReset
2 Disabled 1 DeleteOnReset
3 Disabled 1 DeleteOnReset
4 Disabled 1 DeleteOnReset
5 Disabled 1 DeleteOnReset

DGS-3627:5#
```

STACKING COMMANDS

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

Command	Parameters
config box_priority	current_box_id <value 1-12> priority <value 1-63>
config box_id	current_box_id <value 1-12> new_box_id [auto 1 2 3 4 5 6 7 8 9 10 11 12]
show stack_information	
config stacking mode	[disable enable] {<string>}
show stacking mode	

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

config box_priority

Purpose	Used to configure box priority, which determines which box becomes the priority master. Lower numbers denote a higher priority.
Syntax	config box_priority {current_box_id <value 1-12> priority <value 1-63>}
Description	This command configures box (switch) priority.
Parameters	<i>current_box_id</i> <value 1-12> – Identifies the Switch being configured. Range is 1-12. <i>priority</i> <value 1-63> – Assigns a priority value to the box, with lower numbers having higher priority. The possible priority range is 1-63. This field is important when the stacking mode is automatically configured. Users who wish a certain switch become the primary master of the switch stack should configure their choice for the priority master switch to have the highest priority (and in essence the lowest number).
Restrictions	Only administrator-level and operator-level users can issue this command.

Usage example:

To configure box priority:

```
DGS-3627:5#config box_priority current_box_id 1 priority 1
Command: config box_priority current_box_id 1 priority 1

Success.

DGS-3627:5#
```

config box_id

Purpose	Used to configure box ID. Users can use this command to reassign box IDs.
Syntax	config box_id {current_box_id <value 1-12> new_box_id [auto 1 2 3 4 5 6 7 8 9 10 11 12]}
Description	This command will assign box IDs to switches in a stack.
Parameters	<i>current_box_id</i> – Identifies the Switch being configured. Range is 1-12. <i>new_box_id</i> – The new ID being assigned to the Switch (box). Range is 1-12.

config box_id

- *auto* – Allows the box ID to be assigned automatically.

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

Usage example:

To change a box ID:

```
DGS-3627:5#config box_id current_box_id 1 new_box_id 2
Command: config box_id current_box_id 1 new_box_id 2

Success.

DGS-3627:5#
```

show stack_information

Purpose	Used to display the stack information table.
Syntax	show stack_information
Description	This command display stack information.
Parameters	None.
Restrictions	None.

Usage example:

To display stack information:

```
DGS-3627:5#show stack_information
Command: show stack_information

Topology      : Duplex ring
My Box ID     : 1
Master ID     : 1
BK Master ID  : 2
Box Count     : 3

Box  User          Type          Exist  Prio-  MAC          Prom  Runtime  H/W
ID   Set            Type          rity   rity   version     version version
---  ---            -            ----  ----  -
 1   AUTO          DGS-3627G    Exist  16    00-16-9A-BA-72-CB  1.00-B06  2.20-B35  1A1G
 2   AUTO          DGS-3650     Exist  16    00-17-9C-BA-12-CB  1.00-B06  2.20-B35  2A1G
 3   AUTO          DGS-3650     Exist  16    01-17-1A-CA-72-CB  1.00-B06  2.20-B35  2A1G
 4   -              Not Exist    no
 5   -              Not Exist    no
 6   -              Not Exist    no
 7   -              Not Exist    no
 8   -              Not Exist    no
 9   -              Not Exist    no
10   -              Not Exist    no
11   -              Not Exist    no
12   -              Not Exist    no
-----

DGS-3627:5#
```


config stacking mode

Purpose	Used to configure the stacking mode.
Syntax	config stacking mode [disable enable] {<string>}
Description	This command will enable or disable the stacking mode for the switch. When enabled, the 10G ports on the rear of the switch will be enabled for stacking.
Parameters	<i>enable disable</i> – Use these parameters to enable or disable the stacking mode for the switch. Once this command is executed, it will cause the switch to reboot. This mode cannot be changed when the switch is currently stacked with other switches. <i>string</i> – This string is used to set the confirmation question that will follow the entry of this command. Entering a “/y” will command the switch to prompt the user to answer a confirmation question regarding the reboot of the switch. Entering “/n” will disable the question and the switch will automatically restart once the command has been entered.
Restrictions	Only administrator-level users can issue this command.



NOTE: Only ports 26 and 27 of the DGS-3627 support stacking. Port 25 cannot be used for stacking, and is to be used only as a 10-Gigabit uplink port.

Usage example:

To disable the stacking mode:

```
DGS-3627:5#config stacking mode disable
Command: config stacking mode disable

Change Box bootmode may cause devices work restart, still continue? (y/n)y
```

show stacking mode

Purpose	Used to view the current stacking mode.
Syntax	show stacking mode
Description	This command will display whether the current stacking mode is enabled or disabled.
Parameters	None.
Restrictions	Only administrator-level and operator-level users can issue this command.

Usage example:

To view the current stacking mode:

```
DGS-3627:5#show stacking mode
```

```
Command: show stacking mode
```

```
Stacking mode : Enabled
```

```
DGS-3627:5#
```

NETWORK MANAGEMENT (SNMP) COMMANDS

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

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

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

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

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

Command	Parameters
enable snmp	
disable snmp	
enable snmp linkchange_traps	
disable snmp linkchange_traps	
config snmp linkchange_traps ports	[all <portlist>][enable disable]
show snmp engineID	
create snmp group	<groupname 32> {v1 v2c v3 [noauth_nopriv auth_nopriv auth_priv]} {read_view <view_name 32> write_view <view_name 32> notify_view <view_name 32>}
delete snmp group	<groupname 32>
show snmp groups	
create snmp host	<ipaddr> {v1 v2c v3 [noauth_nopriv auth_nopriv auth_priv]} <auth_string 32>
delete snmp host	<ipaddr>
show snmp host	<ipaddr>
show snmp v6host	{<ipv6addr>}
create trusted_host	[<ipaddr> network <network_address>]
delete trusted_host	[<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 rmon	
disable rmon	

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

enable snmp	
Purpose	Used to enable SNMP on the Switch.
Syntax	enable snmp
Description	This command is used, in conjunction with the disable snmp command below, to enable and disable Simple Network Management Protocol (SNMP) on the Switch.
Parameters	None.
Restrictions	Only administrator-level and operator-level users can issue this

enable snmp

command.

Example Usage:

To enable SNMP:

```
DGS-3627:5#enable snmp
Command: enable snmp

Success.

DGS-3627:5#
```

disable snmp

Purpose	Used to disable SNMP on the Switch.
Syntax	disable snmp
Description	This command is used, in conjunction with the enable snmp command above, to enable and disable Simple Network Management Protocol (SNMP) on the Switch.
Parameters	None.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To disable SNMP:

```
DGS-3627:5#disable snmp
Command: disable snmp

Success.

DGS-3627:5#
```

enable snmp linkchange_traps

Purpose	Used to enable SNMP link change traps on the Switch.
Syntax	enable snmp linkchange_traps
Description	This command is used, in conjunction with the disable snmp linkchange_traps command below, to enable and disable SNMP linkchange traps on the Switch.
Parameters	None.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example Usage:

To enable SNMP linkchange traps:

```
DGS-3627:5#enable snmp linkchange_traps
Command: enable snmp linkchange_traps

Success.
```

```
DGS-3627:5#
```

disable snmp linkchange_traps

Purpose	Used to disable SNMP link change traps on the Switch.
Syntax	disable snmp linkchange_traps
Description	This command is used, in conjunction with the enable snmp linkchange_traps command above, to enable and disable SNMP linkchange traps on the Switch.
Parameters	None.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To disable SNMP linkchange traps:

```
DGS-3627:5#disable snmp linkchange_traps
Command: disable snmp linkchange_traps

Success.

DGS-3627:5#
```

config snmp linkchange_traps

Purpose	Used to configure SNMP link change traps on the Switch.
Syntax	config snmp linkchange_traps ports [all <portlist>][enable disable]
Description	This command is used to configure SNMP linkchange traps on the Switch.
Parameters	<i>all</i> – Configure all ports on the Switch. <i><portlist></i> - Specifies a port or range of ports to be configured. The beginning and end of the port list range are separated by a dash. Non-contiguous portlist entries are separated by a comma. (ex: 1-3,7-9). <i>enable disable</i> – Use these parameters to enable or disable SMMP linkchange traps for the switch.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example Usage:

To configure SNMP linkchange traps on every port:

```
DGS-3627:5#config snmp linkchange_traps ports all enable
Command: enable snmp linkchange_traps all enable

Success.

DGS-3627:5#
```

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	<p>The create snmp user command creates a new SNMP user and adds the user to an SNMP group that is also created by this command. SNMP ensures:</p> <p>Message integrity – Ensures that packets have not been tampered with during transit.</p> <p>Authentication – Determines if an SNMP message is from a valid source.</p> <p>Encryption – Scrambles the contents of messages to prevent it from being viewed by an unauthorized source.</p>
Parameters	<p><i><user_name 32></i> – An alphanumeric name of up to 32 characters that will identify the new SNMP user.</p> <p><i><groupname 32></i> – An alphanumeric name of up to 32 characters that will identify the SNMP group with which the new SNMP user will be associated.</p> <p><i>encrypted</i> – Allows the user to choose a type of authorization for authentication using SNMP. The user may choose:</p> <ul style="list-style-type: none"> • <i>by_password</i> – Requires the SNMP user to enter a password for authentication and privacy. The password is defined by specifying the <i>auth_password</i> below. This method is recommended. • <i>by_key</i> – Requires the SNMP user to enter an encryption key for authentication and privacy. The key is defined by specifying the key in hex form below. This method is not recommended. <p><i>auth</i> - The user may also choose the type of authentication algorithms used to authenticate the snmp user. The choices are:</p> <p><i>md5</i> – Specifies that the HMAC-MD5-96 authentication level will be used. <i>md5</i> may be utilized by entering one of the following:</p> <ul style="list-style-type: none"> • <i><auth password 8-16></i> - An alphanumeric sting of between 8 and 16 characters that will be used to authorize the agent to receive packets for the host. • <i><auth_key 32-32></i> - Enter an alphanumeric sting 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. <p><i>sha</i> – Specifies that the HMAC-SHA-96 authentication level will be used.</p> <ul style="list-style-type: none"> • <i><auth password 8-20></i> - An alphanumeric sting of between 8 and 20 characters that will be used to authorize the agent to receive packets for the host. • <i><auth_key 40-40></i> - Enter an alphanumeric sting 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. <p><i>priv</i> – Adding the <i>priv</i> (privacy) parameter will allow for encryption in addition to the authentication algorithm for higher security. The user may choose:</p> <ul style="list-style-type: none"> • <i>none</i> – Adding this parameter will add no encryption. • <i>des</i> – Adding this parameter will allow for a 56-bit encryption to be added using the DES-56 standard using: <ul style="list-style-type: none"> • <i><priv_password 8-16></i> - 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. • <i><priv_key 32-32></i> - 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.

create snmp user

Restrictions Only administrator-level users can issue this command.

Example usage:

To create an SNMP user on the Switch:

```
DGS-3627:5#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-3627:5#
```

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	The delete snmp user command removes 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-3627:5#delete snmp user dlink
Command: delete snmp user dlink

Success.

DGS-3627:5#
```

show snmp user

Purpose	Used to display information about each SNMP username in the SNMP group username table.
Syntax	Show snmp user
Description	The show snmp user command displays information about each SNMP username in the SNMP group username table.
Parameters	None.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To display the SNMP users currently configured on the Switch:

DGS-3627:5#show snmp user

Command: show snmp user

Username	Group Name	VerAuth-Priv
initial	initial	V3NoneNone

Total Entries: 1

DGS-3627:5#

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	The create snmp view command assigns views to community strings to limit which MIB objects an SNMP manager can access.
Parameters	<p><i><view_name 32></i> – An alphanumeric string of up to 32 characters that identifies the SNMP view that will be created.</p> <p><i><oid></i> – The object ID that identifies an object tree (MIB tree) that will be included or excluded from access by an SNMP manager.</p> <p><i>view type</i> – Sets the view type to be:</p> <ul style="list-style-type: none"> <i>included</i> – Include this object in the list of objects that an SNMP manager can access. <i>excluded</i> – 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-3627:5#create snmp view dlinkview 1.3.6 view_type included

Command: create snmp view dlinkview 1.3.6 view_type included

Success.

DGS-3627:5#

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	The delete snmp view command is used to remove an SNMP view previously created on the Switch.
Parameters	<p><i><view_name 32></i> – An alphanumeric string of up to 32 characters that identifies the SNMP view to be deleted.</p> <p><i>all</i> – Specifies that all of the SNMP views on the Switch will be deleted.</p> <p><i><oid></i> – The object ID that identifies an object tree (MIB tree) that will be deleted from the Switch.</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

To delete a previously configured SNMP view from the Switch:

```
DGS-3627:5#delete snmp view dlinkview all
Command: delete snmp view dlinkview all

Success.

DGS-3627:5#
```

show snmp view

Purpose	Used to display an SNMP view previously created on the Switch.
Syntax	Show snmp view {<view_name 32>}
Description	The show snmp view command displays an SNMP view previously created on the Switch.
Parameters	<i><view_name 32></i> – An alphanumeric string of up to 32 characters that identifies the SNMP view that will be displayed.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To display SNMP view configuration:

```
DGS-3627:5#show snmp view
Command: show snmp view

Vacm View Table Settings
View Name          Subtree          View Type
-----
ReadView           1                Included
WriteView          1                Included
NotifyView         1.3.6            Included
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: 11

DGS-3627:5#

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. <i>read_write</i> or <i>read_only</i> 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	The create snmp community command is used to create an SNMP community string and to assign access-limiting characteristics to this community string.
Parameters	<i><community_string 32></i> – 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. <i>view <view_name 32></i> – 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. <i>read_only</i> – Specifies that SNMP community members using the community string created with this command can only read the contents of the MIBs on the Switch. <i>read_write</i> – 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-3627:5#create snmp community dlink view ReadView read_write
Command: create snmp community dlink view ReadView read_write
Success.
DGS-3627:5#
```

delete snmp community

Purpose	Used to remove a specific SNMP community string from the Switch.
Syntax	delete snmp community <community_string 32>
Description	The delete snmp community 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-3627:5#delete snmp community dlink
Command: delete snmp community dlink

Success.

DGS-3627:5#
```

show snmp community

Purpose	Used to display SNMP community strings configured on the Switch.
Syntax	show snmp community <community_string 32>
Description	The show snmp community 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	Only administrator-level and operator-level users can issue this command.

Example usage:

To display the currently entered SNMP community strings:

```
DGS-3627:5#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-3627:5#
```

config snmp engineID

Purpose	Used to configure a name for the SNMP engine on the Switch.
Syntax	config snmp engineID <snmp_engineID>
Description	The config snmp engineID command configures a name for the SNMP engine on the Switch.
Parameters	<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-3627:5#config snmp engineID 0035636666
Command: config snmp engineID 0035636666

Success.

DGS-3627:5#
```

show snmp engineID

Purpose	Used to display the identification of the SNMP engine on the Switch.
Syntax	Show snmp engineID
Description	The show snmp engineID command displays the identification of the SNMP engine on the Switch.
Parameters	None.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

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

```
DGS-3627:5#show snmp engineID
Command: show snmp engineID

SNMP Engine ID : 0035636666

DGS-3627:5#
```

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>}
Description	The create snmp group command creates 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

create snmp group

the SNMP group with which the new SNMP user will be associated.

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 manager 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-3627:5#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-3627:5#
```

delete snmp group

Purpose	Used to remove an SNMP group from the Switch.
Syntax	delete snmp group <groupname 32>
Description	The delete snmp group 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 with which the new SNMP user will be associated.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To delete the SNMP group named “sg1”.

```
DGS-3627:5#delete snmp group sg1
Command: delete snmp group sg1

Success.

DGS-3627:5#
```

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	The show snmp groups command displays the group-names of SNMP groups currently configured on the Switch. The security model, level, and status of each group are also displayed.
Parameters	None.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To display the currently configured SNMP groups on the Switch:

```
DGS-3627:5#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       : 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

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

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

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

Total Entries: 6

DGS-3627:5#
```


create snmp host

Purpose	Used to create a recipient of SNMP traps generated by the Switch's SNMP agent.
Syntax	create snmp host <ipaddr> [v1 v2c v3 [noauth_nopriv auth_nopriv auth_priv] <auth_string 32>]
Description	The create snmp host command creates a recipient of SNMP traps generated by the Switch's SNMP agent.
Parameters	<p><ipaddr> – The IP address of the remote management station that will serve as the SNMP host for the Switch.</p> <p>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.</p> <p>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.</p> <p>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:</p> <ul style="list-style-type: none"> • 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. <p>noauth_nopriv – Specifies that there will be no authorization and no encryption of packets sent between the Switch and a remote SNMP manager.</p> <p>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.</p> <p>auth_priv – Specifies that authorization will be required, and that packets sent between the Switch and a remote SNMP manager will be encrypted.</p> <ul style="list-style-type: none"> • <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-3627:5#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-3627:5#
```

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	The delete snmp host command deletes a recipient of SNMP traps generated by the Switch's SNMP agent.

delete snmp host

Parameters	<i><ipaddr></i> – 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-3627:5#delete snmp host 10.48.74.100
Command: delete snmp host 10.48.74.100

Success.

DGS-3627:5#
```

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	The show snmp host command is used to display the IP addresses and configuration information of remote SNMP managers that are designated as recipients of SNMP traps that are generated by the Switch's SNMP agent.
Parameters	<i><ipaddr></i> – The IP address of a remote SNMP manager that will receive SNMP traps generated by the Switch's SNMP agent.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To display the currently configured SNMP hosts on the Switch:

```
DGS-3627:5#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-3627:5#
```

show snmp v6host

Purpose	Used to display the IPv6 recipient of SNMP traps generated by the Switch's SNMP agent.
Syntax	show snmp v6host {<ipv6addr>}
Description	The show snmp v6host command is used to display the IPv6 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	<i>v6host <ipv6addr></i> – The IPv6 address of a remote SNMP manager that will receive SNMP traps generated by the Switch's SNMP agent.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To display the currently configured IPv6 SNMP hosts on the Switch:

```
DGS-3627:5#show snmp host
Command: show snmp host

SNMP Host Table
-----
Host IPv6 Address : FF::FF
SNMP Version      : V3 na/np
CommunityName/SNMPv3 User Name : initial

Total Entries: 1

DGS-3627:5#
```

create trusted_host

Purpose	Used to create the trusted host.
Syntax	create trusted_host [<ipaddr> network <network_address>]
Description	The create trusted_host command creates the trusted host. The Switch allows specification of 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	<i><ipaddr></i> – The IP address of the trusted host to be created. <i><network_address></i> – IP address and netmask of the trusted host to be created. The address and mask information can be specified using the traditional format (for example, 10.1.2.3/255.0.0.0 or in CIDR format, 10.1.2.3/8).
Restrictions	Only administrator-level users can issue this command.

Example usage:

To create the trusted host:

```
DGS-3627:5#create trusted_host 10.48.74.121
Command: create trusted_host 10.48.74.121

Success.

DGS-3627:5#
```

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> – IP address and netmask of the trusted host to be viewed. The address and mask information can be specified using the traditional format (for example, 10.1.2.3/255.0.0.0 or in CIDR format, 10.1.2.3/8).
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To display the list of trust hosts:

```
DGS-3627:5#show trusted_host
Command: show trusted_host

Management Stations

IP Address
-----
10.53.13.94

Total Entries: 1

DGS-3627:5#
```

delete trusted_host

Purpose	Used to delete a trusted host entry made using the create trusted_host command above.
Syntax	delete trusted host [ipaddr <ipaddr> network <network_address> all]
Description	This command is used to delete a trusted host entry made using the create trusted_host command above.
Parameters	<i><ipaddr></i> – The IP address of the trusted host. <i>network <network_address></i> – IP address and netmask of the trusted host to be deleted. The address and mask information can be specified using the traditional format (for example, 10.1.2.3/255.0.0.0 or in CIDR format, 10.1.2.3/8). <i>all</i> – Enter this parameter to delete all configured trusted hosts.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To delete a trusted host with an IP address 10.48.74.121:

```
DGS-3627:5#delete trusted_host 10.48.74.121
Command: delete trusted_host 10.48.74.121

Success.

DGS-3627:5#
```

enable snmp traps

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

Example usage:

To enable SNMP trap support on the Switch:

```
DGS-3627:5#enable snmp traps
Command: enable snmp traps

Success.

DGS-3627:5#
```

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

enable snmp authenticate traps

	on the Switch.
Parameters	None.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example Usage:

To turn on SNMP authentication trap support:

```
DGS-3627:5#enable snmp authenticate traps
Command: enable snmp authenticate traps

Success.

DGS-3627:5#
```

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	Only administrator-level and operator-level users can issue this command.

Example usage:

To view the current SNMP trap:

```
DGS-3627:5#show snmp traps
Command: show snmp traps

SNMP Traps      : Enabled
Authenticate Trap : Enabled
Linkchange Trap  : Enabled

DGS-3627:5#
```

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-level and operator-level users can issue this command.

Example usage:

To prevent SNMP traps from being sent from the Switch:

```
DGS-3627:5#disable snmp traps
Command: disable snmp traps
```

Success.

DGS-3627:5#

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-level and operator-level users can issue this command.

Example Usage:

To disable the SNMP authentication trap support:

DGS-3627:5#disable snmp authenticate traps

Command: disable snmp authenticate traps

Success.

DGS-3627:5#

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	The config snmp system_contact 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.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To configure the Switch contact to “MIS Department II”:

DGS-3627:5#config snmp system_contact MIS Department II

Command: config snmp system_contact MIS Department II

Success.

DGS-3627:5#

config snmp system_location

Purpose	Used to enter a description of the location of the Switch.
Syntax	config snmp system_location <sw_location>

config snmp system_location

Description	The config snmp system_location 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.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

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

```
DGS-3627:5#config snmp system_location HQ 5F
Command: config snmp system_location HQ 5F

Success.

DGS-3627:5#
```

config snmp system_name

Purpose	Used to configure the name for the Switch.
Syntax	config snmp system_name <sw_name>
Description	The config snmp system_name command configures the name of the Switch.
Parameters	<sw_name> - A maximum of 255 characters is allowed.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To configure the Switch name for “DGS-3600 Switch”:

```
DGS-3627:5#config snmp system_name DGS-3600 Switch
Command: config snmp system_name DGS-3600 Switch

Success.

DGS-3627:5#
```

enable rmon

Purpose	Used to enable RMON on the Switch.
Syntax	enable rmon
Description	This command is used, in conjunction with the disable rmon command below, to enable and disable remote monitoring (RMON) on the Switch.
Parameters	None.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example Usage:

To enable RMON:


```
DGS-3627:5#enable rmon
Command: enable rmon

Success.

DGS-3627:5#
```

disable rmon

Purpose	Used to disable RMON on the Switch.
Syntax	disable rmon
Description	This command is used, in conjunction with the enable rmon command above, to enable and disable remote monitoring (RMON) on the Switch.
Parameters	None.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To disable RMON:

```
DGS-3627:5#disable rmon
Command: disable rmon

Success.

DGS-3627:5#
```

SWITCH UTILITY COMMANDS (INCLUDING FILE SYSTEM COMMANDS)

The download/upload 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> {{{unit [<unitid 1-12> all]} <drive_id> <pathname 64> {boot_up}}} cfg_fromTFTP [<ipaddr> <ipv6addr>] <path_filename 64> {{{<drive_id> } <pathname 64>}}
upload	[cfg_toTFTP [<ipaddr> <ipv6addr>] <path_filename 64>{{<drive_id> <pathname 64>} log_toTFTP [<ipaddr> <ipv6addr>] <path_filename 64> firmware_toTFTP [<ipaddr> <ipv6addr>] <path_filename 64> {{{<drive_id> <pathname 64>} attack_log_toTFTP [<ipaddr> <ipv6addr>] <path_filename 64> {unit <unit_id 1-12>}}]
config firmware	{{unit <unit_id 1-12>} <drive_id> <pathname 64> boot_up
show config	[active bootup {<drive_id> <pathname 64>}]
config configuration	{<drive_id> <pathname 64> [boot_up active]}
erase	{{unit <unitid 1-12>} <drive_id> <pathname 64>
rename	{{unit <unitid 1-12>} <drive_id> <pathname 64> <filename 64>
dir	{{unit [<unitid 1-12> all]} <drive_id>}
copy	{<drive_id> <pathname 64> {{{unit <unit_id 1-12>} <drive_id> <pathname 64>}}
show boot_file	{{unit <unitid 1-12> all}}
show storage_media_info	{{unit <unitid 1-12> all}}
config file_system_version	<version_number 1-2> {<string>}
ping	<ipaddr> {times <value 1-255>} {timeout <sec 1-99>}
ping6	<ipv6addr> {times <value 1-255> size <value 1-6000> timeout <sec 1-10>}
traceroute	<ipaddr> {ttl <value 1-60> port <value 30000-64900> timeout <value 1-65535> probe <value 1-9>}
enable autoconfig	
disable autoconfig	
show autoconfig	

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> {{{unit [<unitid 1-12> all]} <drive_id> <pathname 64> {boot_up}}} cfg_fromTFTP [<ipaddr> <ipv6addr>] <path_filename 64> {{{<drive_id> } <pathname 64>}}
Description	This command is used to download a new firmware or a Switch configuration file from a TFTP server. The user now has the option of saving the firmware or configuration file on the flash memory located in the Switch using the previously allocated c:\ drive.

download

Parameters	<p><i>firmware_fromTFTP</i> – Download and install new firmware on the Switch from a TFTP server.</p> <ul style="list-style-type: none"> • <i><ipaddr></i> – The IP address of the TFTP server. • <i><ipv6addr></i> - The IPv6 address of the TFTP server. • <i><path_filename 64></i> – The DOS path and filename of the firmware file on the TFTP server. For example, C:\3612.had. • <i>unit <unitid1-12></i>- Enter the ID of the Switch in the switch stack to where to save the file. • <i>all</i> – Use this parameter to select all switches in the switch stack. • <i><drive_id></i> - Enter the drive ID of the internal flash drive to where to save the file. • <i>{<pathname 64>}</i> – The <i>pathname</i> in the command refers to the flash memory located on the switch. This drive is nominated c: and those who wish to save the firmware, instead of uploading it directly to the NV-RAM must specify the path on the flash memory to place this file (ex. c:/firm1). The filename cannot exceed 64 alphanumeric characters. • <i>boot_up</i> – Enter this parameter to use this file as the boot up file upon next reboot of the switch. <p><i>config_fromTFTP</i> – Download and install a configuration file on the Switch from a TFTP server.</p> <ul style="list-style-type: none"> • <i><ipaddr></i> – The IP address of the TFTP server. • <i><ipv6addr></i> - The IPv6 address of the TFTP server. • <i><path_filename 64></i> – The DOS path and filename of the switch configuration file on the TFTP server. For example, C:\3612.had. • <i><drive_id></i> - Enter the drive ID of the internal flash drive to where to save the file. • <i>{<path_filename 64>}</i> – The second <i>path_filename</i> in the command refers to the flash memory located on the switch. This drive is nominated c: and those who wish to save the firmware, instead of uploading it directly to the NV-RAM must specify the path on the flash memory to place this file (ex. c:/config1). The filename cannot exceed 64 alphanumeric characters.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To download a configuration file:

```
DGS-3627:5#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-3627:5#
DGS-3627:5##-----
DGS-3627:5##                      DGS-3627 Configuration
DGS-3627:5##
DGS-3627:5##                      Firmware: Build 2.40-B19
DGS-3627:5##                      Copyright(C) 2008 D-Link Corporation. All rights reserved.
DGS-3627:5##-----
DGS-3627:5#
DGS-3627:5#
DGS-3627:5## BASIC
DGS-3627:5#
DGS-3627:5#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-3600” appears followed by the command prompt.

```
DGS-3627:5#disable authen_policy
Command: disable authen_policy
```

Success.

```
DGS-3627:5#
DGS-3627:5##-----
DGS-3627:5##           End of configuration file for DGS-3627
DGS-3627:5##-----
DGS-3627:5#
```

To download a firmware file to the FLASH memory of the Switch:

```
DGS-3627:5# download firmware_fromTFTP 10.53.13.201 c:\3612firm.had c:\ firm1
Command: download firmware_fromTFTP 10.53.13.201 c:\3612firm.had c:\ firm1
```

```
Connecting to server.....Done.
Download firmware.....Done. Do not power off!
Upload file to FLASH.....Done.
```

```
DGS-3627:5#
```

upload

Purpose	Used to upload a configuration file or log file to a TFTP server.
Syntax	upload [cfg_toTFTP [<ipaddr> <ipv6addr>] <path_filename 64> {{<drive_id> <pathname 64>} log_toTFTP [<ipaddr> <ipv6addr>] <path_filename 64> firmware_toTFTP [<ipaddr> <ipv6addr>] <path_filename 64> {{<drive_id> <pathname 64>} attack_log_toTFTP [<ipaddr> <ipv6addr>] <path_filename 64> {unit <unit_id 1-12>}]
Description	This command is used to upload a configuration file or log file to a TFTP server. The user now has the option of saving the log or configuration file on the flash memory located in the Switch using the previously allocated c:/ drive.
Parameters	<p><i>cfg_toTFTP</i> – Used to upload the current Switch configuration file to a TFTP server, or to upload a configuration file saved in the Switch’s flash memory to a TFTP server.</p> <ul style="list-style-type: none"> • <ipaddr> – The IP address of the TFTP server. • <ipv6addr> - The IPv6 address of the TFTP server. • <path_filename 64> – The DOS path and filename of the configuration file to be uploaded on the TFTP server. For example, C:\3612.cfg. • <drive_id> - Enter the drive ID of the internal flash drive to where to upload the file. • {<path_filename 64>} – The second <i>path_filename</i> in the command refers to the flash memory located on the Switch. This drive is nominated c: and those who wish to save this file to a TFTP server must enter the path and file name of the configuration file located on the flash memory of the Switch using this parameter. <p><i>log_toTFTP</i> – Used to upload a log file on the Switch to a TFTP server, or to upload a log file saved in the Switch’s flash memory to a TFTP server.</p> <ul style="list-style-type: none"> • <ipaddr> – The IP address of the TFTP server. • <ipv6addr> - The IPv6 address of the TFTP server.

upload

- *<path_filename 64>* – The DOS path and filename of the log file to be uploaded on the TFTP server. For example, C:\3612.txt.
- firmware_toTFTP* – Use this parameter to upload firmware to a TFTP server.
- *<ipaddr>* – The IP address of the TFTP server.
 - *<ipv6addr>* - The IPv6 address of the TFTP server.
 - *<path_filename 64>* – The DOS path and filename of the log file to be uploaded on the TFTP server. For example, C:\3627.txt.
 - *<drive_id>* - Enter the drive ID of the internal flash drive to where to upload the file.
 - *{<path_filename 64>}* – The second *path_filename* in the command refers to the flash memory located on the Switch. This drive is nominated c: and those who wish to save this file to a TFTP server must enter the path and file name of the configuration file located on the flash memory of the Switch using this parameter.
- attack_log_toTFTP* - This command is used to upload a switch attack log to a TFTP server, such as a spoofing attack.
- *<ipaddr>* - Enter the IPv4 address of the TFTP server to which to upload the attack log.
 - *<ipv6addr>* - Enter the IPv6 address of the TFTP server to which to upload the attack log.
 - *<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.
 - *unit <unit_id 1-12>* - Select the switch in the switch stack from where these attack log files will be uploaded, denoted by unit ID number.

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

Example usage:

To upload a configuration file to the TFTP server.

```
DGS-3627:5# upload cfg_toTFTP 10.53.13.3 c:\3627.cfg
```

```
Command: upload cfg_toTFTP 10.53.13.3 c:\3627.cfg
```

```
Connecting to server.....Done.
```

```
Upload configuration.....Done.
```

```
DGS-3627:5#
```

To upload a configuration file saved in the flash memory of the Switch to the TFTP server.

```
DGS-3627:5# upload cfg_toTFTP 10.53.13.3 c:\3627.cfg c:\ startup.cfg
```

```
Command: upload cfg_toTFTP 10.53.13.3 c:\3627.cfg c:\ startup.cfg
```

```
Connecting to server.....Done.
```

```
Upload configuration.....Done.
```

```
DGS-3627:5#
```

config firmware

Purpose	Used to configure a firmware file located in the flash memory as the boot up section.
Syntax	config firmware {{unit <unitid 1-12> } <drive_id>} <pathname 64> boot_up
Description	This command is used to configure firmware files located on the flash memory of the Switch, as the boot up configuration file.
Parameters	<p><i>unit <unit_id 1-12></i> - Select the switch in the switch stack where the firmware image is that will be configured, denoted by unit ID number.</p> <p><i><drive_id></i> - Enter the drive ID of the internal Flash drive to where to upload the file.</p> <p><i><pathname 64></i> - Enter the path and file name of the firmware file located in the Switch's flash memory, which will be used as the boot up firmware upon next reboot of the Switch.</p> <p><i>boot_up</i> - Entering this parameter will specify the firmware file as a boot up section.</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure firmware section 1 as a boot up section:

```
DGS-3627:5#config firmware C:\ 3627.had boot_up
Command: config firmware C:\ 3627.had boot_up

Success.

DGS-3627:5#
```

show config

Purpose	Used to display the current or saved version of the configuration settings of the switch.
Syntax	show config [active boot_up {<drive_id>} <pathname 64>]
Description	<p>Use this command 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).</p> <p>The configuration settings are listed by category in the following order:</p>

show config

- | | |
|--|-----------------------------------|
| 1. Basic (serial port, Telnet and web management status) | 21. SNTP |
| 2. Storm control | 22. LACP |
| 3. IP group management (Single IP) | 23. IP |
| 4. Syslog | 24. IGMP snooping |
| 5. QoS | 25. MLD Snooping |
| 6. Port mirroring | 26. Access Authentication Control |
| 7. Traffic segmentation | 27. AAA |
| 8. Port | 28. ARP |
| 9. Port lock | 29. Static Route |
| 10. Time Range | 30. Policy Route |
| 11. ACL | 31. IGMP |
| 12. IP-MAC address binding | 32. PIM |
| 13. VLAN | 33. DVMRP |
| 14. 802.1x | 34. RIP |
| 15. FDB | 35. MD5 |
| 16. MAC address table notification | 36. OSPF |
| 17. STP | 37. DNSR |
| 18. Safeguard Engine | 38. DHCP Relay |
| 19. Banner and Prompt | 39. VRRP |
| 20. SSH | |

Parameters

active – Entering this parameter will display configurations entered without being saved to NVRAM.

boot_up - Entering this parameter will display configurations that are to be used upon the next reboot of the Switch.

drive_id – Enter the drive ID number where the firmware file is located on the flash drive that is to be viewed.

<pathname 64> - The user may enter the path and file name of a configuration file located on the flash memory of the Switch, which will then be displayed

Restrictions None.

Example usage:

To view the current configuration settings:

```
DGS-3627:5#show config active
Command: show config active

#-----
#                               DGS-3627 Gigabit Ethernet Switch
#                               Configuration
#
#                               Firmware: Build 2.40-B19
#                               Copyright(C) 2008 D-Link Corporation. All rights reserved.
#-----

# DOUBLE_VLAN

disable double_vlan

# BASIC

config serial_port auto_logout 10_minutes
enable telnet 23
enable web 80
enable clipaging

# STORM
```

CTRL+C **ESC** **q** Quit **SPACE** **n** Next Page **Enter** Next Entry **a** All

config configuration	
Purpose	Used to configure the configuration file located on the flash memory as a boot up configuration, or as an active configuration.
Syntax	config configuration {<drive_id>} <pathname 64> [boot_up active]
Description	This command is used to configure the configuration file on the flash drive of the Switch. The user may choose to use it as a boot up or active section.
Parameters	<p><i>drive_id</i> – Enter the drive ID number where the configuration file is located on the flash drive that is to be configured.</p> <p><i><pathname 64></i> – Specifies the path and filename of the configuration file located on the flash drive of the Switch.</p> <p><i>boot_up</i> – Entering this parameter will specify the configuration file as a boot up section.</p> <p><i>active</i> – Entering this parameter will first load and then activate this configuration file on the switch.</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure FLASH file “c:/startup.cfg” as the boot up configuration:

```
DGS-3627:5#config configuration C:\ startup.cfg boot_up
Command: config configuration C:\ startup.cfg boot_up

Success.

DGS-3627:5#
```

erase	
Purpose	Used to delete a file located on the internal flash memory of the Switch.
Syntax	erase {{unit [<unitid 1-12>]} <drive_id>} <pathname 64>
Description	This command is used to erase a file located on the internal flash memory of the Switch.
Parameters	<p><i>unit <unit_id 1-12></i> - Select the switch in the switch stack where the file is that will be configured, denoted by unit ID number.</p> <p><i><drive_id></i> - Enter the drive ID of the internal flash drive to be erased.</p> <p><i><pathname 64></i> – Specifies the path and filename of the file located on the flash drive of the Switch, to be deleted.</p>
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To delete file “c:/startup.cfg” from the Switch’s flash memory:


```
DGS-3627:5#erase c:/ startup.cfg
Command: erase c:/ startup.cfg
Please wait, do not power off!
Process .....Done.
```

Success.

```
DGS-3627:5#
```

rename	
Purpose	To rename a file.
Syntax	rename {{unit [<unitid 1-12>]} <drive_id> <pathname 64> <filename 64>
Description	This command is used to rename a filename located on the internal flash memory.
Parameters	<p><i>unit</i> <unit_id 1-12> - Select the switch in the switch stack where the firmware image is, that will be configured, denoted by unit ID number.</p> <p><drive_id> - Enter the drive ID of the internal flash drive to be renamed.</p> <p><pathname 64> - Enter the path and name of the file to be renamed.</p> <p><filename 64> - Enter the new name of the file to be renamed. This entry cannot exceed 64 characters in length.</p>
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To rename a file:

```
DGS-3627:5#rename C:\ abc.txt cba.txt
Command: rename C:\ abc.txt cba.txt

Success.

DGS-3627:5#
```

dir	
Purpose	Used to list the files located on the flash memory drive, labeled c: .
Syntax	dir {{unit [<unitid 1-12> all]} <drive_id>}
Description	This command is used to display files saved to the flash directory of the Switch. Since there is only one labeled drive located on the flash, the user can only input the command <i>dir c:</i> to view the contents of the flash memory.
Parameters	<p><i>unit</i> <unitid 1-12> - Select the switch in the switch stack where the files are, that will be displayed, denoted by unit ID number.</p> <p><i>all</i> - Use this parameter to select all switches in the switch stack.</p> <p><drive_id> - Enter the drive ID of the internal flash drive to be viewed.</p>
Restrictions	None.

Example usage:

To view the directory files on the internal flash drive:

```
DGS-3627:5#dir c:
Command: dir C:\

-----
Current Unit ID: 1
Current Directory: C:\

File Name                               Size(byte)                               Update time
-----
LOG.TXT                                 520124 bytes                              2007/10/27 16:56
RUN.HAD (*)                             2678500 bytes                             2007/10/27 16:25
STARTUP.CFG (*)                          11007 bytes                               2007/10/27 16:24
-----
Total Files                             4
Total Size                               9293625 bytes
Free Space                               2097152 bytes
** means boot up section

DGS-3627:5#
```

copy	
Purpose	Used to copy a file.
Syntax	copy {<drive_id>} <pathname 64> {{unit_id 1-12}} <drive_id> <pathname 64>
Description	This command is used to copy a file from a source location and paste it to a host location. This command is only operable for the storage media accessory.
Parameters	<drive_id> - Enter the drive ID of the internal flash drive where the file is to be copied from. <pathname 64> - Enter the path and name of the file to be renamed. unit <unit_id 1-12> - Select the switch in the switch stack where the firmware image is to be copied to, denoted by unit ID number. <drive_id> - Enter the drive ID of the internal flash drive where the file is to be copied to. <pathname 64> - Enter the path and name of the file to be renamed.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To copy a file:

```
DGS-3627:5#copy C:\ abc.cfg C:\ def.txt
Command: copy C:\ abc.cfg C:\ def.txt

Please wait, do not power off!
Process .....Done.

DGS-3627:5#
```

show boot_file

Purpose	Used to show the currently set boot files located on the Switch.
Syntax	show boot_file {[unit <unitid 1-12> all]}
Description	This command is used to display the name and path of the firmware image and configuration file that have been previously set up by the user, as the boot up files.
Parameters	<i>unit</i> <unit_id 1-12> - Select the switch in the switch stack where the boot file is located, denoted by unit ID number. <i>all</i> – Enter this parameter to display the boot files on all switches in the switch stack.
Restrictions	None.

Example usage:

To rename a file:

```
DGS-3627:5#show boot_file
Command: show boot_file
-----
Unit ID : 1
Boot up firmware image : C:\RUN.HAD
Boot up configuration file: C:\STARTUP.CFG
-----

DGS-3627:5#
```

show storage_media_info

Purpose	Used to view flash memory information on the Switch.
Syntax	show storage_media_info {[unit <unitid 1-12> all]}
Description	This command will display information regarding the internal flash memory of the Switch. This command will display the following information: Drive: The name of the drive of the storage media accessory. Media_Type: Description of the type of storage media accessory currently in use. Size: Description of the size of memory space available on the storage media accessory. Label: Description assigned to this storage media accessory. FS_Type: Description of the type of format of this storage media accessory.
Parameters	<i>unit</i> <unit_id 1-12> - Select the switch in the switch stack where the storage media information is located, denoted by unit ID number. <i>all</i> – Enter this parameter to display the storage media information on all switches in the switch stack.
Restrictions	None.

Example usage:

To view the storage media accessory information:

```
DGS-3627:5#show storage_media_info
Command: show storage_media_info

-----
Unit ID is 1
Drive Media_Type  Size  Label  FS_Type
C:  Flash  15 MB  FLASH-A  FAT16
-----

DGS-3627:5#
```

config file_system_version	
Purpose	Used to configure the file system version.
Syntax	config file_system_version <version_number 1-2> {<string>}
Description	This command is used to configure the file system version. Users may now upgrade the file system version to 2 which will bring another, more stable, file system into the switch. Version one file system is compatible with all firmwares, yet once the file system has been upgraded to version 2, users may not return to release one firmware as it may damage the file system.
Parameters	<i><version_number 1-2></i> - Enter the version number of the file system. If the designated file system version is lower than the current file system version, this command will have no effect. <i>string</i> – This string is used to set the confirmation question that will follow the entry of this command. Entering “/y” will execute the command without prompt. Entering “/n” will not execute the command without prompt. If neither “/y” nor “/n” is specified, it will prompt the user before executing the command.
Restrictions	Only administrator-level users can issue this command. Do NOT power off the switch during the execution of this command.



Note: Do not use release 1 firmware after upgrading the file system version as it may damage the file system of the switch.



Note: Do not power off the switch during the execution of this file as it may damage the file system of the switch.

Example usage:

To view the storage media accessory information:

```
DGS-3627:5#config file_system_version 2
Command: config file_system_version 2

Are you sure you want to update the file system version? (y/n) n

DGS-3627:5#
```

ping	
Purpose	Used to test the connectivity between network devices.
Syntax	ping <ipaddr> {times <value 1-255>} {timeout <sec 1-99>}
Description	The Ping command sends Internet Control Message Protocol (ICMP) echo messages to a remote IP address. The remote IP address will then “echo” or return the message. This is used to confirm connectivity between the Switch and the remote device.
Parameters	<p><i><ipaddr></i> - Specifies the IP address of the host.</p> <p><i>times <value 1-255></i> - 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.</p> <p><i>timeout <sec 1-99></i> - 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.</p>
Restrictions	None.

Example usage:

To ping the IP address 10.48.74.121 four times:

```
DGS-3627:5#ping 10.48.74.121 times 4
Command: ping 10.48.74.121 times 4

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-3627:5#
```

ping6	
Purpose	Used to test the connectivity between IPv6 ready network devices.
Syntax	ping6 <ipv6addr> {times <value 1-255> size <value 1-6000>} {timeout <value 1-10>}
Description	The ping6 command sends Internet Control Message Protocol (ICMPv6) echo messages to a remote IPv6 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	<p><i><ipv6addr></i> - Specifies the IP address of the host.</p> <p><i>times <value 1-255></i> - The number of individual ICMP echo</p>

ping6

messages to be sent. The maximum value is 255.

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 2009::280:C8FF:FE3C:5C8A four times:

```
DGS-3627:5#ping6 2009::280:C8FF:FE3C:5C8A times 4 timeout 10
```

```
Command: ping6 2009::280:C8FF:FE3C:5C8A times 4 timeout 10
```

```
Reply from 2009::280:C8FF:FE3C:5C8A, bytes=100 time<10 ms
```

```
Reply from 2009::280:C8FF:FE3C:5C8A, bytes=100 time<10 ms
```

```
Reply from 2009::280:C8FF:FE3C:5C8A, bytes=100 time<10 ms
```

```
Reply from 2009::280:C8FF:FE3C:5C8A, bytes=100 time<10 ms
```

```
Ping statistics for 2009::280:C8FF:FE3C:5C8A
```

```
Packets: Sent =4, Received =4, Lost =0
```

```
DGS-3627:5#
```

traceroute

Purpose Used to trace the routed path between the Switch and a destination endstation.

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

Description The traceroute command will trace a route between the Switch and a give host on the network.

Parameters

<ipaddr> - Specifies the IP address of the host.

ttl <value 1-60> - The time to live value of the trace route request. This is the maximum number of routers the traceroute command will cross while seeking the network path between two devices.

port <value 30000-64900> - The port number. Must be above 1024.The value range is from 30000 to 64900.

timeout <sec 1-65535> - Defines the time-out period while waiting for a response from the remote device. The user may choose an entry between 1 and 65535 seconds.

probe <value 1-9> - The probe value is the number of times the Switch will send probe packets to the next hop on the intended traceroute path. The default is 1.

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

Example usage:

To trace the routed path between the Switch and 172.18.212.109.

```
DGS-3627:5#traceroute 172.18.212.109
```

```
Command: traceroute 172.18.212.109
```

```
10 ms 172.18.212.109
```

```
Trace complete.
```

```
DGS-3627:5#
```

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-level 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 DHCP server software if you are unsure.

Example usage:

To enable autoconfiguration on the Switch:

```
DGS-3627:5#enable autoconfig
```

```
Command: enable autoconfig
```

```
Success.
```

```
DGS-3627:5#
```

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.



NOTE: If the autoconfig function fails, the user will be prompted with a warning message and the switch will not upload the configuration settings.

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-3627 Gigabit Ethernet Switch
Command Line Interface

Firmware: Build 2.40-B19
Copyright(C) 2008 D-Link Corporation. All rights reserved.

DGS-3627:5#download cfg_fromTFTP 10.41.44.44 c:\cfg\setting.txt
Command: download cfg_fromTFTP 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-3627:5#disable authen_policy
Command: disable authen_policy

Success.

DGS-3627:5#
DGS-3627:5##-----
DGS-3627:5##          End of configuration file for DGS-3627
DGS-3627:5#

*****
* 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 instructs 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-level and operator-level users can issue this command.

Example usage:

To stop the autoconfiguration function:

```
DGS-3627:5#disable autoconfig
Command: disable autoconfig

Success.

DGS-3627:5#
```

show autoconfig

Purpose	Used to display the current autoconfig status of the Switch.
Syntax	show autoconfig
Description	This will list the current status of the autoconfiguration function.
Parameters	None.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To upload an autoconfiguration-:

```
DGS-3627:5#show autoconfig
Command: show autoconfig

Autoconfig State: Disabled.

DGS-3627:5#
```

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	[ports cpu]
clear counters	{ports <portlist>}
clear log	
show log	{index <value_list> }
clear attack_log	{[unit <unit_id 1-12> all]}
show attack_log	{unit <unit_id 1-12>} {index <value_list>}
enable syslog	
disable syslog	
show syslog	
create syslog host	<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]}
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 system_severity	[trap log all] [critical warning information]
show system_severity	
config log_save_timing	[time_interval <min 1-65535> on_demand log_trigger]
show log_save_timing	

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. The beginning and end of the port list range are separated by a dash.
Restrictions	None.

Example usage:

To display the packets analysis for port 2:

```
DGS-3627:5#show packet ports 2
Command: show packet ports 2

Port number : 2
=====
Frame Size/Type          Frame Counts          Frames/sec
-----
64                        3275                  10
65-127                   755                   10
128-255                   316                   1
256-511                   145                   0
512-1023                  15                    0
1024-1518                 0                     0
Unicast RX                152                   1
Multicast RX              557                   2
Broadcast RX              3686                  16

Frame Type              Total                Total/sec
-----
RX Bytes                408973               1657
RX Frames                395                  19
TX Bytes                7918                 178
TX Frames                111                  2

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

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. The beginning and end of the port list range are separated by a dash.
Restrictions	None.

Example usage:

To display the errors of the port 3:

```
DGS-3627:5#show error ports 3
Command: show error ports 3

Port number : 3

          RX Frames          TX Frames
          -----          -----
CRC Error    19      Excessive Deferral    0
Undersize    0      CRC Error          0
Oversize     0      Late Collision       0
Fragment     0      Excessive Collision  0
Jabber       11      Single Collision     0
Drop Pkts    20837   Collision            0
Symbol Error 0

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

show utilization	
Purpose	Used to display real-time port and cpu utilization statistics.
Syntax	show utilization [ports cpu]
Description	This command will display the real-time port and CPU utilization statistics for the Switch.
Parameters	<p><i>ports</i> - Entering this parameter will display the current port utilization of the Switch.</p> <p><i>cpu</i> – Entering this parameter will display the current CPU utilization of the Switch.</p>
Restrictions	None.

Example usage:

To display the port utilization statistics:

```

DGS-3627:5#show utilization ports
Command: show utilization ports

Port  TX/sec  RX/sec  Util    Port  TX/sec  RX/sec  Util
-----  -----  -----  ---    -----  -----  -----  ---
1      0        0        0      22     0        0        0
2      0        0        0      23     0        0        0
3      0        0        0      24     0        0        0
4      0        0        0      25     0        0        0
5      0        0        0      26     0        0        0
6      0        0        0      27     0        0        0
7      0        0        0
8      0        0        0
9      0        0        0
10     0        0        0
11     0        0        0
12     0        0        0
13     0        0        0
14     0        0        0
15     0        0        0
16     0        0        0
17     0        0        0
18     0        0        0
19     0        0        0
20     0        0        0
21     0        0        0
CTRL+C  ESC q Quit  SPACE n Next Page  p Previous Page  r Refresh
    
```

Example usage:

To display the current CPU utilization:

```

DGS-3627:5#show utilization cpu
Command: show utilization cpu

CPU utilization :
-----
Five seconds - 15%    One minute - 25%    Five minutes - 14%

DGS-3627:5#
    
```

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. The beginning and end of the port list range are separated by a dash.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To clear the counters:

```
DGS-3627:5#clear counters ports 2-9
Command: clear counters ports 2-9

Success.

DGS-3627:5#
```

clear log

Purpose	Used to clear the Switch's history log.
Syntax	clear log
Description	This command will clear the Switch's history log.
Parameters	None.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To clear the log information:

```
DGS-3627:5#clear log
Command: clear log

Success.

DGS-3627:5#
```

show log

Purpose	Used to display the switch history log.
Syntax	show log {index <value_list>}
Description	This command will display the contents of the Switch's history log.
Parameters	<i>index <value_list></i> – This command will display the history log entry listed by the <value_list> field. If no parameter is specified, all history log entries will be displayed.
Restrictions	None.

Example usage:

To display the switch history log:

```
DGS-3627:5#show log
Command: show log

Index      Date       Time       Log Text
-----
5          2006-08-21 00:01:09   Successful login through Console (Username: Anonymous,
IP:10.53.13.202, MAC: 00-0C-6E-6B-EB-0C)
4          2006-08-21 00:00:14   System started up
3          2006-08-21 00:00:06   Port 1 link up, 100Mbps FULL duplex
2          2006-08-21 00:00:01   Spanning Tree Protocol is disabled
1          2006-08-21 00:06:31   Configuration saved to flash (Username: Anonymous)

DGS-3627:5#
```

show attack_log	
Purpose	Used to display the switch history of attack log files.
Syntax	show attack_log {unit <unit_id 1-12>} {index <value_list>}
Description	This command will display the contents of the attack log of the Switch. This log displays the time and date of a possible attack on the switch, such as a spoofing attack.
Parameters	<i>unit <unit_id 1-12></i> - Select the switch in the switch stack for which to view attack log files. <i>index <value list></i> – This command will display the history log, beginning at 1 and ending at the value specified by the user in the <i><value_list></i> field. If no parameter is specified, all history log entries will be displayed.
Restrictions	None.

Example usage:

To display the attack log:

```
DGS-3627:5#show attack_log index 1-2
Command: show attack_log index 1-2

Index      Date       Time       Log Text
-----
2          2006-04-25 12:38:00   Possible spoofing attack from 000d010023001 port 23
1          2006-04-25 12:37:42   Possible spoofing attack from 000d010023001 port 23

DGS-3627:5#
```

clear attack_log

Purpose	Used to clear the switch history of attack log files.
Syntax	clear attack_log {[unit <unit_id 1-12> all]}
Description	This command will clear the contents of the attack log of the Switch.
Parameters	<i>unit</i> <unit_id 1-12> - Select the switch in the switch stack for which to clear attack log files. <i>all</i> – Entering this parameter will clear all attack log files in the switch stack.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To clear the attack log:

```
DGS-3627:5#clear attack_log
Command: clear attack_log

Success.

DGS-3627:5#
```

enable syslog

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

Example usage:

To the syslog function on the Switch:

```
DGS-3627:5#enable syslog
Command: enable syslog

Success.

DGS-3627:5#
```

disable syslog

Purpose	Used to enable the system log to be sent to a remote host.
Syntax	disable syslog
Description	The disable syslog command disables the system log to be sent to a remote host.
Parameters	None.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To disable the syslog function on the Switch:

```
DGS-3627:5#disable syslog
Command: disable syslog

Success.

DGS-3627:5#
```

show syslog

Purpose	Used to display the syslog protocol status as enabled or disabled.
Syntax	show syslog
Description	The show syslog command displays the syslog status as enabled or disabled.
Parameters	None.
Restrictions	None.

Example usage:

To display the current status of the syslog function:

```
DGS-3627:5#show syslog
Command: show syslog

Syslog Global State: Enabled

DGS-3627:5#
```

create syslog host

Purpose	Used to create a new syslog host.																
Syntax	create syslog host <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	The create syslog host command is used to create a new syslog host.																
Parameters	<p><i><index 1-4></i> – Specifies that the command will be applied to an index of hosts. There are four available indexes, numbered 1 through 4.</p> <p><i>ipaddress <ipaddr></i> – Specifies the IP address of the remote host where syslog messages will be sent.</p> <p><i>severity</i> – Severity level indicator, as shown below:</p> <p>Bold font indicates that the corresponding severity level is currently supported on the Switch.</p> <table> <thead> <tr> <th>Numerical Code</th> <th>Severity</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>Emergency: system is unusable</td> </tr> <tr> <td>1</td> <td>Alert: action must be taken immediately</td> </tr> <tr> <td>2</td> <td>Critical: critical conditions</td> </tr> <tr> <td>3</td> <td>Error: error conditions</td> </tr> <tr> <td>4</td> <td>Warning: warning conditions</td> </tr> <tr> <td>5</td> <td>Notice: normal but significant condition</td> </tr> <tr> <td>6</td> <td>Informational: informational messages</td> </tr> </tbody> </table>	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
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																

create syslog host

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 that the Switch currently supports.

Numerical Facility

Code

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

local0 – Specifies that local use 0 messages 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

create syslog host

	<p>syslog protocol will use to send messages to the remote host.</p> <p><i>ipaddress <ipaddr></i> – Specifies the IP address of the remote host where syslog messages will be sent.</p> <p><i>state [enable disable]</i> – Allows the sending of syslog messages to the remote host, specified above, to be enabled and disabled.</p>
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To create syslog host:

```
DGS-3627:5#create syslog host 1 ipaddress 10.1.1.1 state enable
Command: create syslog host 1 ipaddress 10.1.1.1 state enable

Success.

DGS-3627:5#
```

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	The config syslog host command is used to configure the syslog protocol to send system log information to a remote host.																		
Parameters	<p><index 1-4> – Specifies that the command will be applied to an index of hosts. There are four available indexes, numbered 1 through 4.</p> <p><i>ipaddress <ipaddr></i> – Specifies the IP address of the remote host where syslog messages will be sent.</p> <p><i>severity</i> – Severity level indicator. These are described in the following: Bold font indicates that the corresponding severity level is currently supported on the Switch.</p> <table border="1"> <thead> <tr> <th>Numerical Code</th> <th>Severity</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>Emergency: system is unusable</td> </tr> <tr> <td>1</td> <td>Alert: action must be taken immediately</td> </tr> <tr> <td>2</td> <td>Critical: critical conditions</td> </tr> <tr> <td>3</td> <td>Error: error conditions</td> </tr> <tr> <td>4</td> <td>Warning: warning conditions</td> </tr> <tr> <td>5</td> <td>Notice: normal but significant condition</td> </tr> <tr> <td>6</td> <td>Informational: informational messages</td> </tr> <tr> <td>7</td> <td>Debug: debug-level messages</td> </tr> </tbody> </table>	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	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																		

config syslog host

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.

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)

config syslog host

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-level and operator-level users can issue this command.

Example usage:

To configure a syslog host:

```
DGS-3627:5#config syslog host 1 severity all
```

```
Command: config syslog host 1 severity all
```

```
Success.
```

```
DGS-3627:5#
```

```
DGS-3627:5#config syslog host 1 facility local0
```

```
Command: config syslog host 1 facility local0
```

```
Success.
```

```
DGS-3627:5#
```

Example usage:

To configure a syslog host for all hosts:

```
DGS-3627:5#config syslog host all severity all
```

```
Command: config syslog host all severity all
```

```
Success.
```

```
DGS-3627:5#
```

```
DGS-3627:5#config syslog host all facility local0
Command: config syslog host all facility local0

Success.

DGS-3627:5#
```

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	The delete syslog host 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-level and operator-level users can issue this command.

Example usage:

To delete a previously configured syslog host:

```
DGS-3627:5#delete syslog host 4
Command: delete syslog host 4

Success.

DGS-3627:5#
```

show syslog host

Purpose	Used to display the syslog hosts currently configured on the Switch.
Syntax	show syslog host {<index 1-4>}
Description	The show syslog host 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-3627:5#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-3627:5#					

config system_severity

Purpose	To configure severity level of an alert required for log entry or trap message.
Syntax	config system_severity [trap log all] [critical warning information]
Description	<p>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).</p> <ul style="list-style-type: none"> • 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	<p>Choose one of the following to identify where severity messages are to be sent.</p> <ul style="list-style-type: none"> • <i>trap</i> – Entering this parameter will define which events occurring on the Switch will be sent to a SNMP agent for analysis. • <i>log</i> – Entering this parameter will define which events occurring on the Switch will be sent to the Switch's log for analysis. • <i>all</i> – 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. <p>Choose one of the following to identify what level of severity warnings are to be sent to the destination entered above.</p> <ul style="list-style-type: none"> • <i>critical</i> – Entering this parameter along with the proper destination, stated above, will instruct the Switch to send only critical events to the Switch's log or SNMP agent. • <i>warning</i> – 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. • <i>information</i> – 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-level and operator-level users can issue this command.

Example usage:

To configure the system severity settings for critical traps only:

<p>DGS-3627:5#config system_severity trap critical Command: config system_severity trap critical</p> <p>Success.</p> <p>DGS-3627:5#</p>
--

show system_severity

Purpose	To display the current severity settings set on the Switch.
Syntax	show system_severity
Description	This command is used to view the severity settings that have been implemented on the Switch using the config system_severity command.
Parameters	None.
Restrictions	None.

Example usage:

To view the system severity settings currently implemented on the Switch:

```
DGS-3627:5#show system_severity
Command: show system_severity

system_severity log   : information
system_severity trap  : critical

DGS-3627:5#
```

config log_save_timing

Purpose	Used to configure the method of saving log files to the switch's flash memory.
Syntax	config log_save_timing [time_interval <min 1-65535> on_demand log_trigger]
Description	The config log_save_timing command allows the user to configure the time method used in saving log files to the switch's flash memory.
Parameters	<p><i>time_interval</i> <min 1-65535> - Use this parameter to configure the time interval that will be implemented for saving log files. The log files will be save every x number of minutes that are configured here.</p> <p><i>on_demand</i> - Users who choose this method will only save log files when they manually tell the Switch to do so, using the save or save log command.</p> <p><i>log_trigger</i> - Users who choose this method will have log files saved to the Switch every time a log event occurs on the Switch.</p>
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To configure the time interval as every 30 minutes for saving log files:

```
DGS-3627:5#config log_save_timing time_interval 30
Command: config log_save_timing time_interval 30

Success.

DGS-3627:5#
```

show log_save_timing

Purpose	Used to display the method configured for saving log files to the switch's flash memory.
Syntax	show log_save_timing
Description	The show log_save_timing command allows the user to view the time method configured for saving log files to the switch's flash memory.
Parameters	None.
Restrictions	None.

Example usage:

To configure the time interval as every 30 minutes for saving log files:

```
DGS-3627:5#show log_save_timing
Command: show log_save_timing
Saving log method: every 30 minute(s)

DGS-3627:5#
```


MULTIPLE SPANNING TREE PROTOCOL (MSTP) COMMANDS

This Switch supports three versions of the Spanning Tree Protocol; 802.1d STP, 802.1w Rapid STP and 802.1s 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 BPDU 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 configuration name defined by an alphanumeric string of up to 32 characters (defined in the config stp mst_config_id command as name <string>).
- A configuration revision number (named here as a revision_level) and;
- 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:

- The Switch must be set to the MSTP setting (config stp version)
- The correct spanning tree priority for the MSTP instance must be entered (config stp priority).
- 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 <1-10> forwarddelay <value 4-30> txholdcount <value 1-10> fbpdudisable [enable disable] lbd [enable disable] lbd_recover_timer [0 <value 60-1000000>]}
config stp ports	<portlist> {externalCost [auto <value 1-200000000>] hellotime <value 1-10> migrate [yes no] edge [true false] p2p [true false auto] state [enable disable] lbd [enable disable] fbpdudisable [enable disable]}
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>}
config stp mst_ports	<portlist> instance_id <value 0-15> {internalCost [auto value 1-200000000] priority <value 0-240>}

Command	Parameters
show stp	
show stp ports	{<portlist>}
show stp instance_id	{<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-level and operator-level users can issue this command.

Example usage:

To enable STP, globally, on the Switch:

```
DGS-3627:5#enable stp
Command: enable stp

Success.

DGS-3627:5#
```

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-level and operator-level users can issue this command.

Example usage:

To disable STP on the Switch:

```
DGS-3627:5#disable stp
Command: disable stp

Success.

DGS-3627:5#
```

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	<p><i>mstp</i> – Selecting this parameter will set the Multiple Spanning Tree Protocol (MSTP) globally on the Switch.</p> <p><i>rstp</i> - Selecting this parameter will set the Rapid Spanning Tree Protocol (RSTP) globally on the Switch.</p> <p><i>stp</i> - Selecting this parameter will set the Spanning Tree Protocol (STP) globally on the Switch.</p>
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To set the Switch globally for the Multiple Spanning Tree Protocol (MSTP):

```
DGS-3627:5#config stp version mstp
```

```
Command: config stp version mstp
```

```
Success.
```

```
DGS-3627:5#
```

config stp

Purpose	Used to setup STP, RSTP and MSTP on the Switch.
Syntax	config stp {maxage <value 6-40> maxhops <value 1-20> hellotime <1-10> forwarddelay <value 4-30> txholdcount <value 1-10> fbpdudisable [enable disable] lbd [enable disable] lbd_recover_timer [<value 0> <value 60-1000000>]}
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	<p><i>maxage <value 6-40></i> – 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.</p> <p><i>maxhops <value 1-20></i> - 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 BPDU 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.</p> <p><i>hellotime <value 1-10></i> – The user may set the time interval between transmission of configuration messages by the root device in STP, or by the designated router in RSTP, thus stating that the Switch is still</p>

config stp

functioning. A time between 1 and 10 seconds may be chosen, with a default setting of 2 seconds.

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. The default value is 3.

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*.

lbd [enable | disable] – This feature is used to temporarily shutdown a port on the Switch when a BPDU packet has been looped back to the switch. When the Switch detects its own BPDU packet coming back, it signifies a loop on the network. STP will automatically be blocked and an alert will be sent to the administrator. The LBD STP port will restart (change to discarding state) when the LBD Recover Time times out. The Loopback Detection function will only be implemented on one port at a time. The default is enabled.

lbd_recover_timer [<value 0> | <value 60-1000000>] - This field will set the time the STP port will wait before recovering the STP state set. 0 will denote that the LBD will never time out or restart until the administrator personally changes it. The user may also set a time between 60 and 1000000 seconds. The default is 60 seconds.

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

Example usage:

To configure STP with maxage 18 and maxhops of 15:

```
DGS-3627:5#config stp maxage 18 maxhops 15
Command: config stp maxage 18 maxhops 15

Success.

DGS-3627:5#
```

config stp ports

Purpose	Used to setup STP on the port level.
Syntax	config stp ports <portlist> {externalCost [auto <value 1-200000000>] hellotime <value 1-10> migrate [yes no] edge [true false] p2p [true false auto] state [enable disable] lbd [enable disable] fbpdu [enable disable]}
Description	This command is used to create and configure STP for a group of ports.
Parameters	<p><i><portlist></i> – Specifies a range of ports to be configured. The beginning and end of the port list range are separated by a dash.</p> <p><i>externalCost</i> – 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 <i>auto</i>.</p> <ul style="list-style-type: none"> <i>auto</i> – 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.

config stp ports

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 1-10> – 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 10 seconds. The default is 2 seconds.

migrate [yes | no] – Setting this parameter as “yes” will set the ports to send out BPDU packets to other bridges, requesting information on their STP setting. If the Switch is configured for RSTP, the port will be capable to migrate from 802.1d STP to 802.1w RSTP. If the Switch is configured for MSTP, the port is capable of migrating from 802.1d STP to 802.1s MSTP. RSTP and MSTP can coexist with standard STP, however the benefits of RSTP and MSTP are not realized on a port where an 802.1d network connects to an 802.1w or 802.1s enabled network. Migration should be set as *yes* on ports connected to network stations or segments that are capable of being upgraded to 802.1w RSTP or 802.1s MSTP on all or some portion of the segment.

edge [true | false] – *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.

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*.

lbd [enable | disable] - Used to enable or disable the loopback detection function on the Switch for the ports configured above in the **config stp** command.

fbpdu [enable | disable] – Allows the forwarding of STP BPDU packets from other network devices when STP is disabled on the Switch. This function can only be in use when STP is globally disabled and forwarding BPDU packets is enabled. The default is *enabled* and BPDU packets will not be forwarded.

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

Example usage:

To configure STP with path cost 19, hellotime set to 5 seconds, migration enable, and state enable for ports 1-5.

```
DGS-3627:5#config stp ports 1-5 externalCost 19 hellotime 5
migrate yes state enable
```

```
Command: config stp ports 1-5 externalCost 19 hellotime 5
migrate yes state enable
```

```
Success.
```

```
DGS-3627:5#
```

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 four 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-level and operator-level users can issue this command.

Example usage:

To create a spanning tree instance 2:

```
DGS-3627:5#create stp instance_id 2
Command: create stp instance_id 2

Warning: there is no VLAN mapping to this instance_id!
Success.

DGS-3627:5#
```

config stp instance_id

Purpose	Used to add or delete an STP instance ID.
Syntax	config stp instance_id <value 1-15> [add_vlan remove_vlan] <vidlist>
Description	<p>This command is used to map VIDs (VLAN IDs) to previously configured STP instances on the Switch by creating an <i>instance_id</i>. 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.</p> <p>Note that switches in the same spanning tree region having the same STP <i>instance_id</i> must be mapped identically, and have the same configuration <i>revision_level</i> number and the same <i>name</i>.</p>
Parameters	<p><value 1-15> - Enter a number between 1 and 15 to define the <i>instance_id</i>. The Switch supports 16 STP regions with one unchangeable default instance ID set as 0.</p> <p><i>add_vlan</i> - Along with the <i>vid_range</i> <vidlist> parameter, this command will add VIDs to the previously configured STP <i>instance_id</i>.</p> <p><i>remove_vlan</i> - Along with the <i>vid_range</i> <vidlist> parameter, this command will remove VIDs to the previously configured STP <i>instance_id</i>.</p> <p><vidlist> - Specify the VID range from configured VLANs set on the Switch. Supported VIDs on the Switch range from ID number 1 to 4094.</p>
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To configure instance ID 2 to add VID 10:

```
DGS-3627:5#config stp instance_id 2 add_vlan 10
Command : config stp instance_id 2 add_vlan 10

Success.

DGS-3627:5#
```

Example usage:

To remove VID 10 from instance ID 2:

```
DGS-3627:5#config stp instance_id 2 remove_vlan 10
Command : config stp instance_id 2 remove_vlan 10

Success.

DGS-3627:5#
```

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-level and operator-level users can issue this command.

Example usage:

To delete STP instance ID 2 from the Switch.

```
DGS-3627:5#delete stp instance_id 2
Command: delete stp instance_id 2

Success.

DGS-3627:5#
```

config stp priority

Purpose	Used to update the STP instance configuration.
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 <i>instance_id</i> for forwarding packets. The lower the priority value set, the higher the priority.
Parameters	<i>priority <value 0-61440></i> - 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 entry must be divisible by 4096. <i>instance_id <value 0-15></i> - Enter the value corresponding to the previously configured instance ID for which to set the priority value. An instance id of 0 denotes the default <i>instance_id</i> (CIST) internally set on

config stp priority

	the Switch.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To set the priority value for *instance_id* 2 as 4096:

```
DGS-3627:5#config stp priority 4096 instance_id 2
Command : config stp priority 4096 instance_id 2

Success.

DGS-3627:5#
```

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>}
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 <i>revision_level</i> and <i>name</i> will be considered as part of the same MSTP region.
Parameters	<i>revision_level</i> <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. <i>name</i> <string> - Enter an alphanumeric string of up to 32 characters to uniquely identify the MSTP region on the Switch. This <i>name</i> , along with the <i>revision_level</i> value will identify the MSTP region configured on the Switch. If no <i>name</i> is entered, the default name will be the MAC address of the device.
Restrictions	Only administrator-level 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 “Zira”:

```
DGS-3627:5#config stp mst_config_id revision_level 10 name Zira
Command: config stp mst_config_id revision_level 10 name Zira

Success.

DGS-3627:5#
```

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>}
Description	This command will update the port configuration for a STP <i>instance_id</i> . If a loop occurs, the MSTP function will use the port priority to select an

config stp mst_ports

	<p>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 port number into the forwarding state and other interfaces will be blocked. Remember that lower priority values mean higher priorities for forwarding packets.</p>
Parameters	<p><i><portlist></i> - Specifies a range of ports to be configured. The beginning and end of the port list range are separated by a dash.</p> <p><i>instance_id <value 0-15></i> - Enter a numerical value between 0 and 15 to identify the <i>instance_id</i> previously configured on the Switch. An entry of 0 will denote the CIST (Common and Internal Spanning Tree).</p> <p><i>internalCost</i> - 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 <i>auto</i>. There are two options:</p> <ul style="list-style-type: none"> <i>auto</i> - Selecting this parameter for the <i>internalCost</i> will set quickest route automatically and optimally for an interface. The default value is derived from the media speed of the interface. <i>value 1-200000000</i> - Selecting this parameter with a value in the range of 1-200000000 will set the quickest route when a loop occurs. A lower <i>internalCost</i> represents a quicker transmission. <p><i>priority <value 0-240></i> - 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.</p>
Restrictions	<p>Only administrator-level and operator-level users can issue this command.</p>

Example usage:

To designate ports 1 to 2 on, with instance ID 1, to have an auto internalCost and a priority of 0:

```
DGS-3627:5#config stp mst_ports 1-2 instance_id 1 internalCost auto priority 0
Command: config stp mst_ports 1-2 instance_id 1 internalCost auto priority 0
Success.
DGS-3627:5#
```

show stp instance_id

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-3627:5#show stp
Command: show stp

STP Bridge Global Settings
-----
```

```

STP Status           : Enabled
STP Version          : STP Compatible
Max Age              : 20
Hello Time           : 2
Forward Delay        : 15
Max Hops             : 20
TX Hold Count        : 3
Forwarding BPDU      : Enabled
Loopback Detection   : Enabled
LBD Recover Time     : 60

DGS-3627:5#
    
```

Status 2 : STP enabled for RSTP

```

DGS-3627:5#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        : 3
Forwarding BPDU      : Enabled
Loopback Detection   : Enabled
LBD Recover Time     : 60

DGS-3627:5#
    
```

Status 3 : STP enabled for MSTP

```

DGS-3627:5#show stp
Command: show stp

STP Bridge Global Settings
-----

STP Status           : Enabled
STP Version          : MSTP
Max Age              : 20
Forward Delay        : 15
Max Hops             : 20
TX Hold Count        : 3
Forwarding BPDU      : Enabled
Loopback Detection   : Enabled
LBD Recover Time     : 60

DGS-3627:5#
    
```

show stp ports

Purpose	Used to display the Switch's current <i>instance_id</i> configuration.
Syntax	show stp ports <portlist>
Description	This command displays the STP Instance Settings and STP Instance Operational Status currently implemented on the Switch.

show stp ports

Parameters	<portlist> – Specifies a range of ports to be configured. The beginning and end of the port list range are separated by a dash.
Restrictions	None

Example usage:

To show STP ports 1 through 9:

```
DGS-3627:5#show stp ports 1-9
Command: show stp ports 1-9

MSTP Port Information
-----
Port Index      : 1 , Hello Time: 2 /2 , Port STP enabled LBD: Yes
External PathCost : Auto/200000 , Edge Port : No /No , P2P : Auto /Yes
Port Forward BPDU enabled

MSTI Designated Bridge   Internal PathCost   Prio   Status   Role
-----
0      8000/0050BA7120D6   200000           128   Forwarding   Root
1      8001/0053131A3324   200000           128   Forwarding   Master

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

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 <i>instance_id</i> 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-3627:5#show stp instance_id 0
Command: show stp instance_id 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 : 32766/00-90-27-39-78-E2
External Root Cost     : 200000
Regional Root Bridge   : 32768/00-53-13-1A-33-24
Internal Root Cost     : 0
Designated Bridge      : 32768/00-50-BA-71-20-D6
Root Port              : 1
Max Age                : 20
Forward Delay          : 15
```

Last Topology Change : 856
Topology Changes Count : 2987

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

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-3627:5#show stp mst_config_id
Command: show stp mst_config_id

Current MST Configuration Identification
-----

Configuration Name : 00:10:20:33:45:00          Revision Level :0
MSTI ID   Vid list
-----
CIST     1-4094

DGS-3627:5#
```

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> vlanid <vidlist>] mac_address <macaddr>}
show fdb	{port <port> [vlan <vlan_name 32> vlanid <vidlist>] mac_address <macaddr> static aging_time}
show ipfdb	<ipaddr>
config multicast filtering_mode	[<vlan_name 32> all] [forward_all_groups forward_unregistered_groups filter_unregistered_groups]
show multicast filtering_mode	{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	<p><vlan_name 32> – The name of the VLAN on which the MAC address resides.</p> <p><macaddr> – The MAC address that will be added to the forwarding table.</p> <p>port <port> – The port number corresponding to the MAC destination address. The Switch will always forward traffic to the specified device through this port.</p>
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To create a unicast MAC FDB entry:

```
DGS-3627:5#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-3627:5#
```

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-level and operator-level users can issue this command.

Example usage:

To create multicast MAC forwarding:

```
DGS-3627:5#create multicast_fdb default 01-00-00-00-00-01
Command: create multicast_fdb default 01-00-00-00-00-01

Success.

DGS-3627:5#
```

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. The beginning and end of the port list range are separated by a dash.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To add multicast MAC forwarding:

```
DGS-3627:5#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-3627:5#
```

config fdb aging_time

Purpose	Used to set the aging time of the forwarding database.
Syntax	config fdb aging_time <sec 10-1000000>
Description	The aging time affects the learning process of the Switch. Dynamic forwarding table entries, which are made up of the source MAC addresses and their associated port numbers, are deleted from the table if they are not accessed within the aging time. The aging time can be from 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-level and operator-level users can issue this command.

Example usage:

To set the FDB aging time:

```
DGS-3627:5#config fdb aging_time 300
Command: config fdb aging_time 300

Success.

DGS-3627:5#
```

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-level and operator-level users can issue this command.

Example usage:

To delete a permanent FDB entry:

```
DGS-3627:5#delete fdb default 00-00-00-00-01-02
Command: delete fdb default 00-00-00-00-01-02

Success.

DGS-3627:5#
```

Example usage:

To delete a multicast FDB entry:

```
DGS-3627:5#delete fdb default 01-00-00-00-01-02
Command: delete fdb default 01-00-00-00-01-02

Success.

DGS-3627:5#
```

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	<p><vlan_name 32> – The name of the VLAN on which the MAC address resides.</p> <p>port <port> – The port number corresponding to the MAC destination address. The Switch will always forward traffic to the specified device through this port.</p> <p>all – Clears all dynamic entries to the Switch's forwarding database.</p>
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To clear all FDB dynamic entries:

```
DGS-3627:5#clear fdb all
Command: clear fdb all

Success.

DGS-3627:5#
```

show multicast_fdb

Purpose	Used to display the contents of the Switch's multicast forwarding database.
Syntax	show multicast_fdb {[vlan <vlan_name 32> vlanid <vidlist>]} mac_address <macaddr>}
Description	This command is used to display the current contents of the Switch's multicast MAC address forwarding database.
Parameters	<p><vlan_name 32> – The name of the VLAN on which the MAC address resides.</p> <p><vlanid> – Displays the entries for the VLANs indicated by the VID list.</p> <p><macaddr> – The MAC address that is present in the forwarding database table.</p>

show multicast_fdb

Restrictions None.

Example usage:

To display multicast MAC address table:

DGS-3627:5#show multicast_fdb vlan default**Command: show multicast_fdb vlan default**

VLAN Name : default
MAC Address : 01-00-5E-00-00-00
Egress Ports : 1-5
Mode : Static

Total Entries : 1**DGS-3627:5#****show fdb**

Purpose	Used to display the current unicast MAC address forwarding database.
Syntax	show fdb {port <port> [vlan <vlan_name 32> vlanid <vidlist>]} mac_address <macaddr> static aging_time}
Description	This command will display the current contents of the Switch's forwarding database.
Parameters	<p><i>port <port></i> – The port number corresponding to the MAC destination address. The Switch will always forward traffic to the specified device through this port.</p> <p><i><vlan_name 32></i> – The name of the VLAN on which the MAC address resides.</p> <p><i><vlanid></i> – Displays the entries for the VLANs indicated by the VID list.</p> <p><i><macaddr></i> – The MAC address that is present in the forwarding database table.</p> <p><i>static</i> – Displays the static MAC address entries.</p> <p><i>aging_time</i> – Displays the aging time for the MAC address forwarding database.</p>
Restrictions	None.

Example usage:

To display unicast MAC address table:

```
DGS-3627:5#show fdb
Command: show fdb

Unicast MAC Address Aging Time = 300

VID  VLAN Name      MAC Address      Port    Type
----  -
1    default          00-00-39-34-66-9A  1      Dynamic
1    default          00-00-51-43-70-00  1      Dynamic
1    default          00-00-5E-00-01-01  1      Dynamic
1    default          00-00-74-60-72-2D  1      Dynamic
1    default          00-00-81-05-00-80  1      Dynamic
1    default          00-00-81-05-02-00  1      Dynamic
1    default          00-00-81-48-70-01  1      Dynamic
1    default          00-00-E2-4F-57-03  1      Dynamic
1    default          00-00-E2-61-53-18  1      Dynamic
1    default          00-00-E2-6B-BC-F6  1      Dynamic
1    default          00-00-E2-7F-6B-53  1      Dynamic
1    default          00-00-E2-82-7D-90  1      Dynamic
1    default          00-00-F8-7C-1C-29  1      Dynamic
1    default          00-01-02-03-04-00  CPU    Self
1    default          00-01-02-03-04-05  1      Dynamic
1    default          00-01-30-10-2C-C7  1      Dynamic
CTRL+C ESC q Quit SPACE n Next Page Enter Next Entry a All
```

show ipfdb

Purpose	Used to display the current network address forwarding database
Syntax	show ipfdb <ipaddr>
Description	The show ipfdb command displays the current network address forwarding database.
Parameters	<ipaddr> - Displays the specified IP address.
Restrictions	None.

Example usage:

To display unicast MAC address table:

```
DGS-3627:5#show ipfdb
Command: show ipfdb

Interface      IP Address      Port    Learned
-----
System        10.1.1.152      1      Dynamic
System        10.2.1.52       1      Dynamic
System        10.1.1.152      1      Dynamic
System        10.51.1.12      1      Dynamic
System        10.12.22.15     1      Dynamic
System        10.57.7.189     1      Dynamic

Total Entries: 6

DGS-3627:5#
```

config multicast filtering_mode

Purpose	Used to configure the multicast packet filtering mode for specific VLANs .
Syntax	config multicast filtering_mode [<vlan_name 32> all]

config multicast filtering_mode

	[forward_all_groups forward_unregistered_groups filter_unregistered_groups]
Description	This command will configure the multicast packet filtering mode for specified VLANs on the Switch.
Parameters	<i><vlan_name 32></i> - Specifies a VLAN by VLAN name to set. If no VLAN is defined here, the rule is applied to all VLANs <i>[forward_all_groups forward_unregistered_groups filter_unregistered_groups]</i> – The user may set the filtering mode to any of these three options.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To configure the multicast filtering mode to filter unregistered groups on all VLANs.

```
DGS-3627:5#config multicast filtering_mode all filter_unregistered_groups
Command: config multicast filtering_mode all filter_unregistered_groups

Success.

DGS-3627:5#
```

show multicast filtering_mode

Purpose	Used to show the multicast packet filtering mode as configured for the VLANs.
Syntax	show multicast filtering_mode {vlan <vlan_name 32>}
Description	This command will display the current multicast packet filtering mode for specified VLANs or all VLANs on the Switch.
Parameters	<i>vlan <vlan_name 32></i> - Specifies a VLAN to display multicast filtering status.
Restrictions	None.

Example usage:

To view the multicast filtering mode for all VLANs:

```
DGS-3627:5#show multicast filtering_mode
Command: show multicast filtering_mode

VLAN Name           Multicast Filter Mode
-----
default             filter_unregistered_groups
v1                  filter_unregistered_groups
v2                  filter_unregistered_groups
v3                  filter_unregistered_groups

DGS-3627:5#
```

BROADCAST STORM 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, the only 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] dlf [enable disable] action [drop shutdown] threshold <value 0-255000> countdown [<value 0> <value 5-30>] time_interval <value 5-30>}
config traffic control_recover	[<portlist> all]
config traffic trap	[none storm_occurred storm_cleared both]
show traffic control	{<portlist>}

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

config traffic control

Purpose	Used to configure broadcast/multicast traffic control.
Syntax	config traffic control [<portlist> all] broadcast [enable disable] multicast [enable disable] dlf [enable disable] action [drop shutdown] threshold <value 0-255000> countdown [<value 0> <value 5-30>] time_interval <value 5-30>}
Description	This command is used to configure traffic control.
Parameters	<p><portlist> – Used to specify a range of ports to be configured for traffic control. The beginning and end of the port list range are separated by a dash.</p> <p><i>all</i> – Specifies all ports are to be configured for traffic control on the Switch.</p> <p><i>broadcast</i> [enable disable] – Enables or disables broadcast storm control.</p> <p><i>multicast</i> [enable disable] – Enables or disables multicast storm control.</p> <p><i>dlf</i> [enable disable] – Enables or disables dlf traffic control.</p> <p><i>action</i> – Used to configure the action taken when a storm control has been detected on the Switch. The user has two options:</p> <ul style="list-style-type: none"> <i>drop</i> - 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. <i>shutdown</i> - Utilizes the Switch's software Traffic Control mechanism to determine the Packet Storm occurring. Once detected, the port will

config traffic control

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/df 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.

- *sec 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. 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.
- *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-level and operator-level users can issue this command.

Example usage:

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

```
DGS-3627:5#config traffic control all broadcast enable
Command: config traffic control all broadcast enable
```

```
Success.
```

```
DGS-3627:5#
```

config traffic control_recover

Purpose	Used to configure traffic control recover for any or all ports.
Syntax	config traffic control_recover [<portlist> all]
Description	Configuring a port for traffic control recover will require an administrator to restart the specified ports if storm control shuts down the port or ports. That is, if a storm triggers the action <i>shutdown</i> for a port, it will remain in the shutdown even if the threshold falls below the value that triggers the storm control action.
Parameters	<portlist> - Used to specify a range of ports. The beginning and end of the port list range are separated by a dash. <i>all</i> – All ports on the Switch.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To configure traffic control recover:

```
DGS-3627:5#config traffic control_recover 1-6
Command: config traffic control_recover 1-6

Success.

DGS-3627:5#
```

config traffic trap

Purpose	Used to configure traps for traffic control.
Syntax	config traffic trap [none storm_occurred storm_cleared both]
Description	Use this to enable traffic storm trap messages.
Parameters	<i>none</i> – Will send no Storm trap warning messages regardless of action taken by the Traffic Control mechanism. <i>storm_occurred</i> – Will send Storm Trap warning messages upon the occurrence of a Traffic Storm only. <i>storm_cleared</i> – Will send Storm Trap messages when a Traffic Storm has been cleared by the Switch only. <i>both</i> – Will send Storm Trap messages when a Traffic Storm has been both detected and cleared by the Switch.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

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

```
DGS-3627:5#config traffic trap storm_occurred
Command: config traffic trap storm_occurred

Success.

DGS-3627:5#
```

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> - Specify a range of ports to display. The beginning and end of the port list range are separated by a dash
Restrictions	None.

Example usage:

To display traffic control setting:

```
DGS-3627:5#show traffic control
Command: show traffic control

Traffic Storm Control Trap :[None]

Port   Thres  Broadcast  Multicast  Unicast  Action  Count  Time  Shutdown
-----  ---  -----  -----  -----  -----  ----  ----  -----
1      131072  Enabled    Disabled   Disabled drop     0      5
2      131072  Enabled    Disabled   Disabled drop     0      5
3      131072  Enabled    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
13     131072  Disabled   Disabled   Disabled drop     0      5
14     131072  Disabled   Disabled   Disabled drop     0      5
15     131072  Disabled   Disabled   Disabled drop     0      5
16     131072  Disabled   Disabled   Disabled drop     0      5
CTRL+C ESC q Quit SPACE n Next Page Enter Next Entry a All

DGS-3627:5#
```

QoS COMMANDS

The Switch supports 802.1p priority queuing. The Switch has seven configurable priority queues. These priority queues are numbered from 6 (Class 6) — 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 Q6 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, 6, 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.



NOTICE: The Switch contains eight classes of service for each port on the Switch. One of these classes is reserved for internal use on the Switch and therefore is not configurable. All references in the following section regarding classes of service will refer to only the seven classes of service that may be used and configured by the Switch's Administrator.

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 1-156249>] tx_rate [no_limit <value 1-156249>]}
show bandwidth_control	{<portlist>}
config scheduling	<class_id 0-6> {max_packet <value 0-15>}
show scheduling	
config 802.1p user_priority	<priority 0-7> <class_id 0-6>
show 802.1p user_priority	
config 802.1p default_priority	[<portlist> all] <priority 0-7>
show 802.1p default_priority	{<portlist>}
config scheduling_mechanism	[strict weight_fair]
show scheduling_mechanism	
enable hol_prevention	
disable hol_prevention	
show hol_prevention	

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	[<portlist> all] {rx_rate [no_limit <value 1-156249>] tx_rate [no_limit <value 1-156249>]}
Description	The config bandwidth_control command is used to configure bandwidth on a port by-port basis.
Parameters	<p><i><portlist></i> – Specifies a port or range of ports to be configured. The beginning and end of the port list range are separated by a dash.</p> <p><i>all</i> – Specifies that the command applies to all ports on the Switch.</p> <p><i>rx_rate</i> – Specifies that one of the parameters below (<i>no_limit</i> or <i><value 1-156249></i>) will be applied to the rate at which the above specified ports will be allowed to receive packets</p> <ul style="list-style-type: none"> ▪ <i>no_limit</i> – Specifies that there will be no limit on the rate of packets received by the above specified ports. ▪ <i><value 1-156249></i> – Specifies the packet limit, in Kbps, that the above ports will be allowed to receive. <p><i>tx_rate</i> – Specifies that one of the parameters below (<i>no_limit</i> or <i><value 1-156249></i>) will be applied to the rate at which the above specified ports will be allowed to transmit packets.</p> <ul style="list-style-type: none"> ▪ <i>no_limit</i> – Specifies that there will be no limit on the rate of packets received by the above specified ports. ▪ <i><value 1-156249></i> – Specifies the packet limit, in Kbps, that the above ports will be allowed to receive.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To configure bandwidth control:

```
DGS-3627:5#config bandwidth_control 1-8 rx_rate 64 tx_rate 64
Command: config bandwidth_control 1-8 rx_rate 64 tx_rate 64

Success.

DGS-3627:5#
```

show bandwidth_control

Purpose	Used to display the bandwidth control table.
Syntax	show bandwidth_control {<portlist>}
Description	The show bandwidth_control command displays the current bandwidth control configuration on the Switch, on a port-by-port basis.
Parameters	<i><portlist></i> – Specifies a port or range of ports to be viewed. The beginning and end of the port list range are separated by a dash.
Restrictions	None.

Example usage:

To display bandwidth control settings:

```
DGS-3627:5#show bandwidth_control 1-10
Command: show bandwidth_control 1-10

Bandwidth Control Table
```

Port	RX Rate (64Kbit/sec)	TX_Rate (64Kbit/sec)
1	no_limit	10
2	no_limit	10
3	no_limit	10
4	no_limit	10
5	no_limit	10
6	no_limit	10
7	no_limit	10
8	no_limit	10
9	no_limit	10
10	no_limit	10

DGS-3627:5#

config scheduling

Purpose	Used to configure the traffic scheduling mechanism for each COS queue.
Syntax	config scheduling <class_id 0-6> {max_packet <value 0-15>}
Description	<p>The Switch contains seven hardware priority queues. Incoming packets must be mapped to one of these seven 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 the <i>max_packet</i> set to 0) is to empty the hardware priority queues in order – from the highest priority queue (hardware queue 6) 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.</p> <p>The <i>max_packets</i> parameter allows users 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 0 and 15 can be specified. For example, if a value of 3 is specified, then the highest hardware priority queue (queue 6) will be allowed to transmit three packets – then the next lowest hardware priority queue (number 5) will be allowed to transmit three packets, and so on, until all of the queues have transmitted three packets. The process will then repeat.</p> <p>Entering a 0 into the <value 0-15> field of the <i>max_packet</i> parameter allows for the creation of a Combination Queue for the forwarding of packets. This Combination Queue allows for a combination of strict and weight-fair (weighted round-robin “WRR”) scheduling. Priority classes that have a 0 in the <i>max_packet</i> field will forward packets with strict priority scheduling. The remaining classes, that do not have a 0 in their <i>max_packet</i> field, will follow a weighted round-robin (WRR) method of forwarding packets — as long as the priority classes with a 0 in their <i>max_packet</i> field are empty. When a packet arrives in a priority class with a 0 in its <i>max_packet</i> field, this class will automatically begin forwarding packets until it is empty. Once a priority class with a 0 in its <i>max_packet</i> field is empty, the remaining priority classes will reset the weighted round-robin (WRR) cycle of forwarding packets, starting with the highest available priority class. Priority classes with an equal level of priority and equal entries in their <i>max_packet</i> field will empty their fields based on hardware priority scheduling.</p>
Parameters	<p><class_id 0-6> – This specifies to which of the seven hardware priority queues the config scheduling command will apply. The seven hardware priority queues are identified by number, from 0 to 6, with the 0 queue being the lowest priority.</p> <p><i>max_packet</i> <value 0-15> – Specifies the maximum number of packets the above specified hardware priority queue will be allowed to transmit before allowing the next lowest priority queue to transmit its packets. A value between 0 and 15 can be specified.</p>

config scheduling

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

Example usage:

To configure the traffic scheduling mechanism for each queue:

```
DGS-3627:5# config scheduling 0 max_packet 12
Command: config scheduling 0 max_packet 12

Success.

DGS-3627:5#
```

show scheduling

Purpose	Used to display the currently configured traffic scheduling on the Switch.
Syntax	show scheduling
Description	The show scheduling command will display the current traffic scheduling mechanisms in use on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display the current scheduling configuration:

```
DGS-3627:5#show scheduling
Command: show scheduling

QOS Output Scheduling

Class ID      MAX. Packets
-----
Class-0      1
Class-1      2
Class-2      3
Class-3      4
Class-4      5
Class-5      6
Class-6      7

DGS-3627:5#
```

config 802.1p user_priority

Purpose	Used to map the 802.1p user priority of an incoming packet to one of the seven hardware queues available on the Switch.	
Syntax	config 802.1p user_priority <priority 0-7> <class_id 0-6>	
Description	This command allows users to configure the method that the Switch will map an incoming packet, based on its 802.1p user priority, to one of the seven 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

config 802.1p user_priority

2	1	Lowest
3	3	Mid-low
4	4	Mid-high
5	5	Mid-high
6	6	Highest
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 to go to the `<class_id 0-6>` (the number of the hardware queue).

`<priority 0-7>` – The 802.1p user priority to associate with the `<class_id 0-6>` (the number of the hardware queue).

`<class_id 0-6>` – The number of the Switch's hardware priority queue. The Switch has seven hardware priority queues available. They are numbered between 0 (the lowest priority) and 6 (the highest priority).

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

Example usage:

To configure 802.1 user priority on the Switch:

```
DGS-3627:5#config 802.1p user_priority 1 6
Command: config 802.1p user_priority 1 6

Success.

DGS-3627:5#
```

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 seven hardware priority queues.
Syntax	show 802.1p user_priority
Description	The show 802.1p user_priority command displays the current mapping of an incoming packet's 802.1p priority value to one of the Switch's seven hardware priority queues.
Parameters	None.
Restrictions	None.

Example usage:

To show 802.1p user priority:

```
DGS-3627:5#show 802.1p user_priority
Command: show 802.1p user_priority

QOS Class of Traffic

Priority-0 -> <Class-2>
Priority-1 -> <Class-0>
Priority-2 -> <Class-1>
Priority-3 -> <Class-3>
Priority-4 -> <Class-4>
Priority-5 -> <Class-5>
Priority-6 -> <Class-6>
```

```
Priority-7 -> <Class-6>
```

```
DGS-3627:5#
```

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 users to specify default priority handling of untagged packets received by the Switch. The priority value entered with this command will be used to determine to which of the seven hardware priority queues the packet is forwarded.
Parameters	<p><i><portlist></i> – Specifies a port or range of ports to be configured. The beginning and end of the port list range are separated by a dash.</p> <p><i>all</i> – Specifies that the command applies to all ports on the Switch.</p> <p><i><priority 0-7></i> – The priority value to assign to untagged packets received by the Switch or a range of ports on the Switch.</p>
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To configure 802.1p default priority on the Switch:

```
DGS-3627:5#config 802.1p default_priority all 5
Command: config 802.1p default_priority all 5
```

```
Success.
```

```
DGS-3627:5#
```

show 802.1p 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	The show 802.1p default_priority command displays the currently configured 802.1p priority value that will be assigned to an incoming, untagged packet before being forwarded to its destination.
Parameters	<i><portlist></i> – Specifies a port or range of ports for which to display the default-priority. The beginning and end of the port list range are separated by a dash.
Restrictions	None.

Example usage:

To display the current 802.1p default priority configuration on the Switch:

```
DGS-3627:5# show 802.1p default_priority
Command: show 802.1p default_priority
```

```
Port   Priority
-----
```

1	0
2	0
3	0
4	0
5	0
6	0
7	0
8	0
9	0
10	0
11	0
12	0
13	0
14	0
15	0
16	0
17	0
18	0
19	0
20	0
CTRL+C ESC q Quit SPACE n Next Page Enter Next Entry a All	

config scheduling_mechanism

Purpose	Used to configure the scheduling mechanism for the QoS function
Syntax	config scheduling_mechanism [strict weight_fair]
Description	<p>The config scheduling_mechanism command allows the user to select between a weight fair (WRR) and a Strict mechanism for emptying the priority classes of service of the QoS function. The Switch contains seven hardware priority classes of service. Incoming packets must be mapped to one of these seven hardware priority classes of service. This command is used to specify the rotation by which these seven hardware priority classes of service are emptied.</p> <p>The Switch's default is to empty the seven priority classes of service in order – from the highest priority class of service (queue 6) to the lowest priority class of service (queue 0). Each queue will transmit all of the packets in its buffer before allowing the next lower priority class of service to transmit its packets. Lower classes of service will be pre-empted from emptying its queue if a packet is received on a higher class of service. The packet that was received on the higher class of service will transmit its packet before allowing the lower class to resume clearing its queue.</p>
Parameters	<p><i>strict</i> – Entering the strict parameter indicates that the highest class of service is the first to be processed. That is, the highest class of service should finish emptying before the others begin.</p> <p><i>weight_fair</i> – Entering the weight fair parameter indicates that the priority classes of service will empty packets in a weighted round-robin (WRR) order. That is to say that they will be emptied in an even distribution.</p>
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To configure the traffic scheduling mechanism for each CoS queue:

```
DGS-3627:5#config scheduling_mechanism strict
Command: config scheduling_mechanism strict
Success.
```

DGS-3627:5#

show scheduling_mechanism

Purpose	Used to display the current traffic scheduling mechanisms in use on the Switch.
Syntax	show scheduling_mechanism
Description	This command will display the current traffic scheduling mechanisms in use on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To show the scheduling mechanism:

```
DGS-3627:5#show scheduling_mechanism
Command: show scheduling_mechanism

QOS scheduling_mechanism
CLASS ID Mechanism
-----
Class-0  strict
Class-1  strict
Class-2  strict
Class-3  strict
Class-4  strict
Class-5  strict
Class-6  strict

DGS-3627:5#
```

enable hol_prevention

Purpose	Used to enable HOL prevention.
Syntax	enable hol_prevention
Description	The enable hol_prevention command enables Head of Line prevention.
Parameters	None.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To enable HOL prevention:

```
DGS-3627:5#enable hol_prevention
Command: enable hol_prevention

Success.

DGS-3627:5#
```

disable hol_prevention

Purpose	Used to disable HOL prevention.
Syntax	disable hol_prevention
Description	The disable hol_prevention command disables Head of Line prevention.
Parameters	None.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To disable HOL prevention:

```
DGS-3627:5#disable hol_prevention
Command: disable hol_prevention

Success.

DGS-3627:5#
```

show hol_prevention

Purpose	Used to show HOL prevention.
Syntax	show hol_prevention
Description	The show hol_prevention command displays the Head of Line prevention state.
Parameters	None.
Restrictions	None.

Example usage:

To view the HOL prevention status:

```
DGS-3627:5#show hol_prevention
Command: show hol_prevention

Device HOL Prevention State: Enabled

DGS-3627:5#
```


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	<p><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.</p> <p>[add delete] – Specify to add or delete ports to be mirrored that are specified in the <i>source ports</i> parameter.</p> <p>source ports – The port or ports being mirrored. This cannot include the Target port.</p> <ul style="list-style-type: none"> <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. The beginning and end of the port list range are separated by a dash. <p>rx – Allows the mirroring of only packets received by (flowing into) the port or ports in the port list.</p> <p>tx – Allows the mirroring of only packets sent to (flowing out of) the port or ports in the port list.</p> <p>both – Mirrors all the packets received or sent by the port or ports in the port list.</p>
Restrictions	The Target port cannot be listed as a source port. Only administrator-level and operator-level users can issue this command.

Example usage:

To add the mirroring ports:

```
DGS-3627:5# config mirror port 1 add source ports 2-7 both
Command: config mirror port 1 add source ports 2-7 both

Success.

DGS-3627:5#
```

Example usage:

To delete the mirroring ports:

```
DGS-3627:5#config mirror port 1 delete source ports 2-4 both
Command: config mirror port 1 delete source ports 2-4 both

Success.

DGS-3627:5#
```

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 users to enter a port mirroring configuration into the Switch, and then turn the port mirroring on and off without having to modify the port mirroring configuration.
Parameters	None.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To enable mirroring configurations:

```
DGS-3627:5#enable mirror
Command: enable mirror

Success.

DGS-3627:5#
```

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 users to enter a port mirroring configuration into the Switch, and then turn the port mirroring on and off without having to modify the port mirroring configuration.
Parameters	None.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To disable mirroring configurations:

```
DGS-3627:5#disable mirror
Command: disable mirror

Success.

DGS-3627:5#
```

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-3627:5#show mirror
Command: show mirror

Current Settings
Mirror Status : Enabled
Target Port   : 1
Mirrored Port
              RX :
              TX : 5-7

DGS-3627:5#
```

VLAN COMMANDS

Along with normal VLAN configurations, this Switch now incorporate Double VLANs. Better known as Q-IN-Q VLANs, Double VLANs allow network providers to expand their VLAN configurations to place VLANs within a larger inclusive VLAN, which adds a new layer to the VLAN configuration. This basically lets large ISP's create L2 Virtual Private Networks and also create transparent LANs for their customers, which will connect two or more customer LAN points without over complicating configurations on the client's side. Not only will over-complication be avoided, but now the administrator has over 4000 VLANs in which over 4000 VLANs can be placed, therefore greatly expanding the VLAN network.

Implementation of this feature adds a VLAN frame to an existing VLAN frame for the ISP VLAN recognition and classification. To ensure devices notice this added VLAN frame, an Ethernet encapsulation, here known as a tpid, is also added to the frame. The device recognizes this tpid and therefore checks the VLAN tagged packet to see if a provider VLAN tag has been added. If so, the packet is then routed through this provider VLAN, which contains smaller VLANs with similar configurations to ensure speedy and guaranteed routing destination of the packet.

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}
delete vlan	<vlan_name 32>
config vlan	<vlan_name 32> {[add [tagged untagged forbidden] <portlist> advertisement [enable disable]}
config vlan	<vlan_name 32> delete <portlist>
config gvrp	[<portlist> all] {state [enable disable] ingress_checking [enable disable] acceptable_frame [tagged_only admit_all] pvid <vlanid 1-4094>}
enable gvrp	
disable gvrp	
show vlan	{[<vlan_name 32> vlanid <vidlist>] ports <portlist>}
show gvrp	{<portlist>}
enable double_vlan	
disable double_vlan	
create double_vlan	<vlan_name 32> spvid <vlanid 1-4094> {tpid <hex 0x0-0xffff>}
config double_vlan	<vlan_name> {[add [access uplink] delete] <portlist> tpid <hex 0x0-0xffff>}
delete double_vlan	<vlan_name>
show double_vlan	{<vlan_name>}
enable pvid auto_assign	
disable pvid auto_assign	
show pvid auto_assign	

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 creation of a VLAN on the Switch.

create vlan

Parameters	<p><i><vlan_name 32></i> – The name of the VLAN to be created.</p> <p><i>tag <vlanid 2-4094></i> – The VLAN ID of the VLAN to be created. Allowed values = 2-4094</p> <p><i>type</i> – This parameter uses the <i>type</i> field of the packet header to determine the packet protocol and destination VLAN:</p> <p><i>1q_vlan</i> – Allows the creation of a normal 802.1Q VLAN on the Switch.</p> <p><i>advertisement</i> – Specifies that the VLAN is able to join GVRP.</p>
Restrictions	Each VLAN name can be up to 32 characters. Only administrator-level and operator-level users can issue this command.

Example usage:

To create a VLAN v1, tag 2:

```
DGS-3627:5#create vlan v1 tag 2
Command: create vlan v1 tag 2

Success.

DGS-3627:5#
```

delete vlan

Purpose	Used to delete a previously configured VLAN on the Switch.
Syntax	delete vlan <vlan_name 32>
Description	This command will delete a previously configured VLAN on the Switch.
Parameters	<i><vlan_name 32></i> – The VLAN name of the VLAN to delete.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To remove the VLAN “v1”:

```
DGS-3627:5#delete vlan v1
Command: delete vlan v1

Success.

DGS-3627:5#
```

config vlan add

Purpose	Used to add additional ports to a previously configured VLAN.
Syntax	config vlan <vlan_name 32> {[add [tagged untagged forbidden] <portlist> advertisement [enable disable]}
Description	This command is used to add ports to the port list of a previously configured VLAN. Additional ports may be specified as tagging, untagging, or forbidden. The default is to assign the ports as untagging.
Parameters	<p><i><vlan_name 32></i> – The name of the VLAN to add or delete ports to.</p> <p><i>add</i> – Specifies which ports to add. The user may also specify if the ports are:</p> <ul style="list-style-type: none"> • <i>tagged</i> – Specifies the additional ports as tagged. • <i>untagged</i> – Specifies the additional ports as untagged. • <i>forbidden</i> – Specifies the additional ports as forbidden. <p><i><portlist></i> – A port or range of ports to add to the VLAN. The beginning and end of the port list range are separated by a dash.</p> <p><i>advertisement [enable disable]</i> – Enables or disables GVRP on the specified VLAN.</p>
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

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

```
DGS-3627:5#config vlan v1 add tagged 4-8
Command: config vlan v1 add tagged 4-8

Success.

DGS-3627:5#
```

config vlan delete

Purpose	Used to delete ports from a previously configured VLAN.
Syntax	config vlan <vlan_name 32> delete <portlist>
Description	This command is used to delete ports from the port list of a previously configured VLAN.
Parameters	<p><i><vlan_name 32></i> – The name of the VLAN from which to delete ports.</p> <p><i><portlist></i> – A port or range of ports to delete from the VLAN. The beginning and end of the port list range are separated by a dash.</p>
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To delete ports 5-7 of the VLAN v1:

```
DGS-3627:5#config vlan v1 delete 5-7
Command: config vlan v1 delete 5-7

Success.

DGS-3627:5#
```

config gvrp

Purpose	Used to configure GVRP on the Switch.
Syntax	config gvrp [<portlist> all] {state [enable disable] ingress_checking [enable disable] acceptable_frame [tagged_only admit_all] pvid <vlanid 1-4094>}
Description	This command is used to configure the GARP VLAN Registration Protocol on the Switch. Configurable settings include ingress checking, the sending and receiving of GVRP information, and the Port VLAN ID (PVID).
Parameters	<p><portlist> – A port or range of ports for which to configure GVRP. The beginning and end of the port list range are separated by a dash.</p> <p>all – Specifies all of the ports on the Switch.</p> <p>state [enable disable] – Enables or disables GVRP for the ports specified in the port list.</p> <p>ingress_checking [enable disable] – Enables or disables ingress checking for the specified port list.</p> <p>acceptable_frame [tagged_only admit_all] – This parameter states the frame type that will be accepted by the Switch for this function. <i>tagged_only</i> implies that only VLAN tagged frames will be accepted, while <i>admit_all</i> implies tagged and untagged frames will be accepted by the Switch.</p> <p>pvid – Specifies the default VLAN ID associated with the port.</p>
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

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

```
DGS-3627:5#config gvrp 1-4 state enable ingress_checking enable
acceptable_frame tagged_only pvid 2
Command: config gvrp 1-4 state enable ingress_checking enable
acceptable_frame tagged_only pvid 2

Success.

DGS-3627:5#
```



Note: In the current firmware version, the PVID for the ports can either be manually configured by the user or auto assigned when these ports are added to a VLAN as an untagged member.

enable gvrp

Purpose	Used to enable GVRP on the Switch.
Syntax	enable gvrp
Description	This command, along with disable gvrp below, is used to enable and disable GVRP globally on the Switch, without changing the GVRP configuration on the Switch.
Parameters	None.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To enable the generic VLAN Registration Protocol (GVRP):

```
DGS-3627:5#enable gvrp
```

```
Command: enable gvrp
```

```
Success.
```

```
DGS-3627:5#
```

disable gvrp

Purpose	Used to disable GVRP on the Switch.
Syntax	disable gvrp
Description	This command, along with enable gvrp above, is used to enable and disable GVRP on the Switch, without changing the GVRP configuration on the Switch.
Parameters	None.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To disable the Generic VLAN Registration Protocol (GVRP):

```
DGS-3627:5#disable gvrp
```

```
Command: disable gvrp
```

```
Success.
```

```
DGS-3627:5#
```

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	<p><vlan_name 32> – The VLAN name of the VLAN for which to display a summary of settings.</p> <p>vlanid <vidlist> - Users may alternately choose the VLAN to be displayed by entering the VLAN ID.</p> <p>ports <portlist> - Users may also view VLANs by designated port.</p>
Restrictions	None.

Example usage:

To display the Switch's current VLAN settings:

```
DGS-3627:5#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:

Total Entries : 1

DGS-3627:5#
```

show gvrp	
Purpose	Used to display the GVRP status for a port list on the Switch.
Syntax	show gvrp {<portlist>}
Description	This command displays the GVRP status for a port list on the Switch.
Parameters	<i><portlist></i> – Specifies a range of ports for which the GVRP status is to be displayed. The beginning and end of the port list range are separated by a dash. Non-contiguous portlist entries are separated by a comma. (ex: 1-3,7-9)
Restrictions	None.

Example usage:

To display GVRP port status:

```
DGS-3627:5#show gvrp
Command: show gvrp

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
11      1      Disabled  Enabled           All Frames
12      1      Disabled  Enabled           All Frames
13      1      Disabled  Enabled           All Frames
14      1      Disabled  Enabled           All Frames
15      1      Disabled  Enabled           All Frames
16      1      Disabled  Enabled           All Frames
17      1      Disabled  Enabled           All Frames
```

18	1	Disabled	Enabled	All Frames
CTRL+C	ESC	q	Quit	SPACE
		n	Next Page	Enter
		a	Next Entry	All

enable double_vlan

Purpose	Used to enable the Double VLAN feature on the Switch.
Syntax	enable double_vlan
Description	This command, along with the disable double_vlan command, enables and disables the Double Tag VLAN. When Double VLANs are enabled, the system configurations for VLANs will return to the default setting, except IP address, log, user accounts and banner setting, in order to enable the Double VLAN mode. In the Double VLAN mode, normal VLANs and GVRP functions are disabled. The Double VLAN default setting is disabled.
Parameters	None.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To enable the Double VLAN feature on the Switch, thus disabling normal VLANs and GVRP.

```
DGS-3627:5#enable double_vlan
Command: enable double_vlan
Current Double VLAN mode : Disabled
Enable Double VLAN need to reset system config. Are you sure?(y/n)y

Success.

DGS-3627:5#
```

disable double_vlan

Purpose	Used to disable the Double VLAN feature on the Switch.
Syntax	disable double_vlan
Description	This command, along with the enable double_vlan command, enables and disables the Double Tag VLAN. When Double VLANs are enabled, the system configurations for VLANs will return to the default setting, except IP address, log, user accounts, and banner setting, in order to enable the Double VLAN mode. In the Double VLAN mode, normal VLANs and GVRP functions are disabled. The Double VLAN default setting is disabled.
Parameters	None.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To disable the Double VLAN feature on the Switch

```
DGS-3627:5#disable double_vlan
Command: disable double_vlan
Current Double VLAN mode : Enabled
Disable Double VLAN need to reset system config. Are you sure?(y/n)y

Success.

DGS-3627:5#
```

create double_vlan

Purpose	Used to create a Double VLAN on the Switch.
Syntax	create double_vlan <vlan_name 32> spvid <vlanid 1-4094> {tpid <hex 0x0-0xffff>}
Description	This command is used to create a Double VLAN (service provider VLAN) on the Switch.
Parameters	<p><i>vlan <vlan_name 32></i> - The name of the Double VLAN to be created. The user is to enter an alphanumeric string of up to 32 characters to identify this VLAN.</p> <p><i>spvid <vlanid 1-4094></i> - The VLAN ID of the service provider VLAN. The user is to identify this VLAN with a number between 1 and 4094.</p> <p><i>tpid <hex 0x0-0xffff></i> - The tag protocol ID. This ID, identified here in hex form, will help identify packets to devices as Double VLAN tagged packets. The default setting is 0x8100.</p>
Restrictions	Only administrator-level and operator-level users can issue this command. Users must have the Switch enabled for Double VLANs.

```
DGS-3400:4#create double_vlan Drazen spvid 6 tpid 0x9100
Command: create double_vlan Drazen spvid 6 tpid 0x9100

Success.

DGS-3400:4#
```

config double_vlan

Purpose	Used to config the parameters for a previously created Double VLAN on the Switch.
Syntax	config double_vlan <vlan_name> {[[add [access uplink] delete] <portlist> tpid <hex 0x0-0xffff>]}
Description	This command is used to configure a Double VLAN (service provider VLAN) on the Switch.
Parameters	<p><i>vlan <vlan_name 32></i> - The name of the Double VLAN to be configured. The user is to enter an alphanumeric string of up to 32 characters to identify this VLAN.</p> <p><i>add</i> – Specify this parameter to add ports configured in the <i><portlist></i> as one of the two following types of ports.</p> <ul style="list-style-type: none"> <i>uplink</i> – Add this parameter to configure these ports as uplink ports. Uplink ports are for connecting Switch VLANs to the Provider VLANs on a remote source. Only gigabit ports can be configured as uplink ports.

config double_vlan

- *access* - Add this parameter to configure these ports as access ports. Access ports are for connecting Switch VLANs to customer VLANs.
- *portlist* – Enter a list of ports to be added to this VLAN. The beginning and end of the port list range are separated by a dash. Non-contiguous portlist entries are separated by a comma. (ex: 1-3,7-9)

delete - Specify this parameter to delete ports configured in the <portlist> from this VLAN.

- *portlist* – Enter a list of ports to be deleted from this VLAN. The beginning and end of the port list range are separated by a dash. Non-contiguous portlist entries are separated by a comma. (ex: 1-3,7-9)

tpid <hex 0x0-0xffff>- The tag protocol ID. This ID, identified here in hex form, will help identify packets to devices as Double VLAN tagged packets. The default setting is 0x8100.

Restrictions Only administrator-level and operator-level users can issue this command. Users must have the Switch enabled for Double VLANs.

Example usage:

To add ports 4 through 8 as access ports to the Double VLAN “Drazen”:

```
DGS-3627:5#config double_vlan Drazen add access 4-8
Command: config double_vlan Drazen add access 4-8

Success.

DGS-3627:5#
```

Example usage:

To delete ports 4 through 8 on the Double VLAN “Drazen”:

```
DGS-3627:5#config double_vlan Drazen delete 4-8
Command: config double_vlan Drazen delete 4-8

Success.

DGS-3627:5#
```

show double_vlan

Purpose	Used to display the Double VLAN settings on the Switch.
Syntax	show double_vlan {<vlan_name>}
Description	This command will display the current double VLAN parameters configured on the Switch.
Parameters	<i>vlan_name</i> - Enter the name of a previously created VLAN for which to display the settings.
Restrictions	None.

Example usage:

To display parameters for the Double VLAN “Drazen”:

```
DGS-3627:5#show double_vlan Drazen
```

```
Command: show double_vlan Drazen
```

```
Global Double VLAN : Enabled
```

```
=====
SPVID       : 6
VLAN Name   : Drazen
TPID        : 0x9200
Uplink Ports :
Access Ports : 4-8
Unknow Ports :
```

```
-----
Total Entries : 1
```

```
DGS-3627:5#
```

enable pvid auto_assign

Purpose	Used to enable auto assignment of PVID.
Syntax	enable pvid auto_assign
Description	If "Auto-assign PVID" is enabled, PVID will be possibly changed by PVID or VLAN configuration. When a user configures a port to VLAN X's untagged membership, this port's PVID will be updated with VLAN X. In the form of VLAN list command, PVID is updated with the last item of the VLAN list. When a user removes a port from the untagged membership of the PVID's VLAN, the port's PVID will be assigned with "default VLAN". The default setting is enabled.
Parameters	None.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To enable the auto-assign PVID:

```
DGS-3627:5#enable pvid auto_assign
```

```
Command: enable pvid auto_assign
```

```
Success.
```

```
DGS-3627:5#
```

disable pvid auto_assign

Purpose	Used to disable auto assignment of PVID.
Syntax	disable pvid auto_assign
Description	If "auto-assign PVID" is disabled, PVID can only be changed by PVID configuration (user changes explicitly). The VLAN configuration will not automatically change PVID. The default setting is enabled.
Parameters	None.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To disable the auto-assign PVID:

```
DGS-3627:5#disable pvid auto_assign
Command: disable pvid auto_assign

Success.

DGS-3627:5#
```

show pvid auto_assign

Purpose	Used to display the PVID auto-assign status.
Syntax	show pvid auto_assign
Description	The show pvid auto_assign command displays the PVID auto assignment state.
Parameters	None.
Restrictions	None.

Example usage:

To display the PVID auto assignment state:

```
DGS-3627:5#show pvid auto_assign
Command: show pvid auto_assign

PVID Auto-assignment: Enabled

DGS-3627:5#
```

PROTOCOL VLAN GROUP COMMANDS

For bridges that implement Port-and-Protocol-based VLAN classification, the VID associated with an Untagged or Priority-tagged Frame is determined based on the Port of arrival of the frame into the bridge and on the protocol identifier of the frame. If there is no protocol VLAN configured on the ingress port, all the untagged packets incoming on the port will be classified into PVID VLAN. This classification mechanism requires defining the protocol groups which specified frame type and protocol value to match for. A protocol group can be bound to a port and given a VLAN ID. If the incoming untagged packet matches the protocol group the VLAN ID will be assigned. A port can bind with multiple protocol groups. This allows untagged packets be classified into different VLANs based on packet content. The same protocol group can be assigned to multiple ports with different VLAN ID assigned, i.e. the same protocol can be given different VLAN ID through binding to different ports.

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

Command	Parameter
create dot1v_protocol_group	group_id <id>
config dot1v_protocol_group	group_id <id> [add delete] protocol [ethernet_2 ieee802.3_snap ieee802.3_llc] <protocol_value>
delete dot1v_protocol_group	group_id <id>
show dot1v_protocol_group	{group_id <id>}
config port dot1v	ports [<portlist> all] [add protocol_group group_id <id> vlan <vlan_name 32> delete protocol_group [group_id <id> all]]
show port dot1v	{ports <portlist>}

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

create dot1v_protocol_group

Purpose	Used to create a protocol group.
Syntax	create dot1v_protocol_group group_id <id>
Description	This command will create a protocol group. This group is to be configured using the config dot1v_protocol_group command where users may set the parameters for this group. After being configured, this group may be attached to a port or range of ports using the config port dot1v command.
Parameters	<i>group_id <id></i> - Enter an integer from 1 to 16 to identify the protocol VLAN group being created here.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To create a protocol group:

```
DGS-3627:5#create dot1v_protocol_group group_id 1
Command: create dot1v_protocol_group group_id 1

Success.

DGS-3627:5#
```

config dot1v_protocol_group

Purpose	Used to configure the parameters for a protocol VLAN group.
Syntax	config dot1v_protocol_group group_id <id> [add delete] protocol [ethernet_2 ieee802.3_snap ieee802.3_llc] <protocol_value>
Description	This command will configure a protocol template for a group. Users may set the frame type to be added or deleted, along with the appropriate <i>protocol_value</i> in hexadecimal form. After being configured, this group may be attached to a port or range of ports using the config port dot1v command.
Parameters	<p><i>group_id <id></i> - Enter an integer from 1 to 16 to identify the protocol VLAN group being configured here.</p> <p><i>add delete</i> - Choose whether to add or delete the protocol to this group. This protocol is identified using the following <i>protocol</i> parameter.</p> <p><i>protocol</i> - Choose the appropriate frame type to be added to this group. This frame type will be identified by the switch by examining the packet header of incoming packets and matching it to the <i>protocol_value</i> stated here. This frame type must be followed by the correct <i>protocol_value</i>. The user has three choices:</p> <ul style="list-style-type: none"> • <i>ethernet_2</i> - Choose this parameter if you wish this protocol group to employ the Ethernet2 frame type. This frame type is identified by the 16-bit (2 octet) IEEE802.3 type field in the packet header, which is to be stated using the following <i>protocol_value</i>. • <i>ieee802.3_snap</i> - Choose this parameter if you wish this protocol group to employ the Sub Network Access Protocol (SNAP) frame type. This frame type is identified by the 16-bit (2 octet) IEEE802.3 type field in the packet header, which is to be stated using the following <i>protocol_value</i>. • <i>ieee802.3_llc</i> - Choose this parameter if you wish this protocol group to employ the Link Logical Control (LLC) frame type. This frame type is identified by the 2-octet IEEE802.3 Link Service Access Point (LSAP) pair field in the packet header, which is to be stated using the following <i>protocol_value</i>. The first octet defines the Destination Service Access Point value and the second octet is the Source Service Access Point (SSAP) value. <p><i><protocol_value></i> - Enter the corresponding protocol value of the protocol identified in the previous field. This value must be stated in a hexadecimal form.</p>
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To configure a protocol template:

```
DGS-3627:5#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-3627:5#
```


delete dot1v_protocol_group

Purpose	Used to delete a protocol VLAN group.
Syntax	delete dot1v_protocol_group group_id <id>
Description	This command will delete a protocol VLAN group.
Parameters	<i>group_id <id></i> - Enter an integer from 1 to 16 to identify the protocol VLAN group being deleted here.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To delete a protocol VLAN group:

```
DGS-3627:5#delete dot1v_protocol_group group_id 1
Command: delete dot1v_protocol_group group_id 1

Success.

DGS-3627:5#
```

show dot1v_protocol_group

Purpose	Used to display the configurations for a protocol VLAN group.
Syntax	show dot1v_protocol_group {group_id <id>}
Description	This command will display the configurations of a protocol VLAN group.
Parameters	<i>group_id <id></i> - Enter an integer from 1 to 16 to identify the protocol VLAN group to be displayed. Entering this command without the group_id parameter will display the configurations for all configured protocol VLAN groups.
Restrictions	None.

Example usage:

To display the configurations for a protocol VLAN group:

```
DGS-3627:5#show dot1v_protocol_group group_id 1
Command: show dot1v_protocol_group group_id 1

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

Total Entries: 1

DGS-3627:5#
```

config port dot1v

Purpose	Used to bind a VLAN with a protocol template on one or more ports.
Syntax	config port dot1v ports [<portlist> all] [add protocol_group group_id <id> vlan vlan_name <vlan_name 32> delete protocol_group [group_id <id> all]]
Description	This command will bind a VLAN with a protocol template on one or more ports. When an ingress untagged packet is identified by the <i>protocol_value</i> stated using the config dot1v_protocol_group command, the switch will assign a pre-configured VLAN and a priority for these ingress untagged packets in order to properly reach their destination.
Parameters	<p><i>ports</i> – Use this parameter to specify ports.</p> <ul style="list-style-type: none"> • <i><portlist></i> - Use this parameter to assign a port or group of ports. • <i>all</i> – Use this parameter to specify all ports on the system. <p><i>add protocol_group group_id <id></i> - Enter an integer from 1 to 16 to identify the protocol VLAN group being assigned to the ports or range of ports configured in the previous field.</p> <p><i>vlan</i> – Use this parameter bind a VLAN with a specific protocol template using either of the following parameters:</p> <ul style="list-style-type: none"> • <i>vlan_name 32</i> – Identify the VLAN name for which to add a tag to ingress untagged packets. <p><i>delete protocol_group</i> – Use this parameter to remove this protocol VLAN group's association with the ports stated in this command, by using the following parameters:</p> <ul style="list-style-type: none"> • <i>group_id <id></i> - Enter this parameter with its corresponding group number, to remove this pre-defined protocol group from the ports specified here. • <i>all</i> – Use this parameter to remove all protocol VLAN groups from the ports specified in this command.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To bind a VLAN with a protocol template:

```
DGS-3627:5#config port dot1v ports 6-8 add protocol_group group_id 1 vlan vlan_name
building1
Command: config port dot1v ports 6-8 add protocol_group group_id 1 vlan vlan_name
building1
```

```
Success.
```

```
DGS-3627:5#
```

show port dot1v

Purpose	Used to display the bound protocol template on a specific port or ports.
Syntax	show port dot1v {ports <portlist>}
Description	This command will display the protocol VLAN group and VLAN for individual ports.
Parameters	<i>ports <portlist></i> - Enter the port or group of ports for which to display the protocol VLAN group settings. Entering this command without this parameter will display all ports and their corresponding protocol VLAN group settings.
Restrictions	None..

Example usage:

To configure the ports for a protocol VLAN group:

```

DGS-3627:5#show port dot1v ports 6-8
Command: show port dot1v ports 6-8

Port: 6
Protocol Group ID      VLAN Name
-----
1                      building1

Port: 7
Protocol Group ID      VLAN Name
-----
1                      building1

Port: 8
Protocol Group ID      VLAN Name
-----
1                      building1

Total Entries: 3

DGS-3627:5#

```

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 1-32> {type [lacp static]}
delete link_aggregation group_id	<value 1-32>
config link_aggregation group_id	<value 1-32> {master_port <port> ports <portlist> state [enable disable]}
config link_aggregation algorithm	[mac_source mac_destination mac_source_dest ip_source ip_destination ip_source_dest]
show link_aggregation	{group_id <value 1-32> 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 1-32> {type [lacp static]}
Description	This command will create a link aggregation group with a unique identifier.
Parameters	<p><value> – Specifies the group ID. The Switch allows up to 32 link aggregation groups to be configured. The group number identifies each of the groups.</p> <p>type – Specify the type of link aggregation used for the group. If the type is not specified the default type is <i>static</i>.</p> <ul style="list-style-type: none"> <i>lacp</i> – 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. <i>static</i> – 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.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To create a link aggregation group:

```
DGS-3627:5#create link_aggregation group_id 1
Command: create link_aggregation group_id 1

Success.

DGS-3627:5#
```

delete link_aggregation group_id

Purpose	Used to delete a previously created link aggregation group.
Syntax	delete link_aggregation group_id <value 1-32>
Description	This command is used to delete a previously configured link aggregation group.
Parameters	<i><value 1-32></i> – Specifies the group ID. The Switch allows up to 32 link aggregation groups to be configured. The group number identifies each of the groups.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To delete link aggregation group:

```
DGS-3627:5#delete link_aggregation group_id 6
Command: delete link_aggregation group_id 6

Success.

DGS-3627:5#
```

config link_aggregation

Purpose	Used to configure a previously created link aggregation group.
Syntax	config link_aggregation group_id <value 1-32> {master_port <port> ports <portlist> state [enable disable]}
Description	This command allows users to configure a link aggregation group that was created with the create link_aggregation command above.
Parameters	<i>group_id <value 32></i> – Specifies the group ID. The Switch allows up to 32 link aggregation groups to be configured. The group number identifies each of the groups. <i>master_port <port></i> – 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. <i>ports <portlist></i> – Specifies a port or range of ports that will belong to the link aggregation group including the master port. The beginning and end of the port list range are separated by a dash. Non-contiguous portlist entries are separated by a comma. (ex: 1-3,7-9) <i>state [enable disable]</i> – Allows users to enable or disable the specified link aggregation group.
Restrictions	Only administrator-level 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 plus port 9:

```
DGS-3627:5#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-3627:5#
```

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	<p><i>mac_source</i> – Indicates that the Switch should examine the source MAC address.</p> <p><i>mac_destination</i> – Indicates that the Switch should examine the destination MAC address.</p> <p><i>mac_source_dest</i> – Indicates that the Switch should examine the source and destination MAC addresses</p> <p><i>ip_source</i> – Indicates that the Switch should examine the source IP address.</p> <p><i>ip_destination</i> – Indicates that the Switch should examine the destination IP address.</p> <p><i>ip_source_dest</i> – Indicates that the Switch should examine the source and the destination IP address.</p>
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To configure link aggregation algorithm for mac-source-dest:

```
DGS-3627:5#config link_aggregation algorithm mac_source_dest
Command: config link_aggregation algorithm mac_source_dest

Success.

DGS-3627:5#
```

show link_aggregation

Purpose	Used to display the current link aggregation configuration on the Switch.
Syntax	show link_aggregation {group_id <value 1-32> algorithm}
Description	This command will display the current link aggregation configuration of the Switch.
Parameters	<p><i><value 1-32></i> – Specifies the group ID. The Switch allows up to 32 link aggregation groups to be configured. The group number identifies each of the groups.</p> <p><i>algorithm</i> – Allows you to specify the display of link aggregation by the algorithm in use by that group.</p>
Restrictions	None.

Example usage:

To display Link Aggregation configuration:

```
DGS-3627:5#show link_aggregation
Command: show link_aggregation

Link Aggregation Algorithm = MAC-source-dest
```

```

Group ID      : 1
Type         : TRUNK
Master Port   : 8
Member Port   : 8,9,10
Active Port   :
Status       : Disabled
Flooding Port : 8

```

```
DGS-3627:5#
```

config lacp_ports

Purpose	Used to configure settings for LACP compliant ports.
Syntax	config lacp_ports <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	<p><i><portlist></i> – Specifies a port or range of ports to be configured. The beginning and end of the port list range are separated by a dash. Non-contiguous portlist entries are separated by a comma. (ex: 1-3,7-9)</p> <p><i>mode</i> – Select the mode to determine if LACP ports will process LACP control frames.</p> <ul style="list-style-type: none"> <i>active</i> – 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. <i>passive</i> – 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-level and operator-level users can issue this command.

Example usage:

To configure LACP port mode settings:

```

DGS-3627:5#config lacp_port 1-12 mode active
Command: config lacp_port 1-12 mode active

```

```
Success.
```

```
DGS-3627:5#
```

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	<p><i><portlist></i> - Specifies a port or range of ports to be configured. The beginning and end of the port list range are separated by a dash. Non-contiguous portlist entries are separated by a comma. (ex: 1-3,7-9) If no parameter is specified, the system will display the current LACP status for all ports.</p>

show lacp_port

Restrictions None.

Example usage:

To display LACP port mode settings:

```
DGS-3627:5#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-3627:5#
```


IP-MAC-PORT BINDING (IMPB)

The IP network layer uses a four-byte address. The Ethernet link layer uses a six-byte MAC address. Binding these two address types together allows the transmission of data between the layers. The primary purpose of IP-MAC-Port binding (IMPB) 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 IMPB-enabled port, the system will block the access by dropping its packet. The maximum number of IP-MAC-Port binding entries is dependant on chip capability (e.g. the ARP table size) and storage size of the device. For the DGS-3600 Series, the maximum number of IMPB entries is 500. The creation of authorized users can be manually configured by CLI or Web. The function is port-based, meaning a user can enable or disable the function on the individual port.

ACL Mode

Due to some special cases that have arisen with IP-MAC-Port binding, this Switch has been equipped with a special ACL Mode for IMPB, 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-Port binding Setting screen. All others will be discarded.

To configure the ACL mode, the user must first set up IP-MAC-Port 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-Port binding (IMPB) 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-Port 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-Port 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-Port binding commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameters
create address_binding ip_mac ipaddress	<ipaddr> mac_address <macaddr> {ports [<portlist> all] mode [arp acl]}
config address_binding ip_mac ipaddress	<ipaddr> mac_address <macaddr> {ports [<portlist> all] mode {arp acl}}
config address_binding ip_mac ports	[<portlist> all] state [enable disable]
show address_binding	[ip_mac {[all ipaddress <ipaddr> mac_address <macaddr>}] blocked {[all vlan_name <vlan_name> mac_address <macaddr>}] ports]

Command	Parameters
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>]]
enable address_binding acl_mode	
disable address_binding acl_mode	
enable address_binding trap_log	
disable address_binding trap_log	

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

create address_binding ip_mac ipaddress	
Purpose	Used to create an IP-MAC-Port binding entry.
Syntax	<ipaddr> mac_address <macaddr> {ports [<portlist> all] mode [arp acl]}
Description	This command will create an IP-MAC-Port binding entry.
Parameters	<p><i><ipaddr></i> The IP address of the device where the IP-MAC-Port binding is made.</p> <p><i><macaddr></i> The MAC address of the device where the IP-MAC-Port binding is made.</p> <p><i><portlist></i> - Specifies a port or range of ports to be configured for address binding. The beginning and end of the port list range are separated by a dash. Non-contiguous portlist entries are separated by a comma. (ex: 1-3,7-9)</p> <p><i>all</i> – Specifies that all ports on the switch will be configured for address binding.</p> <p><i>mode</i> – The user may set the mode for this IP-MAC-Port binding settings by choosing one of the following:</p> <ul style="list-style-type: none"> <i>arp</i> - Choosing this selection will set a normal IP-MAC-Port binding entry for the IP address and MAC address entered. <i>acl</i> - Choosing this entry will allow only packets from the source IP-MAC-Port binding entry created here. All other packets with a different IP address will be discarded by the Switch. This mode can only be used if the ACL Mode has been enabled in the IP-MAC-Port binding Ports window as seen previously.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To create address binding on the Switch:

```
DGS-3627:5#create address_binding ip_mac ipaddress 10.1.1.3
mac_address 00-00-00-00-00-04
Command: create address_binding ip_mac ipaddress 10.1.1.3
mac_address 00-00-00-00-00-04

Success.

DGS-3627:5#
```

To create address binding on the Switch for ACL mode:

```
DGS-3627:5#create address_binding ip_mac ipaddress 10.1.1.3
mac_address 00-00-00-00-00-04 mode acl
Command: create address_binding ip_mac ipaddress 10.1.1.3 mac_address
00-00-00-00-00-04 mode acl

Success.

DGS-3627:5#
```

config address_binding ip_mac ipaddress

Purpose	Used to configure an IP-MAC-Port binding entry.
Syntax	<ipaddr> mac_address <macaddr> {ports [<portlist> all] mode {arp acl}}
Description	This command will configure an IP-MAC-Port binding entry.
Parameters	<p><ipaddr> - The IP address of the device where the IP-MAC-Port binding is made.</p> <p><macaddr> - The MAC address of the device where the IP-MAC-Port binding is made.</p> <p><portlist> - Specifies a port or range of ports to be configured for address binding. The beginning and end of the port list range are separated by a dash. Non-contiguous portlist entries are separated by a comma. (ex: 1-3,7-9)</p> <p>all - Specifies that all ports on the switch will be configured for address binding.</p> <p>mode - The user may set the mode for this IP-MAC-Port binding settings by choosing one of the following:</p> <ul style="list-style-type: none"> arp - Choosing this selection will set a normal IP-MAC-Port binding entry for the IP address and MAC address entered. acl - Choosing this entry will allow only packets from the source IP-MAC-Port binding entry created here. All other packets with a different IP address will be discarded by the Switch. This mode can only be used if the ACL Mode has been enabled in the IP-MAC-Port binding Ports window as seen previously.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To configure address binding on the Switch:

```
DGS-3627:5#config address_binding ip_mac ipaddress
10.1.1.3 mac_address 00-00-00-00-00-05
Command: config address_binding ip_mac ipaddress
10.1.1.3 mac_address 00-00-00-00-00-05

Success.

DGS-3627:5#
```

To configure address binding on the Switch for ACL mode:

```
DGS-3627:5#config address_binding ip_mac ipaddress
10.1.1.3 mac_address 00-00-00-00-00-05 mode acl
Command: config address_binding ip_mac ipaddress
10.1.1.3 mac_address 00-00-00-00-00-05 mode acl

Success.
```

DGS-3627:5#

config address_binding ip_mac ports

Purpose	Used to configure an IP-MAC state to enable or disable for specified ports.
Syntax	config address_binding ip_mac ports [<portlist> all] state [enable disable]
Description	This command will configure IP-MAC state to enable or disable for specified ports.
Parameters	<p><portlist> – Specifies a port or range of ports. The beginning and end of the port list range are separated by a dash. Non-contiguous portlist entries are separated by a comma. (ex: 1-3,7-9)</p> <p>all – Specifies all ports on the switch.</p> <p>state [enable disable] – Enables or disables the specified range of ports.</p>
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To configure address binding on the Switch:

```
DGS-3627:5#config address_binding ip_mac ports 2 state enable
Command: config address_binding ip_mac ports 2 state enable
```

```
Success.
```

```
DGS-3627:5#
```

show address_binding

Purpose	Used to display IP-MAC-Port binding entries.
Syntax	[ip_mac {[all ipaddress <ipaddr> mac_address <macaddr>]} blocked {[all vlan_name <vlan_name> mac_address <macaddr>]} ports]
Description	<p>This command will display IP-MAC-Port binding entries. Three different kinds of information can be viewed.</p> <ul style="list-style-type: none"> • <i>ip_mac</i> – Address Binding entries can be viewed by entering the physical and IP addresses of the device. • <i>blocked</i> – 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. • <i>ports</i> - The number of enabled ports on a device.
Parameters	<p>all – For IP_MAC binding all specifies all the IP-MAC-Port binding entries; for Blocked Address Binding entries all specifies all the blocked VLANs and their bound physical addresses.</p> <p><ipaddr> The IP address of the device where the IP-MAC-Port binding is made.</p> <p><macaddr> The MAC address of the device where the IP-MAC-Port binding is made.</p> <p><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.</p>
Restrictions	None

Example usage:

To show IP-MAC-Port binding on the switch:

```
DGS-3627:5#show address_binding ip_mac ipaddress 10.1.1.8
mac_address 00-00-00-00-00-12
Command: show address_binding ip_mac ipaddress 10.1.1.8
mac_address 00-00-00-00-00-12
```

```
ACL_mode : Enabled
Trap/Log  : Disabled
Enabled ports: 2
```

IP Address	MAC Address	Status	Mode	Ports
10.1.1.8	00-00-00-00-00-12	Active	ACL	1-12

```
Total Entries : 1
```

```
DGS-3627:5#
```

delete address_binding

Purpose	Used to delete IP-MAC-Port binding entries.
Syntax	[ip-mac [ipaddress <ipaddr> mac_address <macaddr> all] blocked [all vlan_name <vlan_name> mac_address <macaddr>]]
Description	<p>This command will delete IP-MAC-Port binding entries. Two different kinds of information can be deleted.</p> <ul style="list-style-type: none"> • <i>IP_MAC</i> – Individual Address Binding entries can be deleted by entering the physical and IP addresses of the device. Toggling to <i>all</i> will delete all the Address Binding entries. • <i>Blocked</i> – Blocked address binding entries (bindings between VLAN names and MAC addresses) can be deleted by entering the VLAN name and the physical address of the device. To delete all the Blocked Address Binding entries, toggle <i>all</i>.
Parameters	<p><ipaddr> The IP address of the device where the IP-MAC-Port binding is made.</p> <p><macaddr> The MAC address of the device where the IP-MAC-Port binding is made.</p> <p><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.</p> <p><i>all</i> – For IP_MAC binding <i>all</i> specifies all the IP-MAC-Port binding entries; for Blocked Address Binding entries <i>all</i> specifies all the blocked VLANs and their bound physical addresses.</p>
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To delete an IP-MAC-Port binding on the Switch:

```
DGS-3627:5#delete address-binding ip-mac ipaddress 10.1.1.1 mac_address 00-00-00-00-00-06
Command: delete address-binding ip-mac ipaddress 10.1.1.1 mac_address 00-00-00-00-00-06

Success.

DGS-3627:5#
```

enable address_binding acl_mode

Purpose	Used to enable the ACL mode for an IP-MAC-Port binding entry.
Syntax	enable address_binding acl_mode
Description	This command, along with the disable address_binding acl_mode will enable and disable the ACL mode for IP-MAC-Port binding on the Switch, without altering previously set configurations. When enabled, the Switch will automatically create two ACL packet content mask entries that can be viewed using the show access_profile command. These two ACL entries will aid the user in processing certain IP-MAC-Port binding entries created.
Parameters	None.
Restrictions	Only administrator-level and operator-level users can issue this command. The ACL entries created when this command is enabled, can only be automatically installed if the Access Profile table has two entries available of the possible 14 entries allowed. These access profile entries can only be deleted using the disable address_binding acl_mode and not through the delete access_profile profile_id command. Also, the show config command will not display the commands for creating the IP-MAC ACL mode access profile entries.

Example usage:

To enable IP-MAC-Port binding ACL mode on the Switch:

```
DGS-3627:5#enable address_binding acl_mode
Command: enable address_binding acl_mode

Success.

DGS-3627:5#
```

disable address_binding acl_mode

Purpose	Used to disable the ACL mode for an IP-MAC-Port binding entry.
Syntax	disable address_binding acl_mode
Description	This command, along with the enable address_binding acl_mode will enable and disable the ACL mode for IP-MAC-Port binding on the Switch, without altering previously set configurations. When disabled, the Switch will automatically delete two previously created ACL packet content mask entries that can be viewed using the show access_profile command.
Parameters	None.
Restrictions	Only administrator-level and operator-level users can issue this command. The ACL entries created when this command is enabled, can only be automatically installed if the Access Profile table has two entries available of the possible 14 entries allowed. These access profile entries can only be deleted using the disable address_binding acl_mode and NOT through the delete access_profile profile_id command. Also, the show config command will not display the commands for creating the IP-MAC ACL mode access profile entries.

Example usage:

To disable IP-MAC-Port binding ACL mode on the Switch:

```
DGS-3627:5#disable address_binding acl_mode
Command: disable address_binding acl_mode

Success.

DGS-3627:5#
```

enable address_binding trap_log

Purpose	Used to enable the trap log for the IP-MAC-Port binding function.
Syntax	enable address_binding trap_log
Description	This command, along with the disable address_binding trap_log will enable and disable the sending of trap log messages for IP-MAC-Port binding. When enabled, the Switch will send a trap log message to the SNMP agent and the Switch log when an ARP packet is received that doesn't match the IP-MAC-Port binding configuration set on the Switch.
Parameters	None.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To enable sending of IP-MAC-Port binding trap log messages on the Switch:

```
DGS-3627:5#enable address_binding trap_log
Command: enable address_binding trap_log

Success.

DGS-3627:5#
```

disable address_binding trap_log

Purpose	Used to disable the trap log for the IP-MAC-Port binding function.
Syntax	disable address_binding trap_log
Description	This command, along with the enable address_binding trap_log will enable and disable the sending of trap log messages for IP-MAC-Port binding. When enabled, the Switch will send a trap log message to the SNMP agent and the Switch log when an ARP packet is received that doesn't match the IP-MAC-Port binding configuration set on the Switch.
Parameters	None.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To disable sending of IP-MAC-Port binding trap log messages on the Switch:

```
DGS-3627:5#disable address_binding trap_log
Command: disable address_binding trap_log

Success.

DGS-3627:5#
```


IP COMMANDS (INCLUDING IP MULTINETTING)

IP Multinetting is a function that allows multiple IP interfaces to be assigned to the same VLAN. This is beneficial to the administrator when the number of IPs on the original interface is insufficient and the network administrator wishes not to resize the interface. IP Multinetting is capable of assigning another IP interface on the same VLAN without affecting the original stations or settings of the original interface.

Two types of interfaces are configured for IP multinetting, primary and secondary, and every IP interface must be classified as one of these. A primary interface refers to the first interface created on a VLAN, with no exceptions. All other interfaces created will be regarded as secondary only, and can only be created once a primary interface has been configured. There may be 256 interfaces per VLAN (one primary, and up to 255 secondary) and they are, in most cases, independent of each other. Primary interfaces cannot be deleted if the VLAN contains a secondary interface. Once the user creates multiple interfaces for a specified VLAN (primary and secondary), that set IP interface cannot be changed to another VLAN.

IP Multinetting is a valuable tool for network administrators requiring a multitude of IP addresses, but configuring the Switch for IP multinetting may cause troubleshooting and bandwidth problems, and should not be used as a long term solution. Problems may include:

- The Switch may use extra resources to process packets for multiple IP interfaces.
- The amount of broadcast data, such as RIP update packets and PIM hello packets, will be increased

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

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

Command	Parameters
create ipif	<ipif_name 12> {<network_address>} <vlan_name 32> {secondary state [enable disable]}
config ipif	<ipif_name 12> [{ipaddress <network_address> vlan <vlan_name 32> state [enable disable]} bootp dhcp ipv6 ipv6address <ipv6networkaddr>]
enable ipif	[<ipif_name 12> all]
disable ipif	[<ipif_name 12> all]
delete ipif	[<ipif_name 12> {ipv6address <ipv6networkaddr>} all]
show ipif	{<ipif_name 12>}
enable ipif_ipv6_link_local_auto	[<ipif_name 12> all]
disable ipif_ipv6_link_local_auto	[<ipif_name 12> all]
show ipif_ipv6_link_local_auto	{<ipif_name 12>}

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

create ipif	
Purpose	Used to create an IP interface on the Switch.
Syntax	create ipif <ipif_name 12> {<network_address>} <vlan_name 32> {secondary state [enabled disabled]}
Description	This command will create an IP interface.
Parameters	<p><ipif_name 12> – The name for the IP interface to be created. The user may enter an alphanumeric string of up to 12 characters to define the IP interface.</p> <p><network_address> – IP address and netmask of the IP interface to be created. The address and mask information can be specified using the traditional format (for example, 10.1.2.3/255.0.0.0) or in CIDR format, (10.1.2.3/8). (This parameter may also appear as <ip_addr/netmask>).</p> <p><vlan_name 32> – The name of the VLAN that will be associated with the</p>

create ipif

above IP interface.

secondary – Enter this parameter if this configured IP interface is to be a *secondary* IP interface of the VLAN previously specified. *secondary* interfaces can only be configured if a *primary* interface is first configured.

state [enable | disable] – Allows the user to enable or disable the IP interface.

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

Example usage:

To create the primary IP interface, p1 on VLAN Tiberius:

```
DGS-3627:5#create ipif p1 10.1.1.1/8 Tiberius state enabled
```

```
Command: create ipif p1 10.1.1.1/8 Tiberius state enabled
```

```
Success.
```

```
DGS-3627:5#
```

To create the secondary IP interface, p2 on VLAN Tiberius:

```
DGS-3627:5#create ipif p2 12.1.1.1/8 Tiberius secondary state enable
```

```
Command: create ipif p2 12.1.1.1/8 Tiberius secondary state enable
```

```
Success.
```

```
DGS-3627:5#
```

config ipif

Purpose	Used to configure the System IP interface.
Syntax	config ipif <ipif_name 12> [{ipaddress <network_address> vlan <vlan_name 32> state [enable disable]} bootp dhcp ipv6 ipv6address <ipv6networkaddr>]
Description	This command is used to configure an IP interface on the Switch. Users may add one IPv4 address per interface but multiple IPv6 addresses may be added to a single interface. The format of IPv6 address resembles xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx where a set of xxxx represents a 16-bit hexadecimal value (ex. 2D83:0C76:3140:0000:0000:020C:417A:3214).
Parameters	<p><i><ipif_name 12></i> - Enter an alphanumeric string of up to 12 characters to identify this IP interface.</p> <p><i>ipaddress <network_address></i> – 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). Only one IPv4 address can be configured per interface.</p> <p><i><vlan_name 32></i> – The name of the VLAN corresponding to the IP interface.</p> <p><i>state [enable disable]</i> – Allows users to enable or disable the IP interface.</p> <p><i>bootp</i> – Allows the selection of the BOOTP protocol for the assignment of an IP address to the Switch's System IP interface. This method is only for IPv4 addresses and if users manually configure an IPv4 address and set this parameter, the manually set IP address will be overwritten by this protocol.</p> <p><i>dhcp</i> – Allows the selection of the DHCP protocol for the assignment</p>

config ipif

of an IP address to the Switch's System IP interface. If you are using the autoconfig feature, the Switch becomes a DHCP client automatically so it is not necessary to change the ipif settings. This method is only for IPv4 addresses and if users manually configure an IPv4 address and set this parameter, the manually set IP address will be overwritten by this protocol.

<ipv6networkaddr> - Use this parameter to statically assign an IPv6 address to this interface. This address should define a host address and a network prefix length. Multiple IPv6 addresses can be configured for a single IP interface. Ex: 3ffe:501:ffff:100::1/64. The /64 represents the prefix length of the IPv6 addresses.

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

Example usage:

To configure the IP interface System:

```
DGS-3627:5#config ipif System ipaddress 10.48.74.122/8
Command: config ipif System ipaddress 10.48.74.122/8

Success.

DGS-3627:5#
```

Example usage:

To configure the IPv6 address for IP interface Tiberius:

```
DGS-3627:5#config ipif Tiberius ipv6 ipv6address 3ffe:501:ffff:100::1/64
Command: config ipif Tiberius ipv6 ipv6address 3ffe:501:ffff:100::1/64

Success.

DGS-3627:5#
```

enable ipif

Purpose	Used to enable an IP interface on the Switch.
Syntax	enable ipif [<i><ipif_name 12></i> all]
Description	This command will enable the IP interface function on the Switch.
Parameters	<i><ipif_name 12></i> – The name of a previously configured IP interface to enable. Enter an alphanumeric entry of up to twelve characters to define the IP interface. <i>all</i> – Entering this parameter will enable all the IP interfaces currently configured on the Switch.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To enable the ipif function on the Switch:

```
DGS-3627:5#enable ipif s2
Command: enable ipif s2

Success.
```

```
DGS-3627:5#
```

disable ipif

Purpose	Used to disable the configuration of an IP interface on the Switch.
Syntax	disable ipif [<ipif_name 12> all]
Description	This command will disable an IP interface on the Switch, without altering its configuration values.
Parameters	<ipif_name 12> – The name previously created to define the IP interface. <i>all</i> – Entering this parameter will disable all the IP interfaces currently configured on the Switch.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To disable the IP interface named “s2”:

```
DGS-3627:5#disable ipif s2
Command: disable ipif s2

Success.

DGS-3627:5#
```

delete ipif

Purpose	Used to delete the configuration of an IP interface on the Switch.
Syntax	delete ipif [<ipif_name 12> {ipv6address <ipv6networkaddr>} all]
Description	This command will delete the configuration of an IP interface on the Switch.
Parameters	<ipif_name 12> – The name of the IP interface to delete. <ipv6networkaddr> - Use this parameter to delete an IPv6 address to this interface. This address should define a host address and a network prefix length. Multiple IPv6 addresses can be configured for a single IP interface. Ex: 3ffe:501:fff:100::1/64. The /64 represents the prefix length of the IPv6 addresses. <i>all</i> – Entering this parameter will delete all the IP interfaces currently configured on the Switch except the System interface.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To delete the IP interface named s2:

```
DGS-3627:5#delete ipif s2
Command: delete ipif s2

Success.

DGS-3627:5#
```

show ipif

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

Example usage:

To display IP interface settings.

```
DGS-3627:5#show ipif System
Command: show ipif System

IP Interface Settings

IP Interface       : System
VLAN Name         : default
Interface Admin State : Enabled
IPv4 Address      : 10.53.13.199/8 (Manual) Primary

DGS-3627:5#
```



NOTE: In the IP Interface Settings table shown above, the Secondary field will have two displays. *FALSE* denotes that the IP interface is a primary IP interface while *TRUE* denotes a secondary IP interface.

enable ipif_ipv6_link_local_auto

Purpose	Used to enable the autoconfiguration of the link local address when no IPv6 address is configured.
Syntax	enable ipif_ipv6_link_local_auto [<ipif_name 12> all]
Description	This command will automatically create an IPv6 link local address for the Switch if no IPv6 address has previously been configured.
Parameters	<ipif_name 12> – The name of the IP interface that will be given an IPv6 link local address. <i>all</i> – Entering this command will assign an IPv6 link-local address to all configured IP Interfaces currently configured on the switch.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To enable the IP interface IPv6 link-local settings .

```
DGS-3627:5#enable ipif_ipv6_link_local_auto all
Command:enable ipif_ipv6_link_local_auto all

Success.

DGS-3627:5#
```

disable ipif_ipv6_link_local_auto

Purpose	Used to disable the autoconfiguration of the IPv6 link local address.
Syntax	disable ipif_ipv6_link_local_auto [<ipif_name 12> all]
Description	This command will disable the automatic creation of an IPv6 link local address for the Switch. Once this command is entered, any previous IPv6 link local address that has been created for the IP interface selected will be deleted from the switch.
Parameters	<ipif_name 12> – The name of the IP interface that will be disabled for having an IPv6 link local address. all – Entering this command will disable IPv6 link-local addresses from being configured on IP Interfaces currently configured on the switch.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To disable the IP interface IPv6 link-local settings.

```
DGS-3627:5#disable ipif_ipv6_link_local_auto all
Command:disable ipif_ipv6_link_local_auto all

Success.

DGS-3627:5#
```

show ipif_ipv6_link_local_auto

Purpose	Used to display the link local automatic configuration state for IPv6.
Syntax	show ipif_ipv6_link_local_auto {<ipif_name 12>}
Description	This command will display the current link local automatic configuration state for IPv6.
Parameters	<ipif_name 12> – The name created for the IP interface, to be viewed.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To display IP interface settings.

```
DGS-3627:5# show ipif_ipv6_link_local_auto
Command: show ipif_ipv6_link_local_auto

IPIF : System      Automatic Link Local Address: Disabled.

DGS-3627:5#
```

IPv6 NEIGHBOR DETECTION COMMANDS

The following commands are used to detect IPv6 neighbors of 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 ra ipif	<ipif_name 12> {state [enable disable] life_time <value 0-9000> reachable_time <value 0-3600000> retrans_time <uint 0-4294967295> hop_limit <value 0-255> managed_flag [enable disable] other_config_flag [enable disable] min_rtr_adv_interval <value 3-1350> max_rtr_adv_interval <value 4-1800>}
config ipv6 nd ra prefix_option ipif	<ipif_name 12> <ipv6networkaddr> {preferred_life_time <uint 0-4294967295> valid_life_time <uint 0-4294967295> on_link_flag [enable disable] autonomus_flag [enable disable]}
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	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	<p><ipif_name 12> - Enter the IPv6 interface name previously created using the create ipif command.</p> <p><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.</p> <p><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.</p>
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To create a static IPv6 neighbor:

```
DGS-3627:5#create ipv6 neighbor_cache ipif Triton 3FFC::1 00-01-02-03-04-05
Command: create ipv6 neighbor_cache ipif Triton 3FFC::1 00-01-02-03-04-05

Success.

DGS-3627:5#
```

delete ipv6 neighbor_cache

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	<p><ipif_name 12> - Enter the IPv6 interface name previously created using the create ipif commands.</p> <p><i>all</i> – Enter this parameter to denote all IPv6 interfaces created on the switch.</p> <p><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.</p> <p><i>static</i> - Enter this command to remove all statically configured neighbor devices from being an IPv6 neighbor of the IP interface previously entered.</p> <p><i>dynamic</i> - Enter this command to remove all dynamically configured neighbor devices from being an IPv6 neighbor of the IP interface previously entered.</p> <p><i>all</i> – Enter this parameter to remove all IPv6 neighbors of the switch.</p>
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To delete a static IPv6 neighbor:

```
DGS-3627:5# delete ipv6 neighbor_cache ipif Zira 3FFC::1
Command: delete ipv6 neighbor_cache ipif Zira 3FFC::1

Success.

DGS-3627:5#
```

show ipv6 neighbor_cache

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	<p><ipif_name 12> - Enter the IP interface for which to view IPv6 neighbors. This will display all IPv6 neighbors of this interface.</p> <p><i>all</i> – Enter this parameter to denote all IPv6 interfaces created on the switch.</p> <p><i>ipv6address</i> <ipv6addr> - Enter the IPv6 address of the neighbor by which to view this information.</p> <p><i>static</i> – Enter this parameter to view all statically entered IPv6 neighbors of the switch.</p> <p><i>dynamic</i> - Enter this command to view all dynamically configured neighbor devices which are IPv6 neighbors of the IP interface previously entered.</p> <p><i>all</i> – Enter this parameter to view all configured neighbor devices which are IPv6 neighbors of the IP interface previously entered.</p>
Restrictions	None.

Example usage:

To display the IPv6 neighbors of a configured IP interface:

```
DGS-3627:5# show ipv6 neighbor_cache ipif Zira all
Command: show ipv6 neighbor_cache ipif Zira all

Neighbor                Link Layer Address Interface  State
-----
FE80::20B:6AFF:FECF:7EC6  00:0B:6A:CF:7E:C6  Zira          R

Total Entries : 1

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

DGS-3627:5#
```

config ipv6 nd ra ipif

Purpose	Used to configure the parameters for router advertisement packets being sent from the switch.
Syntax	config ipv6 nd ra ipif <ipif_name 12> {state [enable disable] life_time <value 0-9000> reachable_time <value 0-3600000> retrans_time <uint 0-4294967295> hop_limit <value 0-255> managed_flag [enable disable] other_config_flag [enable disable] min_rtr_adv_interval <value 3-1350> max_rtr_adv_interval <value 4-1800>}
Description	This command is used to configure the settings for router advertisement packets being sent from the switch.
Parameters	<p><i><ipif_name 12></i> - Enter the IPv6 interface name that will be dispatching these router advertisements.</p> <p><i>state {enable disable}</i> – Use this parameter to enable or disable the sending of router advertisement packets from the IPv6 interface name previously stated.</p> <p><i>life_time <value 0-9000></i> - This time represents the validity of this IPv6 interface to be the default router for the link-local network. A value of 0 represents that this Switch should not be recognized as the default router for this link-local network. The user may set a time between 0 and 9000 seconds with a default setting of 1800 seconds.</p> <p><i>reachable_time <value 0-3600000></i> - This field will set the time that remote IPv6 nodes are considered reachable. In essence, this is the Neighbor Unreachability Detection field once confirmation of the access to this node has been made. The user may set a time between 0 and 3600000 milliseconds with a default setting of 1200000 milliseconds. A very low value is not recommended.</p> <p><i>retrans_time <uint 0-4294967295></i> - Used to set an interval time between 0 and 4294967295 milliseconds for the dispatch of router advertisements by this interface over the link-local network, in response to a Neighbor Solicitation message. If this Switch is set as the default router for this local link, this value should not exceed the value stated in the Life Time field previously mentioned. Setting this field to zero will specify that this switch will not specify the Retransmit Time for the link-local network. (and therefore will be specified by another router on the link-local network. The default value is 0 milliseconds.</p> <p><i>hop_limit <value 0-255></i> - This field sets the number of nodes that this Router Advertisement packet will pass before being dropped. This number is set to depreciate by one after every node it reaches and will be dropped once the Hop Limit reaches 0. The user may set the Hop Limit between 0 and 255 with</p>

config ipv6 nd ra ipif

a default value of 64.

managed_flag [enable | disable] – Used to enable or disable the Managed flag. When enabled, this will trigger the router to use a stateful autoconfiguration process to get both Global and link-local IPv6 addresses for the Switch. The default setting is *Disabled*.

other_config_flag [enable | disable] – Used to enable or disable the alternate configuration flag. When enabled, this will trigger the router to use a stateful autoconfiguration process to get configuration information that is not address information, yet is important to the IPv6 settings of the Switch. The default setting is *Disabled*.

min_rtr_adv_interval <value 3-1350> - Used to set the minimum interval time between the dispatch of router advertisements by this interface over the link-local network. This entry must be no less than 3 seconds and no more than .75 (3/4) of the MaxRtrAdvInterval. The user may configure a time between 3 and 1350 seconds with a default setting of 198 seconds.

max_rtr_adv_interval <value 4-1800> - Used to set the maximum interval time between the dispatch of router advertisements by this interface over the link-local network. This entry must be no less than 4 seconds (4000 milliseconds) and no more than 1800 seconds. The user may configure a time between 4 and 1800 seconds with a default setting of 600 seconds.

Restrictions

Only administrator-level and operator-level users can issue this command.

Example usage:

To configure the parameters for the Router Advertisements:

```
DGS-3627:5#config ipv6 nd ra ipif triton state enable life_time 1000
reachable_time 10000 retrans_time 50000 hop_limit 10 managed_flag enable
other_config_flag enable min_rtr_adv_interval 50 max_rtr_adv_interval 100
Command: config ipv6 nd ra ipif triton state enable life_time 1000 reachable_time
10000 retrans_time 50000 hop_limit 10 managed_flag enable other_config_flag
enable min_rtr_adv_interval 50 max_rtr_adv_interval 100
```

Success.

```
DGS-3627:5#
```

config ipv6 nd ra prefix_option ipif

Purpose	Used to configure the parameters for the prefix option of the router advertisements.
Syntax	config ipv6 nd ra prefix_option ipif <ipif_name 12> <ipv6networkaddr> {preferred_life_time <uint 0-4294967295> valid_life_time <uint 0-4294967295> on_link_flag [enable disable] autonomus_flag [enable disable]}
Description	This command will configure the parameters for the prefix option located in the router advertisements. Users may set a prefix for Global Unicast IPv6 addresses to be assigned to other nodes on the link-local network. This prefix is carried in the Router Advertisement message to be shared on the link-local network. The user must first have a Global Unicast Address set for the Switch.
Parameters	<p><ipif_name 12> - Enter the IPv6 interface name that will be dispatching these router advertisements.</p> <p><ipv6networkaddr> - Enter the IPv6 prefix for Global Unicast IPv6 addresses to be assigned to other nodes on the link-local network. This prefix is carried in the Router Advertisement message to be shared on the link-local network. The user must first have a Global Unicast Address set for the Switch.</p>

config ipv6 nd ra prefix_option ipif

preferred_life_time <uint 0-4294967295> - This field states the time that this prefix is advertised as being preferred on the link local network, when using stateless address configuration. The user may configure a time between 0 and 4294967295 milliseconds, with a default setting of 604800 milliseconds.

valid_life_time <unit 0-4294967295> - This field states the time that this prefix is advertised as valid on the link local network, when using stateless address configuration. The user may configure a time between 0 and 4294967295 milliseconds.

on_link_flag [enable | disable] - Setting this field to *enable* will denote, within the IPv6 packet, that the IPv6 prefix configured here is assigned to this link-local network. Once traffic has been successfully sent to these nodes with this specific IPv6 prefix, the nodes will be considered reachable on the link-local network.

autonomus_flag [enable | disable] - Setting this field to *enable* will denote that this prefix may be used to autoconfigure IPv6 addresses on the link-local network.

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

Example usage:

To configure the prefix option for the interface “Zira”:

```
DGS-3627:5#config ipv6 nd ra prefix_option ipif Zira 3FFE:501:FFFF:100::/64
preferred_life_time 1000 valid_life_time 1000 on_link_flag enable autonomus_flag enable
Command: config ipv6 nd ra prefix_option ipif Zira 3FFE:501:FFFF:100::/64
preferred_life_time 1000 valid_life_time 1000 on_link_flag enable autonomus_flag enable
```

Success.

DGS-3627:5#

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 <unit 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 of 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 this 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 and operator-level users can issue this command.

Example usage:

To configure The IPv6 ND Neighbor Solicitation messages:

```
DGS-3627:5# config ipv6 nd ns ipif Zira retrans_time 1000000
Command: config ipv6 nd ns ipif Zira retrans_time 1000000

Success.

DGS-3627:5#
```

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	<i>ipif <ipif_name 12></i> - 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 and operator-level users can issue this command.

Example usage:

To display the neighbor detection parameters for IPv6:

```
DGS-3627:5#show ipv6 nd
Command: show ipv6 nd

Interface Name      : System
Hop Limit           : 64
NS Retransmit Time  : 0 (ms)
Router Advertisement : Disabled
RA Max Router AdvInterval : 600 (s)
RA Min Router AdvInterval : 198 (s)
RA Router Life Time : 1800 (s)
RA Reachable Time   : 1200000 (ms)
RA Retransmit Time  : 0 (ms)
RA Managed Flag     : Disabled
RA Other Config Flag : Disabled

Interface Name      : Zira
Hop Limit           : 10
NS Retransmit Time  : 50000 (ms)
Router Advertisement : Enabled
RA Max Router AdvInterval : 100 (s)
RA Min Router AdvInterval : 50 (s)
RA Router Life Time : 1000 (s)
RA Reachable Time   : 10000 (ms)
RA Retransmit Time  : 50000 (ms)
RA Managed Flag     : Enabled
RA Other Config Flag : Enabled
Prefix              Preferred Valid OnLink Autonomous
3FFE:501:FFFF:100::/64 604800 2592000 Enabled Enabled

DGS-3627:5#
```

IGMP COMMANDS (INCLUDING IGMP v3)

IGMP or Internet Group Management Protocol is a protocol implemented by systems utilizing IPv4 to collect the membership information needed by the multicast routing protocol through various query messages sent out from the router or switch. Computers and network devices that want to receive multicast transmissions need to inform nearby routers that they will become members of a multicast group. The Internet Group Management Protocol (IGMP) is used to communicate this information. IGMP is also used to periodically check the multicast group for members that are no longer active.

In the case where there is more than one multicast router on a subnetwork, one router is elected as the 'querier'. This router then keeps track of the membership of the multicast groups that have active members. The information received from IGMP is then used to determine if multicast packets should be forwarded to a given subnetwork or not. The router can check, using IGMP, to see if there is at least one member of a multicast group on a given subnetwork. If there are no members on a subnetwork, packets will not be forwarded to that subnetwork.

The current release of the Switch now implements IGMPv3. Improvements of IGMPv3 over version 2 include:

- The introduction of the SSM or Source Specific Multicast. In previous versions of IGMP, the host would receive all packets sent to the multicast group. Now, a host will receive packets only from a specific source or sources. This is done through the implementation of include and exclude filters used to accept or deny traffic from these specific sources.
- In IGMPv2, Membership reports could contain only one multicast group whereas in v3, these reports can contain multiple multicast groups.
- Leaving a multicast group could only be accomplished using a specific leave message in v2. In v3, leaving a multicast group is done through a Membership report which includes a block message in the group report packet.
- For version 2, the host could respond to either a group query but in version 3, the host is now capable to answer queries specific to the group and the source.

IGMPv3 is backwards compatible with other versions of IGMP and all IGMP protocols must be used in conjunction with PIM-DM or DVMRP for optimal use.

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

Command	Parameters
config igmp	[ipif <ipif_name 12> all] {version <value 1-3> query_interval <sec 1-31744> max_response_time <sec 1-25> robustness_variable <value 1-255> last_member_query_interval <value 1-25> state [enable disable]}
show igmp	{ipif <ipif_name 12>}
show igmp group	{group <group> ipif <ipif_name 12>}

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

config igmp	
Purpose	Used to configure IGMP on the Switch.
Syntax	config igmp [ipif <ipif_name 12> all] {version <value 1-3> query_interval <sec 1-31744> max_response_time <sec 1-25> robustness_variable <value 1-255> last_member_query_interval <value 1-25> state [enable disable]}
Description	This command allows users to configure IGMP on the Switch.
Parameters	<p><i><ipif_name 12></i> – The name of the IP interface for which to configure IGMP.</p> <p><i>all</i> – Specifies all the IP interfaces on the Switch.</p> <p><i>version <value 1-3></i> – Select the IGMP version number.</p> <p><i>query_interval <sec 1-31744></i> – The time in seconds between general query transmissions, in seconds.</p> <p><i>max_response_time <sec 1-25></i> – Enter the maximum time in seconds</p>

config igmp

that the Switch will wait for reports from members.

robustness_variable <value 1-255> – This value states the permitted packet loss that guarantees IGMP.

last_member_query_interval <value 1-25> – The Max Response Time inserted into Group-Specific Queries and Group-and-Source specific queries sent in response to Leave Group messages, and is also the amount of time between Group-Specific Query and Group-and-Source specific query messages. The default is 1 second.

state [enable | disable] – Enables or disables IGMP for the specified IP interface.

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

Example Usage:

To configure the IGMPv2 for all IP interfaces.

```
DGS-3627:5#config igmp all version 2
```

```
Command: config igmp all version 2
```

```
Success.
```

```
DGS-3627:5#
```

show igmp

Purpose Used to display the IGMP configuration for the Switch of for a specified IP interface.

Syntax **show igmp {ipif <ipif_name 12>}**

Description This command will display the IGMP configuration for the Switch if no IP interface name is specified. If an IP interface name is specified, the command will display the IGMP configuration for that IP interface.

Parameters <ipif_name 12> – The name of the IP interface for which the IGMP configuration will be displayed.

Restrictions None.

Example usage:

To display IGMP configurations:

```
DGS-3627:5#show igmp
```

```
Command: show igmp
```

IGMP Interface Configurations

Interface	IP Address/Netmask	Ver- sion	Query	Maximum Response Time	Robust- ness Value	Last Member Query Interval	State
System	10.90.90.90/8	1	125	10	2	1	Enabled
p1	20.1.1.1/8	1	125	10	2	1	Enabled

```
Total Entries: 2
```

```
DGS-3627:5#
```

show igmp group

Purpose	Used to display the Switch's IGMP group table.
Syntax	show igmp group {group <group> ipif <ipif_name 12>}
Description	This command will display the IGMP group configuration.
Parameters	<i>group <group></i> – The ID of the multicast group to be displayed. <i><ipif_name 12></i> – The name of the IP interface of which the IGMP group is a member.
Restrictions	None.

Example usage:

To display IGMP group table:

```
DGS-3627:5#show igmp group
Command: show igmp group
```

Interface	Multicast Group	Last Reporter	IP Querier	IP Expire
System	224.0.0.2	10.42.73.111	10.48.74.122	260
System	224.0.0.9	10.20.53.1	10.48.74.122	260
System	224.0.1.24	10.18.1.3	10.48.74.122	259
System	224.0.1.41	10.1.43.252	10.48.74.122	259
System	224.0.1.149	10.20.63.11	10.48.74.122	259

Total Entries: 5

```
DGS-3627:5#
```

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 <vlan_name 32> all] {host_timeout <sec 1-16711450> router_timeout <sec 1-16711450> leave_timer <sec 1-16711450> state [enable disable] fast_leave [enable disable]}
config igmp_snooping querier	[vlan <vlan_name 32> 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]}
config router_ports	<vlan_name 32> [add delete] <portlist>
config router_ports_forbidden	<vlan_name 32> [add delete] <portlist>
enable igmp_snooping	{forward_mcrouter_only}
show igmp_snooping	{vlan <vlan_name 32>}
disable igmp_snooping	{forward_mcrouter_only}
show igmp snooping group	{vlan <vlan_name 32>}
show router_ports	{vlan <vlan_name 32>} {[static dynamic forbidden]}
show igmp_snooping forwarding	{vlan <vlan_name 32>}
create igmp_snooping multicast_vlan	<vlan_name 32> <vlanid 2-4094>
config igmp_snooping multicast_vlan	<vlan_name 32> {member_port <portlist> source_port <portlist> state [enable disable] replace_source_ip <ipaddr>}
delete igmp_snooping multicast_vlan	<vlan_name 32>
show igmp_snooping multicast_vlan	{<vlan_name 32>}
config igmp_snooping multicast_vlan_group	<vlan_name 32> [add multicast_range <range_name 32> delete multicast_range [<range_name 32> all]]
show igmp_snooping multicast_vlan_group	{<vlan_name 32>}

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 <vlan_name 32> all] {host_timeout <sec 1-16711450> router_timeout <sec 1-16711450> leave_timer <sec 1-16711450> state [enable disable]} fast_leave [enable disable]}
Description	This command allows users to configure IGMP snooping on the Switch.
Parameters	<p><i> vlan <vlan_name 32> </i> – The name of the VLAN for which IGMP snooping is to be configured.</p> <p><i> host_timeout <sec 1-16711450> </i> – Specifies the maximum amount of time a host can be a member of a multicast group without the Switch receiving a host membership report. The default is 260 seconds.</p> <p><i> router_timeout <sec 1-16711450> </i> – Specifies the maximum amount of time a route can be a member of a multicast group without the Switch receiving a</p>

config igmp_snooping

host membership report. The default is 260 seconds.

leave_timer <sec 1-16711450> – Specifies the amount of time a Multicast address will stay in the database before it is deleted, after it has sent out a leave group message. The default is 2 seconds.

state [*enable* | *disable*] – Allows you to enable or disable IGMP snooping for the specified VLAN.

fast_leave [*enable* | *disable*] – This parameter allows the user to enable the *fast leave* function. Enabled, this function will allow members of a multicast group to leave the group immediately (without the implementation of the Last Member Query Timer) when an IGMP Leave Report Packet is received by the Switch.

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

Example usage:

To configure IGMP snooping:

```
DGS-3627:5#config igmp_snooping vlan default host_timeout 250 state enable
```

```
Command: config igmp_snooping vlan default host_timeout 250 state enable
```

```
Success.
```

```
DGS-3627:5#
```



NOTE: The *Fast Leave* function in the **config igmp_snooping** command can only be implemented if IGMP is disabled for all IP interfaces on the Switch. Configuring this function when IGMP is enabled will produce the error message “*Cannot set Fast leave when IGMP is running*” and consequently will not be implemented.

config igmp_snooping querier

Purpose	This command configures IGMP snooping querier.
Syntax	config igmp_snooping querier [vlan <vlan_name 32> 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]}
Description	Used to configure 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.
Parameters	<p><vlan_name 32> – The name of the VLAN for which IGMP snooping querier is to be configured.</p> <p><i>query_interval</i> <sec 1-65535> – Specifies the amount of time in seconds between general query transmissions. The default setting is 125 seconds.</p> <p><i>max_response_time</i> <sec 1-25> – Specifies the maximum time in seconds to wait for reports from members. The default setting is 10 seconds.</p> <p><i>robustness_variable</i> <value 1-255> – 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:</p> <ul style="list-style-type: none"> 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).

config igmp_snooping querier

- 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. Although 1 is specified as a valid entry, the robustness variable should not be one or problems may arise.

last_member_query_interval <sec 1-25> – The maximum amount of time between group-specific query messages, including those sent in response to leave-group messages. Users may 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 [enable | disable] – Allows the Switch to be specified as an IGMP Querier or Non-querier.

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

Example usage:

To configure IGMP snooping:

```
DGS-3627:5#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-3627:5#
```

config router_ports

Purpose	Used to configure ports as router ports.
Syntax	config router_ports <vlan_name 32> [add delete] <portlist>
Description	This command allows designation of 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	<i>add delete</i> – Specify whether to add or delete ports as router ports. <vlan_name 32> – The name of the VLAN on which the router port resides. <portlist> – Specifies a port or range of ports that will be configured as router ports. The beginning and end of the port list range are separated by a dash. Non-contiguous portlist entries are separated by a comma. (ex: 1-3,7-9)
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To set up static router ports:

```
DGS-3627:5#config router_ports default add 1-10
```

```
Command: config router_ports default add 1-10
```

Success.

```
DGS-3627:5#
```

config router_ports_forbidden

Purpose	Used to configure ports as forbidden multicast router ports.
Syntax	config router_ports_forbidden <vlan_name 32> [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	<p><i><vlan_name 32></i> – The name of the VLAN on which the router port resides.</p> <p><i>[add delete]</i> - Specifies whether to add or delete forbidden ports of the specified VLAN.</p> <p><i><portlist></i> – Specifies a range of ports that will be configured as forbidden router ports. The beginning and end of the port list range are separated by a dash. Non-contiguous portlist entries are separated by a comma. (ex: 1-3,7-9)</p>
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To set up forbidden router ports:

```
DGS-3627:5#config router_ports_forbidden default add 2-10
Command: config router_ports_forbidden default add 2-10

Success.

DGS-3627:5#
```

enable igmp_snooping

Purpose	Used to enable IGMP snooping on the Switch.
Syntax	enable igmp_snooping {forward_mcrouter_only}
Description	This command allows enabling of IGMP snooping on the Switch. If <i>forward_mcrouter_only</i> is specified, the Switch will only forward all multicast traffic to the multicast router, only. Otherwise, the Switch forwards all multicast traffic to any IP router.
Parameters	<i>forward_mcrouter_only</i> – Specifies that the Switch should only forward all multicast traffic to a multicast-enabled router. Otherwise, the Switch will forward all multicast traffic to any IP router.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To enable IGMP snooping on the Switch:

```
DGS-3627:5#enable igmp_snooping
Command: enable igmp_snooping

Success.
```

DGS-3627:5#

disable igmp_snooping

Purpose	Used to disable IGMP snooping on the Switch.
Syntax	disable igmp_snooping {forward_mcrouter_only}
Description	This command disables IGMP snooping on the Switch. IGMP snooping can be disabled only if IP multicast routing is not being used. Disabling IGMP snooping allows all IGMP and IP multicast traffic to flood within a given IP interface.
Parameters	<i>forward_mcrouter_only</i> – Adding this parameter to this command will disable forwarding all multicast traffic to a multicast-enabled routers. The Switch will then forward all multicast traffic to any IP router. Entering this command without the parameter will disable igmp snooping on the Switch.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To disable IGMP snooping on the Switch:

```
DGS-3627:5#disable igmp_snooping
Command: disable igmp_snooping
```

```
Success.
```

```
DGS-3627:5#
```

Example usage:

To disable forwarding all multicast traffic to a multicast-enabled router:

```
DGS-3627:5#disable igmp_snooping forward_mcrouter_only
Command: disable igmp_snooping forward_mcrouter_only
```

```
Success.
```

```
DGS-3627:5#
```

show igmp_snooping

Purpose	Used to show the current status of IGMP snooping on the Switch.
Syntax	show igmp_snooping {vlan <vlan_name 32>}
Description	This command will display the current IGMP snooping configuration on the Switch.
Parameters	<i><vlan_name 32></i> – The name of the VLAN for which to view the IGMP snooping configuration.
Restrictions	None.

Example usage:

To show IGMP snooping:

```
DGS-3627:5#show igmp_snooping
```

Command: show igmp_snooping

IGMP Snooping Global State : Disabled
Multicast router Only : Disabled

VLAN Name : default
Query Interval : 125
Max Response Time : 10
Robustness Value : 2
Last Member Query Interval : 1
Host Timeout : 260
Router Timeout : 260
Leave Timer : 2
Querier State : Disabled
Querier Router Behavior : Non-Querier
State : Disabled
Fast Leave : Enabled

Total Entries: 1

DGS-3627:5#

show igmp_snooping_group

Purpose	Used to display the current IGMP snooping group configuration on the Switch.
Syntax	show igmp_snooping_group {vlan <vlan_name 32>}
Description	This command will display the current IGMP snooping group configuration on the Switch.
Parameters	<vlan_name 32> – The name of the VLAN for which to view IGMP snooping group configuration information.
Restrictions	None.

Example usage:

To show IGMP snooping group:

```
DGS-3627:5#show igmp_snooping_group
Command: show igmp_snooping_group

VLAN Name   : default
Multicast group: 224.0.0.2
MAC address  : 01-00-5E-00-00-02
Reports     : 1
Port Member  : 2, 5

VLAN Name   : default
Multicast group: 224.0.0.9
MAC address  : 01-00-5E-00-00-09
Reports     : 1
Port Member  : 6, 8

VLAN Name   : default
Multicast group: 234.5.6.7
MAC address  : 01-00-5E-05-06-07
Reports     : 1
Port Member  : 4, 10

Total Entries : 3
DGS-3627:5#
```

show router_ports

Purpose	Used to display the currently configured router ports on the Switch.
Syntax	show router_ports {vlan <vlan_name 32>} {[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. <i>static</i> – Displays router ports that have been statically configured. <i>dynamic</i> – Displays router ports that have been dynamically configured. <i>forbidden</i> - Displays router ports that have been labeled as forbidden.
Restrictions	None.

Example usage:

To display the router ports.

```
DGS-3627:5#show router_ports
```

```
Command: show router_ports
```

```
VLAN Name      : default
```

```
Static router port : 1-2, 10
```

```
Dynamic router port :
```

```
Forbidden router port :
```

```
Total Entries: 1
```

```
DGS-3627:5#
```

show igmp_snooping forwarding

Purpose	Used to display the IGMP snooping forwarding table entries on the Switch.
Syntax	show igmp_snooping forwarding {vlan <vlan_name 32>}
Description	This command will display the current IGMP snooping forwarding table entries currently configured on the Switch.
Parameters	<vlan_name 32> – The name of the VLAN for which to view IGMP snooping forwarding table information.
Restrictions	None.

Example usage:

To view the IGMP snooping forwarding table for VLAN “Marcello”:

```
DGS-3627:5#show igmp_snooping forwarding vlan Marcello
```

```
Command: show igmp_snooping forwarding vlan Marcello
```

```
VLAN Name      : Marcello
```

```
Source IP      : 198.19.1.2
```

```
Multicast group : 239.1.1.1
```

```
Port Member    : 11
```

```
Total Entries: 1
```

```
DGS-3627:5#
```

create igmp_snooping multicast_vlan

Purpose	Used to create a multicast VLAN on the Switch.
Syntax	create igmp_snooping multicast_vlan <vlan_name 32> <vlanid 2-4094>
Description	This command allows you to create a multicast VLAN on the Switch.
Parameters	<vlan_name 32> – The name of the multicast VLAN to be created. This name may be up to 32 characters in length. <vlanid 2-4094> - The corresponding VLAN ID of the multicast VLAN to be created.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To create a multicast VLAN:

```
DGS-3627:5#create igmp_snooping multicast_vlan accounting 2
Command: create igmp_snooping multicast_vlan accounting 2

Success.

DGS-3627:5#
```

config igmp_snooping multicast_vlan

Purpose	Used to configure the settings for a previously created multicast VLAN.
Syntax	config igmp_snooping multicast_vlan <vlan_name 32> {member_port <portlist> source_port <portlist> state [enable disable] replace_source_ip <ipaddr>
Description	This command allows users to configure the settings for a previously created multicast VLAN on the switch.
Parameters	<p><i><vlan_name 32></i> – The name of the multicast VLAN for which IGMP snooping is to be configured. This name may be up to 32 characters in length.</p> <p><i>member_port <portlist></i> - Enter a port or list of ports to be added to the multicast VLAN. Member ports will become the untagged members of the multicast VLAN.</p> <p><i>source_port <portlist></i> - Enter a port or list of ports to be added to the multicast VLAN. Source ports will become the tagged members of the multicast VLAN.</p> <p><i>state [enable disable]</i> – Use these parameters to enable or disable the multicast VLAN.</p> <p><i>replace_source_ip <ipaddr></i> - Use this parameter to replace the source IP address.</p>
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To configure a multicast VLAN:

```
DGS-3627:5#config igmp_snooping multicast_vlan accounting
member_port 4-5 source_port 6 state enable
Command: config igmp_snooping multicast_vlan accounting
member_port 4-5 source_port 6 state enable

Success.

DGS-3627:5#
```

delete igmp_snooping multicast_vlan

Purpose	Used to delete a previously created multicast VLAN on the Switch.
Syntax	delete igmp_snooping multicast_vlan <vlan_name 32>
Description	This command allows you to delete a previously created multicast VLAN on the Switch.
Parameters	<i><vlan_name 32></i> – The name of the multicast VLAN to be deleted. This name may be up to 32 characters in length.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To delete a multicast VLAN called “accounting”:

```
DGS-3627:5#delete igmp_snooping multicast_vlan accounting
Command: delete igmp_snooping multicast_vlan accounting

Success.

DGS-3627:5#
```

show igmp_snooping multicast_vlan

Purpose	Used to display the settings of a multicast VLAN on the Switch.
Syntax	show igmp_snooping multicast_vlan {<vlan_name 32>}
Description	This command allows you to display the settings of a multicast VLAN on the Switch.
Parameters	<vlan_name 32> – The name of the multicast VLAN to be displayed. This name may be up to 32 characters in length.
Restrictions	None.

Example usage:

To show a multicast VLAN:

```
DGS-3627:5#show igmp_snooping multicast_vlan accounting
Command: snow igmp_snooping multicast_vlan accounting

VID           : 2      VLAN Name    : accounting
Member Ports  : 4-5
Source Ports  : 6
Status        : Enabled
Replace Source IP : 0.0.0.0

DGS-3627:5#
```

config igmp_snooping multicast_vlan_group

Purpose	Used to add or remove multicast addresses to or from a previously created Multicast VLAN.
Syntax	config igmp_snooping multicast_vlan_group <vlan_name 32> [add multicast_range <range_name 32> delete multicast_range [<range_name 32> all]]
Description	This command allows users to configure the multicast group which will be learned with the specific multicast VLAN.
Parameters	<p><vlan_name 32> – The name of the multicast VLAN for which IGMP snooping is to be configured. This name may be up to 32 characters in length.</p> <p><i>add multicast_range <range_name 32></i> - Use this parameter to add a multicast address or list of multicast addresses to this multicast VLAN as defined by a range. This range was created using the limited multicast address commands.</p> <p><i>delete multicast_range <range_name 32></i> - Use this parameter to delete a multicast address or list of multicast addresses to this multicast VLAN as defined by a range. This range was created using the limited multicast address commands.</p> <p><i>all</i> - Enter this parameter to remove all multicast addresses range names</p>

config igmp_snooping multicast_vlan_group

from the selected multicast VLAN.

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

Example usage:

To add a multicast range to a previously created multicast VLAN:

```
DGS-3627:5# config igmp_snooping multicast_vlan_group accounting add
multicast_range 1
Command: config igmp_snooping multicast_vlan_group accounting add
multicast_range 1

Success.

DGS-3627:5#
```

show igmp_snooping multicast_vlan_group

Purpose	Used to display the settings of a multicast VLAN group on the Switch.
Syntax	show igmp_snooping multicast_vlan_group {<vlan_name 32>}
Description	This command allows you to display the settings of a multicast VLAN group on the Switch.
Parameters	<vlan_name 32> – The name of the multicast VLAN to be displayed. This name may be up to 32 characters in length.
Restrictions	None.

Example usage:

To display a multicast VLAN:

```
DGS-3627:5#show igmp_snooping multicast_vlan_group accounting
Command: snow igmp_snooping multicast_vlan_group accounting

Multicast VLAN      : accounting

No.  Name                From          To
---  -
1    1                    229.1.1.1    229.1.1.2

DGS-3627:5#
```

MLD SNOOPING COMMANDS

Multicast Listener Discovery (MLD) Snooping is an IPv6 function used similarly to IGMP snooping in IPv4. It is used to discover ports on a VLAN that are requesting multicast data. Instead of flooding all ports on a selected VLAN with multicast traffic, MLD snooping will only forward multicast data to ports that wish to receive this data through the use of queries and reports produced by the requesting ports and the source of the multicast traffic.

MLD snooping is accomplished through the examination of the layer 3 part of an MLD control packet transferred between end nodes and a MLD router. When the Switch discovers that this route is requesting multicast traffic, it adds the port directly attached to it into the correct IPv6 multicast table, and begins the process of forwarding multicast traffic to that port. This entry in the multicast routing table records the port, the VLAN ID and the associated multicast IPv6 multicast group address and then considers this port to be an active listening port. The active listening ports are the only ones to receive multicast group data.

MLD Control Messages

Three types of messages are transferred between devices using MLD snooping. These three messages are all defined by three ICMPv6 packet headers, labeled 130, 131 and 132.

1. **Multicast Listener Query** – Similar to the IGMPv2 Host Membership Query for IPv4, and labeled as 130 in the ICMPv6 packet header, this message is sent by the router to ask if any link is requesting multicast data. There are two types of MLD query messages emitted by the router. The General Query is used to advertise all multicast addresses that are ready to send multicast data to all listening ports, and the Multicast Specific query, which advertises a specific multicast address that is also ready. These two types of messages are distinguished by a multicast destination address located in the IPv6 header and a multicast address in the Multicast Listener Query Message.
2. **Multicast Listener Report** – Comparable to the Host Membership Report in IGMPv2, and labeled as 131 in the ICMP packet header, this message is sent by the listening port to the Switch stating that it is interested in receiving multicast data from a multicast address in response to the Multicast Listener Query message.
3. **Multicast Listener Done** – Akin to the Leave Group Message in IGMPv2, and labeled as 132 in the ICMPv6 packet header, this message is sent by the multicast listening port stating that it is no longer interested in receiving multicast data from a specific multicast group address, therefore stating that it is “done” with the multicast data from this address. Once this message is received by the Switch, it will no longer forward multicast traffic from a specific multicast group address to this listening port.

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

Command	Parameters
enable mld_snooping	{forward_mcrouter_only}
disable mld_snooping	{forward_mcrouter_only}
config mld_snooping	[vlan <vlan_name 32> all] {node_timeout <sec 1-16711450> router_timeout <sec 1-16711450> done_timer <sec 1-16711450> state [enable disable] fast_done [enable disable]}
config mld_snooping mrouter_ports	<vlan_name 32> [add delete] <portlist>
config mld_snooping mrouter_ports_forbidden	<vlan_name 32> [add delete] <portlist>
config mld_snooping querier	[vlan <vlan_name 32> 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]}
show mld_snooping	{vlan <vlan_name 32>}
show mld_snooping group	{vlan <vlan_name 32>}
show mld_snooping mrouter_ports	{vlan <vlan_name 32>} {[static dynamic forbidden]}
show mld_snooping forwarding	{vlan <vlan_name 32>}

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

enable mld_snooping

Purpose	Used to enable MLD snooping globally on the switch.
Syntax	enable mld_snooping {forward_mcrouter_only}
Description	This command, in conjunction with the disable mld_snooping will enable and disable MLD snooping globally on the Switch without affecting configurations.
Parameters	<i>forward_mcrouter_only</i> - Specifies that the Switch should only forward all multicast traffic to a multicast-enabled router. Otherwise, the Switch will forward all multicast traffic to any IP router.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To enable MLD snooping globally on the Switch:

```
DGS-3627:5#enable mld_snooping
Command: enable mld_snooping

Success.

DGS-3627:5#
```

disable mld_snooping

Purpose	Used to disable MLD snooping globally on the switch.
Syntax	disable mld_snooping {forward_mcrouter_only}
Description	This command, in conjunction with the enable mld_snooping will enable and disable MLD snooping globally on the switch without affecting configurations.
Parameters	<i>forward_mcrouter_only</i> – Specify to disable the Switch from forwarding all multicast traffic to a multicast-enabled router. Otherwise, the Switch will forward all multicast traffic to any IP router.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To disable MLD snooping globally on the Switch:

```
DGS-3627:5#disable mld_snooping
Command: disable mld_snooping

Success.

DGS-3627:5#
```

config mld_snooping

Purpose	Used to configure MLD snooping on the Switch.
Syntax	config mld_snooping [vlan <vlan_name 32> all] {node_timeout <sec 1-16711450> router_timeout <sec 1-16711450> done_timer <sec 1-16711450> state [enable disable] fast_done [enable disable]}
Description	This command allows the user to configure MLD snooping on the Switch.

config mld_snooping

Parameters	<p><i>vlan</i> <vlan_name 32> – The name of the VLAN for which MLD snooping is to be configured.</p> <p><i>all</i> – Entering this parameter will configure MLD snooping for all VLANs on the Switch.</p> <p><i>node_timeout</i> <sec 1-16711450> – Specifies the link node timeout, in seconds. After this timer expires, this node will no longer be considered as listening node. The user may specify a time between 1 and 16711450 with a default setting of 260 seconds.</p> <p><i>router_timeout</i> <sec 1-16711450> – Specifies the maximum amount of time a router can remain in the Switch's routing table as a listening node of a multicast group without the Switch receiving a node listener report. The user may specify a time between 1 and 16711450 with a default setting of 260 seconds.</p> <p><i>done_timer</i> <sec 1-16711450> – Specifies the maximum amount of time a router can remain in the Switch after receiving a done message from the group without receiving a node listener report. The user may specify a time between 1 and 16711450 with a default setting of 2 seconds.</p> <p><i>state</i> [enable disable] – Allows the user to enable or disable MLD snooping for the specified VLAN.</p> <p><i>fast_done</i> [enable disable] – This parameter allows the user to enable the <i>fast done</i> function. Enabled, this function will allow members of a multicast group to leave the group immediately when a <i>done</i> message is received by the Switch.</p>
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To configure MLD snooping:

```
DGS-3627:5#config mld_snooping vlan default node_timeout 250 state enable
Command : config mld_snooping vlan default node_timeout 250 state enable
```

```
Success.
```

```
DGS-3627:5#
```

config mld_snooping mrouter_ports

Purpose	Used to configure ports as router ports on the Switch.
Syntax	config mld_snooping mrouter_ports <vlan_name 32> [add delete] <portlist>
Description	This command allows the user to designate a range of ports as being connected to a multicast-enabled router. This command will ensure that all packets with this router as its destination will reach the multicast-enabled router.
Parameters	<p><i>vlan</i> <vlan_name 32> – The name of the VLAN on which the router port resides.</p> <p><i>add delete</i> – Specify to add or delete ports as router ports.</p> <p><i><portlist></i> - Specify a port or range of ports to be configured as router ports. The beginning and end of the port list range are separated by a dash. Non-contiguous portlist entries are separated by a comma. (ex: 1-3,7-9)</p>
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To configure MLD snooping multicast router ports:

```
DGS-3627:5#config mld_snooping mrouter_ports default add 1-10
Command : config mld_snooping mrouter_ports default add 1-10

Success.

DGS-3627:5#
```

config mld_snooping mrouter_ports_forbidden

Purpose	Used to configure ports on the Switch as forbidden router ports.
Syntax	config mld_snooping mrouter_ports_forbidden <vlan_name 32> [add delete] <portlist>
Description	This command allows the user to designate a port or range of ports as being forbidden from being connected to multicast enabled routers. This ensures that these configured forbidden ports will not send out routing packets.
Parameters	<i>vlan <vlan_name 32></i> – The name of the VLAN on which the router port will be forbidden. <i>add delete</i> – Specify to add or delete ports as forbidden router ports. <i><portlist></i> - Specify a port or range of ports to be configured as forbidden router ports. The beginning and end of the port list range are separated by a dash. Non-contiguous portlist entries are separated by a comma. (ex:1-3,7-9)
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To configure MLD snooping forbidden multicast router ports:

```
DGS-3627:5#config mld_snooping mrouter_ports_forbidden default add 11-12
Command : config mld_snooping mrouter_ports_forbidden default add 11-12

Success

DGS-3627:5#
```

config mld_snooping querier

Purpose	Used to configure the timers and settings for the MLD snooping querier for the Switch.
Syntax	config mld_snooping querier [vlan <vlan_name 32> 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]}
Description	This command allows the user to configure the time between general query transmissions, the maximum time to wait for reports from listeners and the permitted packet loss guaranteed by MLD snooping.
Parameters	<i>vlan <vlan_name 32></i> – The name of the VLAN for which to configure the MLD querier. <i>all</i> – Specifies all VLANs are to be configured for the MLD querier. <i>query_interval <sec 1-65535></i> - Specifies the amount of time between general query transmissions. The user may specify a time between 1 and 65535 seconds with a default setting of 125 seconds. <i>max_response_time <sec 1-25></i> - The maximum time to wait for reports from listeners. The user may specify a time between 1 and 25 seconds with a default setting of 10 seconds. <i>robustness_variable <value 1-255></i> - Provides fine-tuning to allow for expected packet

config mld_snooping querier

loss on a subnet. The user may choose a value between 1 and 255 with a default setting of 2. If a subnet is expected to be lossy, the user may wish to increase this interval.

last_listener_query_interval <sec 1-25> - The maximum amount of time to be set between group-specific query messages. This interval may be reduced to lower the amount of time it takes a router to detect the loss of a last listener group. The user may set this interval between 1 and 25 seconds with a default setting of 1 second.

state [enable | disable] – Enabling the querier state will set the Switch as a MLD querier and disabling it will set it as a Non-querier. The default setting is enabled.

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

Example usage:

To configure the MLD snooping querier:

```
DGS-3627:5#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-3627:5#
```

NOTE: The robustness variable of the MLD snooping querier is used in creating the following MLD message intervals:

Group Listener Interval – This is the amount of time that must pass before a multicast router decides that there are no more listeners present of a group on a network. Calculated as (robustness variable * query interval) + (1 * query interval).

Querier Present Interval - This is the amount of time that must pass before a multicast router decides that there are no other querier devices present. Calculated as (robustness variable * query interval) + (0.5 * query response interval).

Last Listener Query Count – This is the amount of group-specific queries sent before the router assumes there are no local listeners in this group. The default value is the value of the robustness variable.



show mld_snooping

Purpose	Used to display the current status of the MLD snooping function on the Switch.
Syntax	show mld_snooping {vlan<vlan_name 32>}
Description	This command allows the user to display the current status of the MLD snooping function on the Switch.
Parameters	<i>vlan</i> <vlan_name 32> – The name of the VLAN for which to view the MLD snooping configurations. If no parameter is specified, the Switch will display all current MLD snooping configurations.
Restrictions	None.

Example usage:

To display the MLD snooping settings

```

DGS-3627:5#show mld_snooping
Command: show mld_snooping

MLD Snooping Global State      : Disabled
Multicast router Only         : Disabled

VLAN Name                      : default
Query Interval                 : 125
Max Response Time              : 10
Robustness Value               : 2
Last Listener Query Interval   : 1
Node Timeout                   : 260
Router Timeout                 : 260
Done Timer                     : 2
Querier State                  : Disabled
Querier Router Behavior        : Non-Querier
State                          : Disabled
Fast Done                      : Disabled

Total Entries : 1

DGS-3627:5#
    
```

show mld_snooping group

Purpose	Used to display MLD snooping group configurations on the Switch.
Syntax	show mld_snooping group {vlan <vlan_name 32>}
Description	This command displays MLD snooping group configurations on the Switch.
Parameters	<i>vlan <vlan_name 32></i> – The name of the VLAN for which to view the MLD snooping group configurations. If no parameter is specified, the Switch will display all current MLD snooping group configurations.
Restrictions	None.

Example usage:

To display the MLD snooping group settings:


```
DGS-3627:5#show mld_snooping group
```

```
Command : show mld_snooping group
```

```
VLAN Name       : default
Multicast Group  : FF02 ::13
MAC Address      : 33-33-00-00-00-13
Reports         : 1
Listening Port   : 1, 7
```

```
VLAN Name       : default
Multicast Group  : FF02 ::14
MAC Address      : 33-33-00-00-00-14
Reports         : 1
Listening Port   : 2, 7
```

```
VLAN Name       : default
Multicast Group  : FF02 ::15
MAC Address      : 33-33-00-00-00-15
Reports         : 1
Listening Port   : 2, 9
```

```
VLAN Name       : default
Multicast Group  : FF02 ::16
MAC Address      : 33-33-00-00-00-16
Reports         : 1
Listening Port   : 2, 7
```

```
VLAN Name       : default
Multicast Group  : FF02 ::17
MAC Address      : 33-33-00-00-00-17
Reports         : 1
Listening Port   : 2, 7
```

```
Total Entries :5
```

```
DGS-3627:5#
```

show mld_snooping mrouter_ports

Purpose	Used to display the current router ports set on the Switch.
Syntax	show mld_snooping mrouter_ports {vlan<vlan_name 32>} {[static dynamic forbidden]}
Description	This command display the current router ports set on the Switch.
Parameters	<p><i>vlan <vlan_name 32></i> – The name of the VLAN on which the router port resides.</p> <p><i>static</i> – Displays router ports that have been statically configured.</p> <p><i>dynamic</i> – Displays router ports that have been dynamically configured.</p> <p><i>forbidden</i> – Displays router ports that have been configured as forbidden.</p> <p>If no parameter is specified, the Switch will display all currently configured router ports on the Switch.</p>
Restrictions	None.

Example usage:

To display the MLD snooping multicast router port settings:

DGS-3627:5#show mld_snooping mrouter_ports

Commands : show mld_snooping mrouter_ports

VLAN Name : default

Static mrouter port : 1-10

Dynamic mrouter port :

Forbidden mrouter port :

Total Entries : 1

DGS-3627:5#

show mld_snooping forwarding

Purpose	Used to display the MLD snooping forwarding table entries on the Switch.
Syntax	show mld_snooping forwarding {vlan <vlan_name 32>}
Description	This command will display the current MLD snooping forwarding table entries currently configured on the Switch.
Parameters	<vlan_name 32> – The name of the VLAN for which to view MLD snooping forwarding table information.
Restrictions	None.

Example usage:

To view the MLD snooping forwarding table for VLAN “accounting”:

DGS-3627:5#show mld_snooping forwarding vlan accounting

Command: show mld_snooping forwarding vlan accounting

VLAN Name : accounting

Source IP : 2001::1

Multicast Group : FF1E::1

Port Member : 10

Total Entries: 1

DGS-3627:5#

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>}
config dhcp_relay add ipif	<ipif_name 12> <ipaddr>
config dhcp_relay delete ipif	<ipif_name 12> <ipaddr>
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>}
Description	This command is used to configure the DHCP/BOOTP relay feature.
Parameters	<i>hops <value 1-16></i> Specifies the maximum number of relay agent hops that the DHCP packets can cross. <i>time <sec 0-65535></i> If this time is exceeded, the Switch will relay the DHCP packet.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To config DHCP relay:

```
DGS-3627:5#config dhcp_relay hops 2 time 23
Command: config dhcp_relay hops 2 time 23

Success.

DGS-3627:5#
```

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 which to forward (relay) DHCP/BOOTP relay packets.
Parameters	<ipif_name 12> The name of the IP interface in which DHCP relay is to

config dhcp_relay add ipif

	be enabled.
	<ipaddr> The DHCP server IP address.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To add an IP destination to the DHCP relay table:

```
DGS-3627:5#config dhcp_relay add ipif System 10.58.44.6
Command: config dhcp_relay add ipif System 10.58.44.6

Success.

DGS-3627:5#
```

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-level and operator-level users can issue this command.

Example usage:

To delete an IP destination from the DHCP relay table:

```
DGS-3627:5#config dhcp_relay delete ipif System 10.58.44.6
Command: config dhcp_relay delete ipif System 10.58.44.6

Success.

DGS-3627:5#
```

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. 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, which receives the packet, and if the server is capable of option 82, it can implement policies like restricting the number of IP

config dhcp_relay option_82 state

	addresses that can be assigned to a single remote ID or circuit ID. The DHCP server will then echo 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 then 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 is connected to the DHCP client that sent the DHCP request.
Parameters	<p><i>enable</i> – Choose this parameter to enable the addition of option 82 information to a packet.</p> <p><i>disable</i>- Choose <i>disable</i> the relay agent from inserting and removing DHCP relay information (option 82 field) in messages between DHCP servers and clients, and the check and policy settings will have no effect.</p>
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To configure DHCP relay option 82 state:

```
DGS-3627:5#config dhcp_relay option_82 state enable
Command: config dhcp_relay option_82 state enable

Success.

DGS-3627:5#
```

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. 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.
Parameters	<p><i>enable</i> – Choose this parameter to enable validity checking of option 82 within packets.</p> <p><i>disable</i> - When the field is toggled to <i>disable</i>, the relay agent will not check the validity of the packet's option 82 field.</p>
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To configure DHCP relay option 82 check:

```
DGS-3627:5#config dhcp_relay option_82 check enable
Command: config dhcp_relay option_82 check enable

Success.

DGS-3627:5#
```

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	<p><i>replace</i> - The option 82 field will be replaced if the option 82 field already exists in the packet received from the DHCP client.</p> <p><i>drop</i> - The packet will be dropped if the option 82 field already exists in the packet received from the DHCP client.</p> <p><i>keep</i> - The option 82 field will be retained if the option 82 field already exists in the packet received from the DHCP client.</p>
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To configure DHCP relay option 82 policy:

```
DGS-3627:5#config dhcp_relay option_82 policy replace
Command: config dhcp_relay option_82 policy replace

Success.

DGS-3627:5#
```

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	<i>ipif <ipif_name 12></i> - 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-3627:5#show dhcp_relay
Command: show dhcp_relay

DHCP/BOOTP Relay Status           : Enabled
DHCP/BOOTP Hops Count Limit       : 2
DHCP/BOOTP Relay Time Threshold   : 23
DHCP Relay Agent Information Option 82 State : Enabled
DHCP Relay Agent Information Option 82 Check : Enabled
DHCP Relay Agent Information Option 82 Policy : Replace

Interface  Server 1  Server 2  Server 3  Server 4
-----  -
System    10.58.44.6
```

DGS-3627:5#

Example usage:

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

```

DGS-3627:5#show dhcp_relay ipif System
Command: show dhcp_relay ipif System

DHCP/Bootp Relay Status      : Disabled
DHCP/Bootp Hops Count Limit  : 4
DHCP/Bootp Relay Time Threshold : 0
DHCP Relay Agent Information Option 82 State : Disabled
DHCP Relay Agent Information Option 82 Check : Disabled
DHCP Relay Agent Information Option 82 Policy : Replace

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

```

DGS-3627:5#

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-level and operator-level users can issue this command.

Example usage:

To enable DHCP relay:

```

DGS-3627:5#enable dhcp_relay
Command: enable dhcp_relay

Success.

DGS-3627:5#

```

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-level and operator-level users can issue this command.

Example usage:

To disable DHCP relay:

```
DGS-3627:5#disable dhcp_relay
Command: disable dhcp_relay

Success.

DGS-3627:5#
```


DHCP SERVER COMMANDS

For this release, the Switch now has the capability to act as a DHCP server to devices within its locally attached network. DHCP, or Dynamic Host Configuration Protocol, allows the switch to delegate IP addresses, subnet masks, default gateways and other IP parameters to devices that request this information. This occurs when a DHCP enabled device is booted on or attached to the locally attached network. This device is known as the DHCP client and when enabled, it will emit query messages on the network before any IP parameters are set. When the DHCP server receives this request, it returns a response to the client, containing the previously mentioned IP information that the DHCP client then utilizes and sets on its local configurations.

The user can configure many DHCP related parameters that it will utilize on its locally attached network, to control and limit the IP settings of clients desiring an automatic IP configuration, such as the lease time of the allotted IP address, the range of IP addresses that will be allowed in its DHCP pool, the ability to exclude various IP addresses within the pool as not to make identical entries on its network, or to assign the IP address of an important device (such as a DNS server or the IP address of the default route) to another device on the network.

Users also have the ability to bind IP addresses within the DHCP pool to specific MAC addresses in order to keep consistent the IP addresses of devices that may be important to the upkeep of the network that require a static IP address.

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 dhcp pool	<pool_name 12>
delete dhcp pool	{<pool_name 12> all}
create dhcp pool manual_binding	<pool_name 12> <ipaddr> hardware_address <macaddr> {type [Ethernet IEE802]}
delete dhcp pool manual_binding	<pool_name 12> [<ipaddr> all]
show dhcp pool manual_binding	{<pool_name 12>}
show dhcp_binding	{<pool_name 12>}
clear dhcp_binding	{<pool_name 12>}
config dhcp ping_packets	<number 2-10>
config dhcp ping_timeout	<millisecond 500-2000>
config dhcp pool boot_file	<pool_name 12> <file_name 64>
config dhcp pool default_router	<pool_name 12> <ipaddr> {<ipaddr>} {<ipaddr>}
config dhcp pool dns_server_address	<pool_name 12> <ipaddr> {<ipaddr>} {<ipaddr>}
config dhcp pool domain_name	<pool_name 12> <domain_name 64>
config dhcp pool lease	<pool_name 12> [<day 0-365> <hour 0-23> <minute 0-59> infinite]
config dhcp pool netbios_name_server	<pool_name 12> <ipaddr> {<ipaddr>} {<ipaddr>}
config dhcp pool netbios_node_type	<pool_name 12> {broadcast peer_to_peer mixed hybrid}
config dhcp pool network_addr	<pool_name 12> <network_address>
config dhcp pool next_server	<pool_name 12> <ipaddr>
enable dhcp_server	
disable dhcp_server	
show dhcp_server	
create dhcp excluded_address begin_address	<ipaddr> end_address <ipaddr>

Command	Parameters
delete dhcp excluded_address	
show dhcp excluded_address	

Each command is listed in detail in the following sections.

create dhcp pool

Purpose	Used to create a DHCP pool.
Syntax	create dhcp pool <pool_name 12>
Description	This command will create a DHCP pool for the DHCP server. Once created, this pool may be modified for accepting DHCP clients into this pool.
Parameters	<i><pool_name 12></i> - Enter an name of up to 12 alphanumeric characters to identify the pool to be created with this command.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To create the DHCP pool Floor2:

```
DGS-3627:5#create dhcp pool Floor2
Command:create dhcp pool Floor2

Success.

DGS-3627:5#
```

delete dhcp pool

Purpose	Used to delete a DHCP pool.
Syntax	delete dhcp pool {<pool_name 12> all}
Description	This command will delete a DHCP pool that was created with the create dhcp pool command.
Parameters	<i><pool_name 12></i> - Enter an name of up to 12 alphanumeric characters to identify the pool to be deleted with this command. <i>all</i> - Enter this command to delete all created DHCP pool.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To delete the DHCP pool Floor2:

```
DGS-3627:5# delete dhcp pool Floor2
Command:delete dhcp pool Floor2

Success.

DGS-3627:5#
```

create dhcp pool manual_binding

Purpose	Used to create a DHCP pool manual binding entry.
Syntax	create dhcp pool manual_binding <pool_name 12> <ipaddr> hardware_address <macaddr> {type [Ethernet IEE802]}
Description	This command will create a DHCP manual pool binding entry for a previously created pool. When a MAC address is entered in this command, it will be bound to a IP address from the given pool either by the user, or automatically by the Switch.
Parameters	<p><i><pool_name 12></i> - Enter the name of the previously created pool that will contain the manual binding entry.</p> <p><i><ipaddr></i> - Enter the IP address to be statically bound to a device within the local network that will be specified by entering the Hardware Address in the following field.</p> <p><i>hardware_address <macaddr></i> - Enter the MAC address of the device to be statically bound to the IP address entered in the previous field.</p> <p><i>type [Ethernet IEE802]</i> - This field is used to specify the type of connection for which this manually bound entry will be set. <i>Ethernet</i> will denote that the manually bound device is connected directly to the Switch, while the <i>IEEE802</i> denotes that the manually bound device is outside the local network of the Switch.</p>
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To create a manual binding DHCP entry:

```
DGS-3627:5# create dhcp pool manual_binding engineering 10.10.10.1
hardware_address 02.02.02.02.02.02 type Ethernet
Command: create dhcp pool manual_binding engineering 10.10.10.1
hardware_address 02.02.02.02.02.02 type Ethernet

Success.

DGS-3627:5#
```

delete dhcp pool manual_binding

Purpose	Used to delete a previously created DHCP manual binding entry.
Syntax	delete dhcp pool manual_binding <pool_name 12> [<ipaddr> all]
Description	This command will delete a DHCP manual binding entry created with the create dhcp pool manual_binding command.
Parameters	<p><i><pool_name 12></i> - Enter the previously created pool name from which to delete a manual binding DHCP entry.</p> <p><i><ipaddr></i> - Enter the IP address of the manual binding entry to be deleted.</p> <p><i>all</i> - Enter this command to delete all manual binding entries for the given pool.</p>
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To display the multicast range Trinity:

```
DGS-3627:5#delete dhcp pool manual_binding Floor2 10.10.10.1
Command: delete dhcp pool manual_binding Floor2 10.10.10.1

Success.

DGS-3627:5#
```

show dhcp pool manual_binding

Purpose	Used to display the manual binding settings for a DHCP pool.
Syntax	show dhcp pool manual_binding {<pool_name 12>}
Description	This command will display the manual binding entries for the selected DHCP pool.
Parameters	<pool_name 12> - Enter the name of the DHCP pool for which to view manual binding entries. Entering this command without the pool name will display all manual binding entries of the DHCP server.
Restrictions	None.

Example usage:

To display the manual binding entries of the DHCP pool accounting:

```
DGS-3627:5# show dhcp pool manual_binding accounting
Command: show dhcp pool manual_binding accounting

Pool Name      IP Address      Hardware Address  Type
-----
accounting     192.168.0.1     01-22-b7-35-ce-99 Ethernet
accounting     192.168.0.2     0a-52-f7-34-ce-88 Ethernet

Total Entries : 2

DGS-3627:5#
```

show dhcp_binding

Purpose	Used to show the DHCP binding information.
Syntax	show dhcp_binding {<pool_name 12>}
Description	This command is used to display the DHCP binding information by created pool. Entering the command without the pool name will display all information regarding DHCP binding on the switch.
Parameters	<pool_name 12> - Enter the name of the DHCP pool for which to view manual binding information.
Restrictions	None.

Example usage:

To display the DHCP binding information on the Switch:

DGS-3627:5#show dhcp_binding

Command:show dhcp_binding

DHCP Binding Table

Pool Name	IP Address	Hardware Address	Type	Status	Life Time (secs)
engineering	192.168.0.1	01-22-b7-35-ce-99	Ethernet	Manual	864000

Total Entries : 1

DGS-3627:5#

clear dhcp_binding

Purpose	Used to clear the DHCP binding information.
Syntax	clear dhcp_binding {<pool_name 12>}
Description	This command is used to clear the DHCP binding settings for a particular created DHCP pool.
Parameters	<pool_name 12> - Enter the name of the DHCP pool for which to clear the manual binding information.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To display the DHCP binding information on the Switch:

DGS-3627:5#clear dhcp_binding

Command:clear dhcp_binding

Success.

DGS-3627:5#

config dhcp ping_packets

Purpose	Used to set the number of ping packets that will be sent out to find if an IP address is available.
Syntax	config dhcp ping_packets <number 2-10>
Description	This command will set the number of ping packets that will be sent out to find if an IP address is available to be allocated as a valid DHCP IP address.
Parameters	<number 2-10> - Enter a number between 2 and 10 to denote the number of ping packets that the Switch will send out on the network containing the IP address to be allotted. If the ping request is not returned, the IP address is considered unique to the local network and then allotted to the requesting client. The default setting is 2 packets.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To configure the number of ping packets to be used for DHCP:

```
DGS-3627:5#config dhcp ping_packets 2
Command: config dhcp ping_packets 2

Success.

DGS-3627:5#
```

config dhcp ping_timeout

Purpose	Used to set the time the Switch will wait before timing out a ping packet.
Syntax	config dhcp ping_timeout <millisecond 500-2000>
Description	This command is used set the time the Switch will wait before timing out a ping packet. If no answer is received, the IP address is considered unused and may be allocated to a requesting client.
Parameters	<i><millisecond 500-2000></i> - The user may set a time between 500 and 2000 milliseconds that the Switch will wait before timing out a ping packet. The default setting is 500 milliseconds.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To configure the Ping timeout:

```
DGS-3627:5#config dhcp ping_timeout 500
Command: config dhcp ping_timeout 500

Success.

DGS-3627:5#
```

config dhcp pool boot_file

Purpose	Used to specify the Boot File that will be used as the boot image of the DHCP client
Syntax	config dhcp pool boot_file <pool_name 12> <file_name 64>
Description	This command is used to specify the Boot File that will be used as the boot image of the DHCP client. This image is usually the operating system that the client uses to load its IP parameters.
Parameters	<i><pool_name 12></i> - Enter the previously created pool name from which the boot file will be set. <i><file_name 64></i> - Enter the name of the boot file that will be used for DHCP clients.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To set the boot file:

```
DGS-3627:5#config dhcp pool boot_file accounting boot.had
Command: config dhcp pool boot_file accounting boot.had

Success.
```

DGS-3627:5#

config dhcp pool default_router

Purpose	Used to configure the default router for the DHCP client.
Syntax	config dhcp pool default_router <pool_name 12> <ipaddr> {<ipaddr>} {<ipaddr>}
Description	This command is used to configure the default router for DHCP clients requesting DHCP information for the switch. Users may add up to three IP addresses to identify the router, but must specify at least one.
Parameters	<i><pool_name 12></i> - Enter the previously created pool name for which to add a default router. <i><ipaddr></i> - Enter the IP address for the default router for this pool. Users may specify up to three default routers but users must add at least one.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To configure the default router:

```
DGS-3627:5#config dhcp pool default_router accounting 10.245.32.1
Command: config dhcp pool default_router accounting 10.245.32.1

Success.

DGS-3627:5#
```

config dhcp pool dns_server_address

Purpose	Used to configure the IP addresses of DNS servers for a specific DHCP pool.
Syntax	config dhcp pool dns_server_address <pool_name 12> <ipaddr> {<ipaddr>} {<ipaddr>}
Description	This command is used to configure the DNS server IP addresses for a specific DHCP pool for the switch. The DNS Server correlates IP addresses to host names when queried. Users may add up to three DNS Server addresses.
Parameters	<i><pool_name 12></i> - Enter the previously created pool name for which to add a DNS address. <i><ipaddr></i> - Enter the IP address for the DNS server for this pool. Users may specify up to three DNS servers.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To configure the DNS server address for a DHCP pool:

```
DGS-3627:5# config dhcp pool dns_server_address accounting 10.245.32.1
Command: config dhcp pool dns_server_address accounting 10.245.32.1

Success.
```

```
DGS-3627:5#
```

config dhcp pool domain_name

Purpose	Used to configure the domain name for the DHCP pool of the Switch.
Syntax	config dhcp pool domain_name <pool_name 12> <domain_name 64>
Description	This command is used to configure the domain name for the DHCP pool of the Switch. This domain name represents a general group of networks that collectively make up the domain.
Parameters	<pool_name 12> - Enter the previously created pool name for which to add a default router. <domain_name 64> - The Domain Name may be an alphanumeric string of up to 64 characters.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To configure the domain name for a DHCP pool:

```
DGS-3627:5# config dhcp pool domain_name accounting d_link.com
Command: config dhcp pool domain_name accounting d_link.com

Success.

DGS-3627:5#
```

config dhcp pool lease

Purpose	Used to configure the lease time of DHCP clients within a DHCP pool.
Syntax	config dhcp pool lease <pool_name 12> [<day 0-365> <hour 0-23> <minute 0-59> infinite]
Description	Using this command, the user can specify the lease time for the DHCP client. This time represents the amount of time that the allotted address is valid on the local network.
Parameters	<pool_name 12> - Enter the previously created pool name for which to set the lease time for accepted DHCP clients. <i>day 0-365</i> – Enter the amount of days for the lease. The default setting is one day. <i>hour 0-23</i> – Enter the number of hours for the lease. <i>minute 0-59</i> - Enter the number of minutes for the lease. <i>infinite</i> – Enter this parameter to set the allotted IP address to never be timed out of its lease.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To configure the lease time for the DHCP pool:

```
DGS-3627:5# config dhcp pool lease accounting infinite
Command: config dhcp pool lease accounting infinite

Success.
```



```
DGS-3627:5#
```

config dhcp pool netbios_name_server

Purpose	Used to configure the IP address(es) for the Net BIOS name server,
Syntax	config dhcp pool netbios_name_server <pool_name 12> <ipaddr> {<ipaddr>} {<ipaddr>}
Description	This command is used to enter the IP address of a Net BIOS Name Server that will be available to a Microsoft DHCP Client. This Net BIOS Name Server is actually a WINS (Windows Internet Naming Service) Server that allows Microsoft DHCP clients to correlate host names to IP addresses within a general grouping of networks. The user may establish up to three Net BIOS Name Servers.
Parameters	<i><pool_name 12></i> - Enter the previously created pool name for which to set the Net BIOS name server for DHCP clients. <i><ipaddr></i> - Enter the IP address for the Net BIOS name server for this pool. Users may specify up to three Net BIOS name servers.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To configure the Net BIOS name server for the DHCP pool:

```
DGS-3627:5# config dhcp pool netbios_name_server accounting 10.98.254.2
Command: config dhcp pool netbios_name_server accounting 10.98.254.2

Success.

DGS-3627:5#
```

config dhcp pool netbios_node_type

Purpose	Used to set the Net BIOS node type for the DHCP server.
Syntax	config dhcp pool netbios_node_type <pool_name 12> {broadcast peer_to_peer mixed hybrid}
Description	This command is used to allow users to set the type of node server for the previously configured Net BIOS Name server. The user has four choices for node types which are <i>Broadcast</i> , <i>Peer to Peer</i> , <i>Mixed</i> and <i>Hybrid</i> .
Parameters	<i><pool_name 12></i> - Enter the previously created pool name for which to set the Net BIOS node type for DHCP clients. <i>{broadcast peer_to_peer mixed hybrid}</i> – Users may choose the node type for the Net BIOS from one of the four listed.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To configure the Net BIOS node type for the DHCP pool:

```
DGS-3627:5#config dhcp pool netbios_node_type accounting hybrid
Command: config dhcp pool netbios_node_type accounting hybrid

Success.
```

```
DGS-3627:5#
```

config dhcp pool network_addr

Purpose	Used to configure the network address and corresponding subnet mask for the DHCP pool.
Syntax	config dhcp pool network_addr <pool_name 12> <network_address>
Description	This command will allow users to enter the IP address pool to be assigned to requesting DHCP Clients. This address will not be chosen but the first 3 sets of numbers in the IP address will be used for the IP address of requesting DHCP Clients. (ex. If this entry is given the IP address 10.10.10.2, then assigned addresses to DHCP Clients will resemble 10.10.10.x, where x is a number between 1 and 255 but does not include the assigned 10.10.10.2)
Parameters	<p><i><pool_name 12></i> - Enter the previously created pool name for which to set the network address.</p> <p><i><network_address></i> - IP address and netmask that is the address of this DHCP pool. The address and mask information can be specified using the traditional format (for example, 10.1.2.3/255.0.0.0 or in CIDR format, 10.1.2.3/8).</p>
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To configure the network address for the DHCP pool:

```
DGS-3627:5#config dhcp pool network_addr accounting 10.1.1.1/8
Command:config dhcp pool network_addr accounting 10.1.1.1/8

Success.

DGS-3627:5#
```

config dhcp pool next_server

Purpose	Used to configure the IP address of the server that has the boot file for the DHCP pool.
Syntax	config dhcp pool next_server <pool_name 12> <ipaddr>
Description	This command is used to configure the IP address of the server that has the boot file for the DHCP pool.
Parameters	<i><pool_name 12></i> - Enter the previously created pool name for which to set the next server. <i><ipaddr></i> - Enter the IP address of the next server which has the boot file.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To configure the IP address of the next server:

```
DGS-3627:5#config dhcp pool next_server accounting 10.99.88.77
Command: config dhcp pool next_server accounting 10.99.88.77

Success.

DGS-3627:5#
```

enable dhcp_server

Purpose	Used to enable the DHCP function on the switch.
Syntax	enable dhcp_server
Description	This command, along with the disable dhcp_server will enable and disable the DHCP server function without affecting configurations.
Parameters	None.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To enable DHCP server:

```
DGS-3627:5# enable dhcp_server
Command: enable dhcp_server

Success.

DGS-3627:5#
```

disable dhcp_server

Purpose	Used to disable the DHCP function on the switch.
Syntax	disable dhcp_server
Description	This command, along with the enable dhcp_server will enable and disable the DHCP server function without affecting configurations.
Parameters	None.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To disable the DHCP server:

```
DGS-3627:5# disable dhcp_server
Command: disable dhcp_server

Success.

DGS-3627:5#
```

show dhcp_server

Purpose	Used to display the DHCP server settings.
Syntax	show dhcp_server
Description	This command will display the DHCP server settings for its Global state, ping packet count and ping timeout.
Parameters	None.
Restrictions	None.

Example usage:

To display the DHCP server settings:

```
DGS-3627:5#show dhcp_server
Command:show dhcp_server

DHCP Server Global State: Disable
Ping Packet Number      : 2
Ping Timeout            : 500 ms

DGS-3627:5#
```

create dhcp excluded_address begin_address

Purpose	Used to configure IP addresses that will be excluded from the DHCP Server pool of addresses.
Syntax	create dhcp excluded_address begin_address <ipaddr> end_address <ipaddr>
Description	This command will allow the user to set an IP address, or a range of IP addresses that are NOT to be included in the range of IP addresses that the Switch will allot to clients requesting DHCP service.
Parameters	<i>begin_address <ipaddr></i> - Enter the beginning IP address of the range of IP addresses to be excluded from the DHCP pool. <i>end_address <ipaddr></i> - Enter the ending IP address of the range of IP addresses to be excluded from the DHCP pool.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To display the multicast range Trinity:

```
DGS-3627:5#create dhcp excluded_address begin_address 10.10.10.1
end_address 10.10.10.10
Command: create dhcp excluded_address begin_address 10.10.10.1
end_address 10.10.10.10

Success.

DGS-3627:5#
```

delete dhcp excluded_address begin_address

Purpose	Used to delete IP addresses that have been configured as excluded from the DHCP Server pool of addresses.
Syntax	delete dhcp excluded_address begin_address <ipaddr> end_address <ipaddr>
Description	This command will allow the user to delete a previously set IP address, or a range of IP addresses that are NOT to be included in the range of IP addresses that the Switch will allot to clients requesting DHCP service.
Parameters	<i>begin_address <ipaddr></i> - Enter the beginning IP address of the range of IP addresses to be deleted from the excluded IP address list, from the DHCP pool. <i>end_address <ipaddr></i> - Enter the ending IP address of the range of IP addresses to be deleted from the excluded IP address list, from the DHCP pool.

delete dhcp excluded_address begin_address

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

Example usage:

To display the multicast range accounting:

```
DGS-3627:5#delete dhcp excluded_address begin_address 10.10.10.1
end_address 10.10.10.10
Command: delete dhcp excluded_address begin_address 10.10.10.1
end_address 10.10.10.10

Success.

DGS-3627:5#
```

show dhcp excluded_address

Purpose	Used to display the excluded IP addresses of the DHCP server function.
Syntax	show dhcp excluded_address
Description	This command is used to display the excluded IP addresses of the DHCP server function.
Parameters	None.
Restrictions	None.

Example usage:

To display the DHCP server settings:

```
DGS-3627:5#show dhcp excluded_address
Command:show dhcp excluded_address

Index      Begin Address      End Address
-----
1          192.168.0.1        192.168.0.100
2          10.10.10.10        10.10.10.10

Total Entries : 2

DGS-3627:5#
```

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
config limited multicast address	<portlist> {from <multicast_ipaddr> to <multicast_ipaddr> access [permit deny] state [enable disable]}
delete limited multicast address	[all <portlist>]
show limited multicast address	{<portlist>}
create multicast_range	<range_name 32> from <multicast_ipaddr> to <multicast_ipaddr>
delete multicast_range	[<range_name 32> all]
show multicast_range	{<range_name 32>}
config limited_multicast_addr	ports <portlist> {add multicast_range <range_name 32> delete multicast_range [<range_name 32> all] {access [permit deny] state [enable disable]}}
show limited_multicast_addr	{ports <portlist>}

Each command is listed in detail in the following sections.

config limited multicast address

Purpose	Used to configure limited IP multicast address range.
Syntax	config limited multicast address <portlist> {from <multicast_ipaddr> to <multicast_ipaddr> access [permit deny] state [enable disable]}
Description	The config limited multicast address command allows the user to configure the multicast address range, access level, and state.
Parameters	<p><i><portlist></i> - A port or range of ports to config the limited multicast address. The beginning and end of the port list range are separated by a dash. Non-contiguous portlist entries are separated by a comma. (ex:1-3,7-9)</p> <p><i>from</i> - Enter the lowest multicast IP address of the range.</p> <p><i>to</i> - Enter the highest multicast IP address of the range.</p> <p><i>access</i> - Use the access field to either <i>permit</i> or <i>deny</i> to limit or grant access to a specified range of Multicast addresses on a particular port or range of ports.</p> <p><i>state</i> - This parameter allows the user to <i>enable</i> or <i>disable</i> the limited multicast address range on a specific port or range of ports.</p>
Restrictions	Only administrator-level and operator-level users can issue this command. This command is used as a backwards compatible command for legacy devices and firmware.

Example usage:

To configure the limited multicast address on ports 1-3:

```
DGS-3627:5#config limited multicast address 1-3 from 224.1.1.1 to 224.1.1.2 access
permit state enable
Command: config limited multicast address 1-3 from 224.1.1.1 to 224.1.1.2 access
```

```
permit state enable
```

```
Success.
```

```
DGS-3627:5#
```

delete limited multicast address

Purpose	Used to delete Limited IP multicast address range.
Syntax	delete limited multicast address [all <portlist>]
Description	The delete limited multicast address command allows the user to delete all multicast address ranges or a selected range based on what port or ports the range has been assigned to.
Parameters	<i>all</i> - Allows the user to delete all limited multicast addresses that have been configured on the Switch. <i><portlist></i> - Allows the user to delete only those multicast address ranges that have been assigned to a particular port or range of ports. The beginning and end of the port list range are separated by a dash. Non-contiguous portlist entries are separated by a comma. (ex: 1-3,7-9)
Restrictions	Only administrator-level and operator-level users can issue this command. This command is used as a backwards compatible command for legacy devices.

Example usage:

To delete the limited multicast address on ports 1-3:

```
DGS-3627:5#delete limited multicast address 1-3
```

```
Command: delete limited multicast address 1-3
```

```
Success.
```

```
DGS-3627:5#
```

show limited multicast address

Purpose	Used to show per-port limited IP multicast address range.
Syntax	show limited multicast address {<portlist>}
Description	The show limited multicast address command allows users to show multicast address range by ports.
Parameters	<i><portlist></i> A port or range of ports on which the limited multicast address range to be shown has been assigned. The beginning and end of the port list range are separated by a dash. Non-contiguous portlist entries are separated by a comma. (ex: 1-3,7-9)
Restrictions	None. This command is used as a backwards compatible command for legacy devices.

Example usage:

To show the limited multicast address on ports 1-2:

```
DGS-3627:5#show limited multicast address 1-2
```

```
Command: show limited multicast address 1-2
```



```

Port : 1
State : Disabled
Access : None

No.      Name      From      To
-----  -
Port : 2
State : Disabled
Access : None

No.      Name      From      To
-----  -

DGS-3627:5#
    
```

create multicast_range	
Purpose	Used to create a range of multicast IP addresses that will be specified under a given name.
Syntax	create multicast range <range_name 32> from <multicast_ipaddr> to <multicast_ipaddr>
Description	This command will create a multicast range of IP addresses that will be specified under a given name. Once created, this range name can be added to the config limited_multicast_addr command, therefore setting a list of multicast addresses that will be permitted or denied by the switch.
Parameters	<p><i><range_name 32></i> - Enter a name of up to 32 alphanumeric characters that will be used to identify this multicast range.</p> <p><i>from <multicast_ipaddr></i> - Enter the beginning IP address of the multicast range.</p> <p><i>to <multicast_ipaddr></i> - Enter the ending IP address of the multicast range.</p>
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To create the multicast range “accounting”:

```

DGS-3627:5#create multicast range accounting from 224.19.62.34 to
224.19.62.200
Command: create multicast range accounting from 224.19.62.34 to
224.19.62.200

Success.

DGS-3627:5#
    
```

delete multicast_range	
Purpose	Used to delete a range of multicast IP addresses that will be specified under a given name.
Syntax	delete multicast range [<range_name 32> all]
Description	This command will delete a multicast range that was created with the

delete multicast_range

	create multicast_range command.
Parameters	<p><i><range_name 32></i> - Enter a name of up to 32 alphanumeric characters that will be used to identify this multicast range to be deleted.</p> <p><i>all</i> – Use this parameter to delete all multicast address ranges configured on the Switch.</p>
Restrictions	Only administrator-level and operator-level users can issue this command.

DGS-3627:5#delete multicast range accounting

Command: create multicast range accounting

Success.

DGS-3627:5#

show multicast_range

Purpose	Used to display a range of multicast IP addresses that are specified under a given name.
Syntax	show multicast range [<i><range_name 32></i> all]
Description	This command will display a multicast range that was created with the create multicast_range command.
Parameters	<p><i><range_name 32></i> - Enter a name of up to 32 alphanumeric characters that will be used to identify this multicast range to be displayed.</p> <p>Entering this command without the specified range_name will display all multicast ranges created on the Switch.</p>
Restrictions	None.

Example usage:

To display the multicast range “accounting”:

DGS-3627:5#show multicast range accounting

Command:show multicast range accounting

No.	Name	From	To
1	Trinity	224.19.62.34	224.19.62.200

Total Entries: 1

DGS-3627:5#

config limited_multicast_addr

Purpose	Used to add or delete ports to a previously created multicast address range and then to give that range access to or denial from the Switch.
Syntax	config limited_multicast_addr ports <i><portlist></i> [add multicast_range <i><range_name 32></i> delete multicast_range [<i><range_name 32></i> all] { access [permit deny] state [enable disable]}]

config limited_multicast_addr

Description	This command will perform three tasks for the multicast range. It may add switch ports to the range, delete ports from the multicast range and it may also give these multicast addresses access to the switch, or configure them to be restricted from accessing the Switch.
Parameters	<p><i>ports <portlist></i> - Used to add a list of ports to the multicast range. The beginning and end of the port list range are separated by a dash. Non-contiguous portlist entries are separated by a comma. (ex: 1-3,7-9)</p> <p><i>add</i> – Use this parameter to add ports to the multicast range specified by the following parameter.</p> <ul style="list-style-type: none"> <i>multicast_range <range_name 32></i> - Enter a name of up to 32 alphanumeric characters that will be used to identify this multicast range to be configured. <p><i>delete</i> – Use this parameter to delete ports from the multicast range specified by the following parameters.</p> <ul style="list-style-type: none"> <i>multicast_range <range_name 32></i> - Enter a name of up to 32 alphanumeric characters that will be used to identify this multicast range to be configured. <i>all</i> – Use this parameter to delete these ports from all multicast ranges. <p><i>access</i> – Use this parameter to grant or deny permission of the multicast addresses for the ports based on the following parameters.</p> <ul style="list-style-type: none"> <i>permit</i> – Use this parameter to grant permission to the switch for this multicast range. <i>deny</i> – Use this parameter to deny access from the switch for this multicast range. <p><i>state [enable disable]</i> – Use these parameters to enable or disable this multicast configuration.</p>
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To add ports to the multicast range:

```
DGS-3627:5#config limited_multicast_addr ports 5-8 add multicast_range
accounting
Command: config limited_multicast_addr ports 5-8 add multicast_range accounting

Success.

DGS-3627:5#
```

Example usage:

To grant the multicast range permission to access the ports:

```
DGS-3627:5#config limited_multicast_addr ports 5-8 access permit
Command: config limited_multicast_addr ports 5-8 add access permit

Success.

DGS-3627:5#
```

show limited_multicast_addr

Purpose	Used to display the limited multicast address range on a per port basis.
Syntax	show limited_multicast_addr {ports <portlist>}
Description	This command will display the limited multicast address range on a per port basis.
Parameters	<i>ports <portlist></i> - Enter a port or list of ports to be displayed. The beginning and end of the port list range are separated by a dash. Non-contiguous portlist entries are separated by a comma. (ex: 1-3,7-9) Entering this command without the portlist parameter will display the limited multicast range for all ports on the switch.
Restrictions	None.

Example usage:

To display the multicast range Trinity:

```
DGS-3627:5#show limited_multicast_addr ports 5
Command: show limited_multicast_addr ports 5

Port   : 5
State  : Disabled
Access : None

No.    Name                From                To
----  -
1      accounting          224.19.62.34       224.19.62.200

Total Entries: 1

DGS-3627:5#
```

802.1X COMMANDS

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	
show 802.1x auth_state	{ports [<portlist> all]}
show 802.1x 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> enable_reauth [enable disable]}]
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> key <passwd 32> [default {auth_port <udp_port_number 1-65535> acct_port <udp_port_number 1-65535>}]
config radius delete	<server_index 1-3>
config radius	<server_index 1-3> {ipaddress <server_ip> key <passwd 32> [auth_port <udp_port_number 1-65535> acct_port <udp_port_number 1-65535>}]
show radius	
show acct_client	
show auth_client	
show auth_diagnostics	{ports [<portlist> all]}
show auth_session statistics	{ports [<portlist> all]}
show auth_statistics	{ports [<portlist> all]}
create 802.1x user	<username 15>
show 802.1x user	
delete 802.1x user	
create 802.1x guest_vlan	<vlan_name 32>
config 802.1x guest_vlan ports	[<portlist> all] state [enable disable]
show 802.1x guest_vlan	
delete 802.1x guest_vlan	<vlan_name 32>

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	The enable 802.1x command enables 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-level and operator-level users can issue this command.

Example usage:

To enable 802.1x switch wide:

```
DGS-3627:5#enable 802.1x
Command: enable 802.1x

Success.

DGS-3627:5#
```

disable 802.1x

Purpose	Used to disable the 802.1x server on the Switch.
Syntax	disable 802.1x
Description	The disable 802.1x command is used to disable 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-level and operator-level users can issue this command.

Example usage:

To disable 802.1x on the Switch:

```
DGS-3627:5#disable 802.1x
Command: disable 802.1x

Success.

DGS-3627:5#
```

show 802.1x auth_configuration

Purpose	Used to display the current configuration of the 802.1x server on the Switch.
Syntax	show 802.1x auth_configuration {ports [<portlist> all]}
Description	The show 802.1x auth_configuration command is used to display the 802.1x Port-based or MAC-based Network Access control local users currently configured on the Switch.
Parameters	<i>ports</i> <portlist> – Specifies a port or range of ports to view. The beginning and end of the port list range are separated by a dash. Non-contiguous portlist entries are separated by a comma. (ex: 1-3,7-9) <i>all</i> – Specify to view all ports. The following details are displayed:

show 802.1x auth_configuration

802.1x Enabled / Disabled – Shows the current status of 802.1x functions on the Switch.

Authentication Mode – Shows the authentication mode, whether it be by MAC address or by port.

Authentication Protocol: Radius_Eap – Shows the authentication protocol suite in use between the Switch and a RADIUS server. May read *Radius_Eap* or *Radius_Pap*.

Port number – Shows the physical port number on the Switch.

Capability: Authenticator/None – Shows the capability of 802.1x functions on the port number displayed above. There are two 802.1x capabilities that can be set on the Switch: Authenticator and None.

AdminCtlDir: Both / In – Shows whether a controlled Port that is unauthorized will exert control over communication in both receiving and transmitting directions, or just the receiving direction.

OpenCtlDir: Both / In – Shows whether a controlled Port that is unauthorized will exert control over communication in both receiving and transmitting directions, or just the receiving direction.

Port Control: ForceAuth / ForceUnauth / Auto – Shows the administrative control over the port's authorization status. ForceAuth forces the Authenticator of the port to become Authorized. ForceUnauth forces the port to become Unauthorized.

QuietPeriod – Shows the time interval between authentication failure and the start of a new authentication attempt.

TxPeriod – Shows the time to wait for a response from a supplicant (user) to send EAP Request / Identity packets.

SuppTimeout – Shows the time to wait for a response from a supplicant (user) for all EAP packets, except for the Request / Identity packets.

ServerTimeout – Shows the length of time to wait for a response from a Radius server.

MaxReq – Shows the maximum number of times to retry sending packets to the supplicant.

ReAuthPeriod – Shows the time interval between successive re-authentications.

ReAuthenticate: Enabled / Disabled – Shows whether or not to re-authenticate.

Restrictions None.

Example usage:

To display the 802.1x authentication states:

```
DGS-3627:5#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
```

```
Port number      : 1
Capability        : None
AdminCrIDir      : Both
OpenCrIDir       : Both
Port Control      : Auto
QuietPeriod       : 60 sec
TxPeriod          : 30 sec
SuppTimeout       : 30 sec
ServerTimeout     : 30 sec
MaxReq            : 2 times
ReAuthPeriod      : 3600 sec
ReAuthenticate    : Disabled
```

CTRL+C **ESC** **q** Quit **SPACE** **n** Next Page **Enter** Next Entry **a** All

show 802.1x auth_state

Purpose	Used to display the current authentication state of the 802.1x server on the Switch.
Syntax	show 802.1x auth_state {ports [<portlist> all]}
Description	The show 802.1x auth_state command is used to display the current authentication state of the 802.1x Port-based or MAC-based Network Access Control server application on the Switch.
Parameters	<p><i>ports <portlist></i> – Specifies a port or range of ports to be viewed. The beginning and end of the port list range are separated by a dash. Non-contiguous portlist entries are separated by a comma. (ex: 1-3,7-9)</p> <p><i>all</i> – Specify to view all ports.</p> <p>The following details what is displayed:</p> <p>Port number – Shows the physical port number on the Switch.</p> <p>Auth PAE State: Initialize / Disconnected / Connecting / Authenticating / Authenticated / Held / ForceAuth / ForceUnauth – Shows the current state of the Authenticator PAE.</p> <p>Backend State: Request / Response / Fail / Idle / Initialize / Success / Timeout – Shows the current state of the Backend Authenticator.</p> <p>Port Status: Authorized / Unauthorized – Shows the result of the authentication process. Authorized means that the user was authenticated, and can access the network. Unauthorized means that the user was not authenticated, and cannot access the network.</p>
Restrictions	None.

Example usage:

To display the 802.1x auth state for Port-based 802.1x:

```
DGS-3627:5#show 802.1x auth_state
Command: show 802.1x auth_state
```

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
6	ForceAuth	Success	Authorized
7	ForceAuth	Success	Authorized
8	ForceAuth	Success	Authorized
9	ForceAuth	Success	Authorized
10	ForceAuth	Success	Authorized
11	ForceAuth	Success	Authorized
12	ForceAuth	Success	Authorized
13	ForceAuth	Success	Authorized
14	ForceAuth	Success	Authorized
15	ForceAuth	Success	Authorized
16	ForceAuth	Success	Authorized
17	ForceAuth	Success	Authorized
18	ForceAuth	Success	Authorized
19	ForceAuth	Success	Authorized
20	ForceAuth	Success	Authorized

CTRL+C **ESC** **q** Quit **SPACE** **n** Next Page **Enter** Next Entry **a** All

Example usage:

To display the 802.1x auth state for MAC-based 802.1x:

```
DGS-3627:5#show 802.1x auth_state
Command: show 802.1x auth_state

Port number : 1
Index   MAC Address      Auth PAE State   Backend State    Port Status
-----  -
1       00-08-02-4E-DA-FA  Authenticated   Idle             Authorized
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
CTRL+C | ESC | q Quit | SPACE | n Next Page | Enter Next Entry | a All
```

config 802.1x auth_mode	
Purpose	Used to configure the 802.1x authentication mode on the Switch.
Syntax	config 802.1x auth_mode {port_based mac_based}
Description	The config 802.1x auth_mode command is used to enable either the port-based or MAC-based 802.1x authentication feature on the Switch.
Parameters	<i>[port_based mac_based]</i> – The Switch allows users to authenticate 802.1x by either port or MAC address.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure 802.1x authentication by MAC address:

```
DGS-3627:5#config 802.1x auth_mode mac_based
Command: config 802.1x auth_mode mac_based

Success.

DGS-3627:5#
```

config 802.1x capability ports	
Purpose	Used to configure the 802.1x capability of a range of ports on the Switch.
Syntax	config 802.1x capability ports [<portlist> all] [authenticator none]

config 802.1x capability ports

Description	The config 802.1x command has four capabilities that can be set for each port. Authenticator, Supplicant, Authenticator and Supplicant, and None.
Parameters	<p><i><portlist></i> – Specifies a port or range of ports to be configured. The beginning and end of the port list range are separated by a dash. Non-contiguous portlist entries are separated by a comma. (ex: 1-3,7-9)</p> <p><i>all</i> – Specifies all of the ports on the Switch.</p> <p><i>authenticator</i> – A user must pass the authentication process to gain access to the network.</p> <p><i>none</i> – The port is not controlled by the 802.1x functions.</p>
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To configure 802.1x capability on ports 1-10:

```
DGS-3627:5#config 802.1x capability ports 1 – 10 authenticator
Command: config 802.1x capability ports 1 – 10 authenticator

Success.

DGS-3627:5#
```

config 802.1x auth_parameter

Purpose	Used to configure the 802.1x authentication parameters on a range of ports. The default parameter will return all ports in the specified range to their default 802.1x settings.
Syntax	config 802.1x auth_parameter ports [<i><portlist></i> <i>all</i>] [<i>default</i> <i>{direction</i> [<i>both</i> <i>in</i>] <i>port_control</i> [<i>force_unauth</i> <i>auto</i> <i>force_auth</i>] <i>quiet_period</i> <i><sec 0-65535></i> <i>tx_period</i> <i><sec 1-65535></i> <i>supp_timeout</i> <i><sec 1-65535></i> <i>server_timeout</i> <i><sec 1-65535></i> <i>max_req</i> <i><value 1-10></i> <i>reauth_period</i> <i><sec 1-65535></i> <i>enable_reauth</i> [<i>enable</i> <i>disable</i>]}]
Description	The config 802.1x auth_parameter command is used to configure the 802.1x Authentication parameters on a range of ports. The default parameter will return all ports in the specified range to their default 802.1x settings.
Parameters	<p><i><portlist></i> – Specifies a port or range of ports to be configured. The beginning and end of the port list range are separated by a dash. Non-contiguous portlist entries are separated by a comma. (ex: 1-3,7-9)</p> <p><i>all</i> – Specifies all of the ports on the Switch.</p> <p><i>default</i> – Returns all of the ports in the specified range to their 802.1x default settings.</p> <p><i>direction</i> [<i>both</i> <i>in</i>] – Determines whether a controlled port blocks communication in both the receiving and transmitting directions, or just the receiving direction.</p> <p><i>port_control</i> – Configures the administrative control over the authentication process for the range of ports. The user has the following authentication options:</p> <ul style="list-style-type: none"> <i>force_auth</i> – Forces the Authenticator for the port to become authorized. Network access is allowed.

config 802.1x auth_parameter

- *auto* – Allows the port's status to reflect the outcome of the authentication process.
- *force_unauth* – Forces the Authenticator for the port to become unauthorized. Network access will be blocked.

quiet_period <sec 0-65535> – Configures the time interval between authentication failure and the start of a new authentication attempt.

tx_period <sec 1-65535> - Configures the time to wait for a response from a supplicant (user) to send EAP Request/Identity packets.

supp_timeout <sec 1-65535> - Configures the time to wait for a response from a supplicant (user) for all EAP packets, except for the Request/Identity packets.

server_timeout <sec 1-65535> - Configure the length of time to wait for a response from a RADIUS server.

max_req <value 1-10> – Configures the number of times to retry sending packets to a supplicant (user).

reauth_period <sec 1-65535> – Configures the time interval between successive re-authentications.

enable_reauth [*enable* | *disable*] – Determines whether or not the Switch will re-authenticate. Enabled causes re-authentication of users at the time interval specified in the Re-authentication Period field, above.

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

Example usage:

To configure 802.1x authentication parameters for ports 1 to 10:

```
DGS-3627:5#config 802.1x auth_parameter ports 1-10 direction both
Command: config 802.1x auth_parameter ports 1-10 direction both

Success.

DGS-3627:5#
```

config 802.1x init

Purpose	Used to initialize the 802.1x function on a range of ports.
Syntax	config 802.1x init {port_based ports [<portlist> all] mac_based [ports] [<portlist> all] {mac_address <macaddr>}}
Description	The config 802.1x init command is used to immediately initialize the 802.1x functions on a specified range of ports or for specified MAC addresses operating from a specified range of ports.
Parameters	<p><i>port_based</i> – This instructs the Switch to initialize 802.1x functions based only on the port number. Ports approved for initialization can then be specified.</p> <p><i>mac_based</i> – This instructs the Switch to initialize 802.1x functions based only on the MAC address. MAC addresses approved for initialization can then be specified.</p> <p><i>ports</i> <portlist> – Specifies a port or range of ports to be configured. The beginning and end of the port list range are separated by a dash. Non-contiguous portlist entries are separated by a comma. (ex: 1-3,7-9)</p> <p><i>all</i> – Specifies all of the ports on the Switch.</p> <p><i>mac_address</i> <macaddr> - Enter the MAC address to be initialized.</p>
Restrictions	Only administrator-level and operator-level users can issue this

config 802.1x init

command.

Example usage:

To initialize the authentication state machine of all ports:

```
DGS-3627:5# config 802.1x init port_based ports all
Command: config 802.1x init port_based ports all

Success.

DGS-3627:5#
```

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	The config 802.1x reauth command is used to re-authenticate a previously authenticated device based on port number or MAC address.
Parameters	<p><i>port_based</i> – 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.</p> <p><i>mac_based</i> – 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.</p> <p><i>ports <portlist></i> – Specifies a port or range of ports to be re-authorized. The beginning and end of the port list range are separated by a dash. Non-contiguous portlist entries are separated by a comma. (ex:1-3,7-9)</p> <p><i>all</i> – Specifies all of the ports on the Switch.</p> <p><i>mac_address <macaddr></i> - Enter the MAC address to be re-authorized.</p>
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To configure 802.1x reauthentication for ports 1-18:

```
DGS-3627:5#config 802.1x reauth port_based ports 1-11
Command: config 802.1x reauth port_based ports 1-11

Success.

DGS-3627:5#
```

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> key <passwd 32> [default {auth_port <udp_port_number 1-65535> acct_port <udp_port_number 1-65535>}]

config radius add

Description	The config radius add command is used to configure the settings the Switch will use to communicate with a RADIUS server.
Parameters	<p><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.</p> <p><server_ip> – The IP address of the RADIUS server.</p> <p>key – Specifies that a password and encryption key will be used between the Switch and the RADIUS server.</p> <ul style="list-style-type: none"> <passwd 32> – The shared-secret key used by the RADIUS server and the Switch. Up to 32 characters can be used. <p>default – Uses the default udp port number in both the “auth_port” and “acct_port” settings.</p> <p>auth_port <udp_port_number 1-65535> – The UDP port number for authentication requests. The default is 1812.</p> <p>acct_port <udp_port_number 1-65535> – The UDP port number for accounting requests. The default is 1813.</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure the RADIUS server communication settings:

```
DGS-3627:5#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-3627:5#
```

config radius delete

Purpose	Used to delete a previously entered RADIUS server configuration.
Syntax	config radius delete <server_index 1-3>
Description	The config radius delete 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 three 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-3627:5#config radius delete 1
Command: config radius delete 1

Success.

DGS-3627:5#
```

config radius

Purpose	Used to configure the Switch's RADIUS settings.
Syntax	config radius <server_index 1-3> {ipaddress <server_ip> key <passwd 32> auth_port <udp_port_number 1-65535> acct_port <udp_port_number 1-65535>}
Description	The config radius command is used to configure the Switch's RADIUS settings.
Parameters	<p><i><server_index 1-3></i> – 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.</p> <p><i>ipaddress <server_ip></i> – The IP address of the RADIUS server.</p> <p><i>key</i> – Specifies that a password and encryption key will be used between the Switch and the RADIUS server.</p> <ul style="list-style-type: none"> <i><passwd 32></i> – The shared-secret key used by the RADIUS server and the Switch. Up to 32 characters can be used. <p><i>auth_port <udp_port_number 1-65535></i> – The UDP port number for authentication requests. The default is 1812.</p> <p><i>acct_port <udp_port_number 1-65535></i> – The UDP port number for accounting requests. The default is 1813.</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure the RADIUS settings:

```
DGS-3627:5#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-3627:5#
```

show radius

Purpose	Used to display the current RADIUS configurations on the Switch.
Syntax	show radius
Description	The show radius 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-3627:5#show radius
Command: show radius

Index  IP Address      Auth-Port  Acct-Port  Status  Key
-----  -----
1      10.1.1.1        1812       1813       Active  switch
2      20.1.1.1        1800       1813       Active  dgs3627
3      30.1.1.1        1812       1813       Active  dlink

Total Entries : 3

DGS-3627:5#
```

show acct_client

Purpose	Used to display the current RADIUS accounting client.
Syntax	show acct_client
Description	The show acct_client command is used to display the current RADIUS accounting client currently configured on the Switch.
Parameters	None.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To view the current RADIUS accounting client:

```
DGS-3627:5#show acct_client
Command: show acct_client

radiusAcctClient
-----
radiusAcctClientInvalidServerAddresses    0
radiusAcctClientIdentifier                D-Link

radiusAuthServerEntry                    0
-----
radiusAccServerIndex                      1
radiusAccServerAddress                    10.53.13.199
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 Enter Next Entry a All
```

show auth_client

Purpose	Used to display the current RADIUS authentication client.
---------	---

show auth_client

Syntax	show auth_client
Description	The show auth_client command is used to display the current RADIUS authentication client currently configured on the Switch.
Parameters	None.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To view the current RADIUS authentication client:

```
DGS-3627:5#show auth_client
Command: show auth_client

radiusAuthClient
radiusAuthClientInvalidServerAddresses      0
radiusAuthClientIdentifier                  D-Link

radiusAuthServerEntry                       0
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 Enter Next Entry a All
```

show auth_diagnostics

Purpose	Used to display the current authentication diagnostics.
Syntax	show auth_diagnostics {ports [<portlist> all]}
Description	The show auth_diagnostics command is used to display the current authentication diagnostics of the Switch on a per port basis.
Parameters	<i>ports <portlist></i> – Specifies a port or range of ports to be displayed. The beginning and end of the port list range are separated by a dash. Non-contiguous portlist entries are separated by a comma. (ex: 1-3,7-9)
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To display the current authentication diagnostics for port 1:

```
DGS-3627:5#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 h Next Page Enter Next Entry a All
    
```

show auth_session_statistics

Purpose	Used to display the current authentication session statistics.
Syntax	show auth_session_statistics {ports [<portlist> all]}
Description	The show auth_session_statistics command is used to display the current authentication session statistics of the Switch on a per port basis.
Parameters	<p><i>ports <portlist></i> – Specifies a port or range of ports to be viewed. The beginning and end of the port list range are separated by a dash. Non-contiguous portlist entries are separated by a comma. (ex: 1-3,7-9)</p> <p><i>all</i> – Specifies that all ports will be viewed.</p>
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To display the current authentication session statistics for port 1:

```

DGS-3627:5#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          Marcello

CTRL+C ESC q Quit SPACE h Next Page Enter Next Entry a All
    
```

show auth_statistics

Purpose	Used to display the current authentication statistics.
Syntax	show auth_statistics {ports <portlist> all}
Description	The show auth_statistics command is used to display the current authentication statistics of the Switch on a per port basis.
Parameters	<i>ports <portlist></i> – Specifies a port or range of ports. The beginning and end of the port list range are separated by a dash. Non-contiguous portlist entries are separated by a comma. (ex: 1-3,7-9)
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To display the current authentication statistics for port 1:

```
DGS-3627:5#show auth_statistics ports 1
Command: show auth_statistics ports 1

Port 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 [Enter] Next Entry [a] All
```

create 802.1x user

Purpose	Used to create a new 802.1x user.
Syntax	create 802.1x user <username 15>
Description	The create 802.1x user command is used to create new 802.1x users.
Parameters	<i><username 15></i> – A username of up to 15 alphanumeric characters in length.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To create an 802.1x user:

```
DGS-3627:5#create 802.1x user ctsnow
Command: create 802.1x user ctsnow

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

DGS-3627:5#
```

show 802.1x user

Purpose	Used to display the 802.1x user accounts on the Switch.
Syntax	show 802.1x user
Description	The show 802.1x user command is used to display the 802.1x Port-based or MAC-based Network Access control local users currently configured on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To view 802.1X users currently configured on the Switch:

```
DGS-3627:5#show 802.1x user
```

```
Command: show 802.1x user
```

```
Current Accounts:
```

```
Username      Password
-----      -
```

```
ctsnow       Tibeirus
```

```
Total entries: 1
```

```
DGS-3627:5#
```

delete 802.1x user

Purpose	Used to delete an 802.1x user account on the Switch.
Syntax	delete 802.1x user <username 15>
Description	The delete 802.1x user command is used to delete the 802.1x Port-based or MAC-based Network Access control local users currently configured on the Switch.
Parameters	<username 15> – A username can be as many as 15 alphanumeric characters.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To delete 802.1x users:

```
DGS-3627:5#delete 802.1x user ctsnow
```

```
Command: delete 802.1x user ctsnow
```

```
Success.
```

```
DGS-3627:5#
```

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	The create 802.1x guest_vlan command is used to configure a pre-defined VLAN as a 802.1x Guest VLAN. Guest 802.1X VLAN clients are those who have not been authorized for 802.1x or they haven't

create 802.1x guest_vlan

	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 an 802.1x Guest VLAN. This VLAN must have first been created with the create vlan command mentioned earlier in this manual.
Restrictions	Only administrator-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-3627:5#create 802.1x guest_vlan Tiberius
Command: create 802.1x guest_vlan Tiberius

Success.

DGS-3627:5#
```

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	The config 802.1x guest_vlan ports command is used to configure ports to be enabled or disabled for the 802.1x guest VLAN.
Parameters	<p><portlist> - Specify a port or range of ports to be configured for the 802.1x Guest VLAN. The beginning and end of the port list range are separated by a dash. Non-contiguous portlist entries are separated by a comma. (ex: 1-3,7-9)</p> <p><i>all</i> – Specify this parameter to configure all ports for the 802.1x Guest VLAN.</p> <p><i>state [enable disable]</i> – Use these parameters to enable or disable port listed here as enabled or disabled for the 802.1x Guest VLAN.</p>
Restrictions	Only administrator-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 default VLAN.

Example usage:

To configure the ports for a previously created 802.1x Guest VLAN as enabled.

```
DGS-3627:5#config 802.1x guest_vlan ports 1-5 state enable
Command: config 802.1x guest_vlan ports 1-5 state enable

Success.

DGS-3627:5#
```

show 802.1x guest_vlan

Purpose	Used to view the configurations for a 802.1x Guest VLAN.
Syntax	show 802.1x guest_vlan
Description	The show 802.1x guest_vlan command is used to display the settings for the VLAN that has been enabled as an 802.1x Guest VLAN. Guest 802.1X 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	None.

Example usage:

To display the configurations for a previously created 802.1x Guest VLAN.

```
DGS-3627:5#show 802.1x guest_vlan
Command: show 802.1x guest_vlan

Guest VLAN Setting
-----
Guest VLAN : Tiberius
Enable guest VLAN ports: 5-8

DGS-3627:5#
```

delete 802.1x guest_vlan

Purpose	Used to delete an 802.1x Guest VLAN.
Syntax	delete 802.1x guest_vlan <vlan_name 32>
Description	The delete 802.1x guest_vlan command is used to delete a 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	Only administrator-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-3627:5#delete 802.1x guest_vlan Zira
Command: delete 802.1x guest_vlan Zira

Success.

DGS-3627:5#
```

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.

Access profiles allow you to establish criteria to determine whether or not the Switch will forward packets based on the information contained in each packet's header. These criteria can be specified on a VLAN-by-VLAN basis.

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 you want to deny all traffic to the subnet 10.42.73.0 to 10.42.73.255, you must first **create** an access profile that instructs the Switch to examine all of the relevant fields of each frame:

CREATE ACCESS_PROFILE PROFILE_ID 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**. 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 you want to restrict traffic, you must use the **deny** parameter.

Now that an access profile has been created, you must add the criteria the Switch will use to decide if a given frame should be forwarded or filtered. Here, we want to filter any packets that have an IP source address between 10.42.73.0 and 10.42.73.255:

config access_profile profile_id 1 add access_id 1 ip source_ip 10.42.73.1 port 1 deny

Here 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, you can assign an **access_id** that both identifies the rule and establishes a priority within the list of rules. A lower **access_id** gives the rule a higher priority. In case of a conflict in the rules entered for an access profile, the rule with the highest priority (lowest **access_id**) will take precedence.

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. Finally, 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.

Due to a chipset limitation, the Switch supports a maximum of fourteen access profiles. The rules used to define the access profiles are limited to a total of 1792 rules for the Switch. One rule can support ACL per port or per portmap.

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

Command	Parameters
create access_profile profile_id	<value 1-14> [ethernet {vlan source_mac <macmask 000000000000-ffffffff> destination_mac <macmask 000000000000-ffffffff> 802.1p ethernet_type} ip {vlan source_ip_mask <netmask> destination_ip_mask <netmask> dscp [icmp {type code} igmp [type] tcp {src_port_mask <hex 0x0-0xffff> dst_port_mask <hex 0x0-0xffff> flag_mask [all {urg ack psh rst syn fin}]} udp {src_port_mask <hex 0x0-0xffff> dst_port_mask <hex 0x0-0xffff>} protocol_id_mask <hex 0x0-0xff> {user_define_mask <hex 0x0-0xffffffff>}}] packet_content {offset_chunk_1 <value 0-31> <hex 0x0-0xffffffff> offset_chunk_2 <value 0-31> <hex 0x0-0xffffffff> offset_chunk_3 <value 0-31> <hex 0x0-0xffffffff> offset_chunk_4 <value 0-31> <hex 0x0-0xffffffff>} ipv6 {[class flowlabel] source_ipv6_mask <ipv6mask> destination_ipv6_mask <ipv6mask>}]}
delete access_profile	{profile_id <value 1-14> all}
config access_profile profile_id	<value 1-14> [add access_id [auto_assign <value 1-128>] [ethernet {vlan <vlan_name 32> source_mac <macaddr 000000000000-ffffffff> destination_mac <macaddr 000000000000-ffffffff> 802.1p <value 0-7> ethernet_type <hex 0x0-0xffff>} port [<portlist> all] [permit {priority <value 0-7> replace_priority} rx_rate {no_limit <value 1-156249>}] counter [enable

Command	Parameters
	disable}] mirror deny] ip {vlan <vlan_name 32> source_ip <ipaddr> destination_ip <ipaddr> dscp <value 0-63> [icmp {type <value 0-255> code <value 0-255>} igmp {type <value 0-255>} tcp {src_port <value 0-65535> dst_port <value 0-65535> urg ack psh rst syn fin} udp {src_port <value 0-65535> dst_port <value 0-65535>} protocol_id <value 0 - 255> {user_define <hex 0x0-0xffffffff>}}] port [<portlist> all] [permit {priority <value 0-7> {replace_priority} rx_rate {no_limit <value 1-156249>}}] counter [enable disable}] mirror deny] packet_content {offset_chunk_1 <hex0x0-0xffffffff> offset_chunk_2 <hex0x0-0xffffffff> offset_chunk_3 <hex0x0-0xffffffff> offset_chunk_4 <hex0x0-0xffffffff>} port [<portlist> all] [permit {priority <value 0-7> {replace_priority} rx_rate {no_limit <value 1-156249>}}] counter [enable disable}] mirror deny] ipv6 {{{class <value 0-255> flowlabel <hex 0x0-0xffff> source_ipv6 <ipv6addr> destination_ipv6 <ipv6addr>}}] port [<portlist> all] [permit {priority <value 0-7> {replace_priority} rx_rate {no_limit <value 1-156249>}}] counter [enable disable}] mirror deny]]] {time_range <range_name 32>} delete access_id <value 1-128>}
show access_profile	{profile_id <value 1-14>}
enable cpu_interface_filtering	
disable cpu_interface_filtering	
create cpu_access_profile profile_id	<value 1-5> [ethernet {vlan source_mac <macmask> destination_mac <macmask> ethernet_type} ip {vlan source_ip_mask <netmask> destination_ip_mask <netmask> dscp [icmp {type code} igmp {type} tcp {src_port_mask <hex 0x0-0xffff> dst_port_mask <hex 0x0-0xffff> flag_mask [all {urg ack psh rst syn fin}]} udp {src_port_mask <hex 0x0-0xffff> dst_port_mask <hex 0x0-0xffff>} protocol_id_mask {<hex 0x0-0xff> {user_define_mask <hex 0x0-0xffffffff>}}] packet_content_mask {offset 0-15 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> offset 16-31 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> {offset 32-47 <hex 0x0-0xffffffff> <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> <hex 0x0-0xffffffff> offset 64-79 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff>} ipv6 {{{class flowlabel} source_ipv6_mask <ipv6mask> destination_ipv6_mask <ipv6mask>}}]
delete cpu_access_profile	[profile_id <value 1-5> all]
config cpu_access_profile	profile_id <value 1-5> [add access_id <value 1-100> [ethernet {vlan <vlan_name 32> source_mac <macaddr> destination_mac <macaddr> ethernet_type <hex 0x0-0xffff>} port [<portlist> all] [permit deny] ip {vlan <vlan_name 32> source_ip <ipaddr> destination_ip <ipaddr> dscp <value 0-63> [icmp {type <value 0-255> code <value 0-255>} igmp {type <value 0-255>} tcp {src_port <value 0-65535> dst_port <value 0-65535> urg ack psh rst syn fin}]} udp {src_port <value 0-65535> dst_port <value 0-65535>} protocol_id <value 0-255> {user_define <hex 0x0-0xffffffff>}}] port [<portlist> all] [permit deny] 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> <hex 0x0-0xffffffff> offset_48-63 <hex 0x0-0xffffffff> <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> <hex 0x0-0xffffffff>} ipv6 {{{class <value 0-255> flowlabel <hex 0x0-0xffff>} source_ipv6 <ipv6addr> destination_ipv6 <ipv6addr>}}] port [<portlist> all] [permit deny]]] {time_range <range_name 32>} delete access_id <value 1-100>}
show cpu_access_profile	{profile_id <value 1-5>}

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

create access_profile (for Ethernet)

Purpose	Used to create an access profile on the Switch by examining the Ethernet part of the packet header. Masks entered can 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.
Syntax	create access_profile profile_id <value 1-14> [ethernet {vlan source_mac <macmask 000000000000-ffffffff> destination_mac <macmask 000000000000-ffffffff> 802.1p ethernet_type}
Description	This command will allow the user to create a profile for packets that may be accepted or denied by the Switch by examining the Ethernet part of the packet header. Specific values for rules pertaining to the Ethernet part of the packet header may be defined by configuring the config access_profile command for Ethernet, as stated below.
Parameters	<p><i>profile_id</i> <value 1-14> - Specifies an index number between 1 and 14 that will identify the access profile being created with this command.</p> <p><i>ethernet</i> - Specifies that the Switch will examine the layer 2 part of each packet header with emphasis on one or more of the following:</p> <ul style="list-style-type: none"> <i>vlan</i> – Specifies that the Switch will examine the VLAN part of each packet header. <i>source_mac</i> <macmask> – Specifies a MAC address mask for the source MAC address. This mask is entered in the following hexadecimal format: 000000000000-FFFFFFFF <i>destination_mac</i> <macmask> – Specifies a MAC address mask for the destination MAC address in the following format: 000000000000-FFFFFFFF <i>802.1p</i> – Specifies that the Switch will examine the 802.1p priority value in the frame's header. <i>ethernet_type</i> – Specifies that the Switch will examine the Ethernet type value in each frame's header.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To create an Ethernet access profile:

```
DGS-3627:5# create access_profile profile_id 1 ethernet vlan 802.1p
Command: create access_profile profile_id 1 ethernet vlan 802.1p

Success.

DGS-3627:5#
```

config access_profile (for Ethernet)

Purpose	Used to configure the Ethernet access profile on the Switch and to define specific values for the rules 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.
Syntax	profile_id <value 1-14> [add access_id [auto_assign <value 1-128>] [ethernet {vlan <vlan_name 32> source_mac <macaddr 000000000000-ffffffff> destination_mac <macaddr 000000000000-ffffffff> 802.1p <value 0-7> ethernet_type <hex 0x0-0xffff>} port [<portlist> all] [permit {priority <value 0-7> {replace_priority} rx_rate {no_limit <value 1-156249>}}] counter [enable disable]} mirror deny] {time_range <range_name 32>} delete access_id <value 1-128>]
Description	This command is used to define the rules used by the Switch to either filter or forward packets based on the Ethernet part of each packet header.
Parameters	<i>profile_id</i> <value 1-14> - Enter an integer between 1 and 14 that is used to identify the

config access_profile (for Ethernet)

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 lower the profile ID, the higher the priority the rule will be given.

add access_id <value 1-128> - Adds an additional rule to the above specified access profile. The value specifies the relative priority of the additional rule. Up to 128 different rules may be configured for the Ethernet access profile.

- *auto_assign* – Choose this parameter to configure the Switch to automatically assign a numerical value (between 1 and 128) for the rule being configured.

ethernet - Specifies that the Switch will look only into the layer 2 part of each packet to determine if it is to be filtered or forwarded based on one or more of the following:

- *vlan <vlan_name 32>* – Specifies that the access profile will apply to only this previously created VLAN.
- *source_mac <macaddr>* – Specifies that the access profile will apply to only packets with this source MAC address. MAC address entries may be made in the following format: **000000000000-FFFFFFFFFFFF**
- *destination_mac <macaddr>* – Specifies that the access profile will apply to only packets with this destination MAC address. MAC address entries may be made in the following format: **000000000000-FFFFFFFFFFFF**
- *802.1p <value 0-7>* – Specifies that the access profile 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.

port <portlist> | all - The access profile for Ethernet may be defined for each port on the Switch. Up to 128 rules may be configured for each port. The user may select all ports by entering the *all* parameter. The beginning and end of the port list range are separated by a dash. Non-contiguous portlist entries are separated by a comma. (ex: 1-3,7-9)

permit – Specifies that packets that match the access profile are permitted to be forwarded by the Switch.

- *priority <value 0-7>* – This parameter is specified to re-write the 802.1p default priority previously set in the Switch, which is used to determine the CoS queue to which packets are forwarded. Once this field is specified, packets accepted by the Switch that match this priority are forwarded to the CoS queue specified previously by the user.
- *{replace_priority}* – Enter this parameter if you want to re-write the 802.1p default priority of a packet to the value entered in the Priority field, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being forwarded by the Switch.

rx_rate – Use this to limit Rx bandwidth for the profile being configured. This rate is implemented using the following equation – 1 value = 64kbit/sec. (ex. If the user selects a rx rate of 10 then the ingress rate is 640kbit/sec.) The user may select a value between 1-156249 or no limit. The default setting is *no_limit*.

counter [enable | disable] – Use this parameter to enable the counter function. When enabled, this counter will count the number of packets that match the profile stated with this command. If the counter command is enabled using the *flow_meter* command, the counter command here will be overridden and therefore will not count packets. This command is optional and the default setting is *disabled*.

mirror - Selecting *mirror* specifies that packets that match the access profile are mirrored to a port defined in the **config mirror port** command. Port Mirroring must be enabled and a target port must be set.

deny – Specifies that packets that do not match the access profile are not permitted to be forwarded by the Switch and will be filtered.

{time_range <range_name 32>} – Choose this parameter and enter the name of the Time Range settings that has been previously configured using the **config time_range** command. This will set specific times when this access rule will be enabled or disabled on the Switch.

Parameters

config access_profile (for Ethernet)

delete access_id <value 1-128> – Use this command to delete a specific rule from the Ethernet profile. Up to 128 rules may be specified for the Ethernet access profile.

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

Example usage:

To configure a rule for the Ethernet access profile:

```
DGS-3627:5#config access profile profile_id 1 add access_id 1 ethernet vlan
Tiberius 802.1p 1 port 1 permit priority 1 replace priority
Command: config access profile profile_id 1 add access_id 1 ethernet vlan
Tiberius 802.1p 1 port 1 permit priority 1 replace priority
```

Success.

```
DGS-3627:5#
```

create access_profile (IP)

Purpose	Used to create an access profile on the Switch by examining the IP part of the packet header. Masks entered can 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.
Syntax	create access_profile profile_id <value 1-14> ip {vlan source_ip_mask <netmask> destination_ip_mask <netmask> dscp [icmp {type code} igmp {type}] tcp {src_port_mask <hex 0x0-0xffff> dst_port_mask <hex 0x0-0xffff> flag_mask [all {urg ack psh rst syn fin}]} udp {src_port_mask <hex 0x0-0xffff> dst_port_mask <hex 0x0-0xffff> protocol_id_mask <hex 0x0-0xff> {user_define_mask <hex 0x0-0xffffffff}}}
Description	This command will allow the user to create a profile for packets that may be accepted or denied by the Switch by examining the IP part of the packet header. Specific values for rules pertaining to the IP part of the packet header may be defined by configuring the config access_profile command for IP, as stated below.
Parameters	<p><i>ip</i> - Specifies that the Switch will look into the IP fields in each packet with special emphasis on one or more of the following:</p> <ul style="list-style-type: none"> • <i>profile_id <value 1-14></i> - Specifies an index number between 1 and 14 that will identify the access profile being created with this command. • <i>vlan</i> - Specifies that the Switch will examine the VLAN part of each packet header. • <i>source_ip_mask <netmask></i> – Specifies an IP address mask for the source IP address. • <i>destination_ip_mask <netmask></i> – Specifies an IP address mask for the destination IP address. • <i>dscp</i> – Specifies that the Switch will examine the DiffServ Code Point (DSCP) field in each frame's header. • <i>icmp</i> – Specifies that the Switch will examine the Internet Control Message Protocol (ICMP) field in each frame's header. <ul style="list-style-type: none"> • <i>type</i> – Specifies that the Switch will examine each frame's ICMP Type field. • <i>code</i> – Specifies that the Switch will examine each frame's ICMP Code field. • <i>igmp</i> – Specifies that the Switch will examine each frame's Internet Group Management Protocol (IGMP) field. <ul style="list-style-type: none"> • <i>type</i> – Specifies that the Switch will examine each frame's IGMP Type field. • <i>tcp</i> – Specifies that the Switch will examine each frames Transport Control Protocol

create access_profile (IP)

Parameters	<p>(TCP) field.</p> <ul style="list-style-type: none"> • <i>src_port_mask</i> <hex 0x0-0xffff> – Specifies a TCP port mask for the source port. • <i>dst_port_mask</i> <hex 0x0-0xffff> – Specifies a TCP port mask for the destination port. • <i>flag_mask</i> [<i>all</i> {<i>urg</i> <i>ack</i> <i>psh</i> <i>rst</i> <i>syn</i> <i>fin</i>}] – Enter the appropriate <i>flag_mask</i> 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 <i>all</i>, <i>urg</i> (urgent), <i>ack</i> (acknowledgement), <i>psh</i> (push), <i>rst</i> (reset), <i>syn</i> (synchronize) and <i>fin</i> (finish). • <i>udp</i> – Specifies that the Switch will examine each frame's User Datagram Protocol (UDP) field. <ul style="list-style-type: none"> • <i>src_port_mask</i> <hex 0x0-0xffff> – Specifies a UDP port mask for the source port. • <i>dst_port_mask</i> <hex 0x0-0xffff> – Specifies a UDP port mask for the destination port. • <i>protocol_id_mask</i> – Specifies that the Switch will examine each frame's Protocol ID field. <ul style="list-style-type: none"> • <hex 0x0-0xff> - Enter a hexadecimal value that will identify the protocol to be discovered in the packet header. • <i>user_define</i> <hex 0x0-0xffffffff> – Enter a hexadecimal value that will identify the user defined protocol to be discovered in the packet header.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To configure a rule for the IP access profile:

```
DGS-3627:5# create access_profile profile_id 2 ip protocol_id_mask 0xFF
Command: create access_profile profile_id 2 ip protocol_id_mask 0xFF

Success.

DGS-3627:5#
```

config access_profile (IP)

Purpose	Used to configure the IP access profile on the Switch and to define specific values for the rules 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.
Syntax	config access_profile profile_id <value 1-14> [add access_id [auto_assign <value 1-128>] ip { source_ip <ipaddr> destination_ip <ipaddr> dscp <value 0-63> [icmp igmp tcp { src_port <value 0-65535> dst_port <value 0-65535> urg ack psh rst syn fin } udp { src_port <value 0-65535> dst_port <value 0-65535>} protocol_id <value 0-255> { user_define <hex 0x0-0xffffffff>}}] port [<portlist> all] [permit { priority <value 0-7> { replace_priority } rx_rate { no_limit <value 1-156249>}}] counter [enable disable]}] mirror deny] { time_range <range_name 32>} delete access_id <value 1-128>]
Description	This command is used to define the rules used by the Switch to either filter or forward packets based on the IP part of each packet header.
Parameters	<i>profile_id</i> <value 1-14> - Enter an integer between 1 and 14 that is 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 lower the profile ID, the higher the priority the rule will be given.

config access_profile (IP)

add access_id <value 1-128> - Adds an additional rule to the above specified access profile. The value specifies the relative priority of the additional rule. Up to 128 different rules may be configured for the IP access profile.

- *auto_assign* – Choose this parameter to configure the Switch to automatically assign a numerical value (between 1 and 128) for the rule being configured.

ip – Specifies that the Switch will look into the IP fields in each packet to see if it will be either forwarded or filtered based on one or more of the following:

- *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.
- *igmp* – Specifies that the access profile will apply to packets that have this IGMP type.
- *tcp* - Specifies that the Switch will examine each frames Transport Control Protocol (TCP) field.
 - *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.
- Enter the type of TCP flag to be masked. The choices are:
 - *urg*: TCP control flag (urgent)
 - *ack*: TCP control flag (acknowledgement)
 - *push*: 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 Universal 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 header.
 - *dst_port <value 0-65535>* – Specifies that the access profile will apply only to packets that have this UDP destination port in their 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 appropriate rules.
 - *user_define <hex 0x0-0xffffffff>* – Enter a hexadecimal value that will identify the protocol to be discovered in the packet header.

port <portlist> | all - The access profile for IP may be defined for each port on the Switch. Up to 128 rules may be configured for each port. Selecting *all* will configure this rule for all ports on the Switch. The beginning and end of the port list range are separated by a dash. Non-contiguous portlist entries are separated by a comma. (ex: 1-3,7-9)

permit – Specifies that packets that match the access profile are permitted to be forwarded by the Switch.

- *priority <value 0-7>* – This parameter is specified to re-write the 802.1p default priority previously set in the Switch, which is used to determine the CoS queue to which packets are forwarded to. Once this field is specified, packets accepted by the Switch that match this priority are forwarded to the CoS queue specified previously by the user.
- *{replace_priority}* – Enter this parameter to re-write the 802.1p default priority of a packet to the value entered in the Priority field, which meets the criteria specified

config access_profile (IP)

previously in this command, before forwarding it on to the specified CoS queue. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being forwarded by the Switch.

replace_dscp <value 0-63> – Allows the user to specify a value to be written to the DSCP field of an incoming packet that meets the criteria specified in the first part of the command. This value will over-write the value in the DSCP field of the packet.

rx_rate - Use this to limit Rx bandwidth for the profile being configured. This rate is implemented using the following equation – 1 value = 64kbit/sec. (ex. If the user selects a rx rate of 10 then the ingress rate is 640kbit/sec.) The user may select a value between 1-156249 or no limit. The default setting is no limit.

counter [enable | disable] – Use this parameter to enable the counter function. When enabled, this counter will count the number of packets that match the profile stated with this command. If the counter command is enabled using the *flow_meter* command, the counter command here will be overridden and therefore will not count packets. This command is optional and the default setting is *disabled*.

mirror - Selecting *mirror* specifies that packets that match the access profile are mirrored to a port defined in the **config mirror port** command. Port Mirroring must be enabled and a target port must be set.

deny – Specifies that packets that do not match the access profile are not permitted to be forwarded by the Switch and will be filtered.

{time_range <range_name 32>} – Choose this parameter and enter the name of the Time Range settings that has been previously configured using the **config time_range** command. This will set specific times when this access rule will be enabled or disabled on the Switch.

delete access_id <value 1-128> – Use this command to delete a specific rule from the IP profile. Up to 128 rules may be specified for the IP access profile.

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

Example usage:

To configure a rule for the IP access profile:

```
DGS-3627:5#config access_profile profile_id 2 add access_id 2 ip protocol_id 2 port 2 deny
Command: config access_profile profile_id 2 add access_id 2 ip protocol_id 2 port 2 deny
```

```
Success.
```

```
DGS-3627:5#
```

create access_profile (packet content)

Purpose	Used to create an access profile on the Switch by examining the Ethernet part of the packet header. Packet content masks entered will specify certain bytes of the packet header to be identified by the Switch. When the Switch recognizes a packet with the identical byte as the one configured, it will either forward or filter the packet, based on the user's command. Specific values for the rules are entered using the config access_profile command, below.
Syntax	create access_profile profile_id <value 1-14> 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>}
Description	This command is used to identify packets by examining the Ethernet packet header, by byte and then decide whether to filter or forward it, based on the user's configuration. The user will specify which bytes to examine by entering them into the command, in hex form, and then selecting whether to filter or forward them, using the config access_profile command.
Parameters	<i>packet_content_mask</i> – The offset field is used to examine the packet header which

create access_profile (packet content)

is divided up into four “chunks” where each chunk represents 4 bytes. Values within the packet header chunk to be identified are to be marked in hexadecimal form in the “mask” field. The following table will help you identify the bytes in the respective chunks.

chunk0	chunk1	chunk2.....	chunk29	chunk30	chunk31
b126	b2	b6	b114	b118	b122
b127	b3	b7	b115	b119	b123
b1	b4	b8	b116	b120	b124
b0	b5	b9	b117	b121	b125

Check the box of the chunk, from 1 to 4, you wish to examine and then enter the hexadecimal value in the **mask** field.

profile_id <value 1-14> - Specifies an index number between 1 and 14 that will identify the access profile being created with this command.

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

Example usage:

To create an Access profile by packet content mask:

```
DGS-3627:5#create access_profile packet_content_mask offset_chunk_1 1
0xFFFFFFFF profile_id 3
Command: create access_profile packet_content_mask offset_chunk_1 1
0xFFFFFFFF profile_id 3
```

Success.

```
DGS-3627:5#
```

config access_profile profile_id (packet content)

Purpose	To configure the rule for a previously created access profile command based on the packet content mask. Packet content masks entered will specify certain bytes of the packet header to be identified by the Switch. When the Switch recognizes a packet with the identical byte as the one configured, it will either forward or filter the packet, based on the users command entered here.
Syntax	config access_profile profile_id <value 1-14> [add access_id <value 1-128> 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>} port [<portlist> all] [permit { priority <value 0-7> { replace_priority } rx_rate { no_limit <value 1-156249>}}] counter [enable disable }] mirror deny } { time_range <range_name 32>} delete access_id <value 1-128>]
Description	This command is used to set the rule for a previously configured access profile setting based on packet content mask. These rules will determine if the Switch will forward or filter the identified packets, based on user configuration specified in this command. Users will set bytes to identify by entering them in hex form, offset from the first byte of the packet.
Parameters	<p><i>profile_id</i> <value 1-14> - Enter an integer between 1 and 14 that is 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 lower the profile ID, the higher the priority the rule will be given.</p> <p><i>add access_id</i> - Adds an additional rule to the above specified access profile.</p> <ul style="list-style-type: none"> <i>auto_assign</i> – Adding this parameter will automatically assign an access_id to identify the rule. <value 1-128> - The value specifies the relative priority of the additional rule. Up to 128 different rules may be configured for the Ethernet access profile. <p><i>offset_chunk_1</i> – The offset field is used to examine the packet header which is divided up</p>

config access_profile profile_id (packet content)

into 4 “chunks” where each chunk represents 4 bytes. Values within the packet header chunk to be identified are to be marked in hexadecimal form in the “mask” field. The following table will help you identify the bytes in the respective chunks.

<u>chunk0</u>	<u>chunk1</u>	<u>chunk2</u>	<u>chunk29</u>	<u>chunk30</u>	<u>chunk31</u>
b126	b2	b6	b114	b118	b122
b127	b3	b7	b115	b119	b123
b1	b4	b8	b116	b120	b124
b0	b5	b9	b117	b121	b125

Check the box of the chunk, from 1-4, you wish to examine and then enter the hexadecimal value in the **mask** field.

port <portlist> | all - The access profile for IP may be defined for each port on the Switch. Up to 128 rules may be configured for each port. Selecting *all* will configure this rule for all ports on the Switch. The beginning and end of the port list range are separated by a dash. Non-contiguous portlist entries are separated by a comma. (ex:1-3,7-9)

permit – Specifies that packets that match the access profile are permitted to be forwarded by the Switch.

- *priority <value 0-7>* – This parameter is specified to re-write the 802.1p default priority previously set in the Switch, which is used to determine the CoS queue to which packets are forwarded to. Once this field is specified, packets accepted by the Switch that match this priority are forwarded to the CoS queue specified previously by the user.
- *{replace_priority}* – Enter this parameter to re-write the 802.1p default priority of a packet to the value entered in the Priority field, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being forwarded by the Switch.

replace_dscp <value 0-63> – Allows the user to specify a value to be written to the DSCP field of an incoming packet that meets the criteria specified in the first part of the command. This value will over-write the value in the DSCP field of the packet.

rx_rate - Use this to limit Rx bandwidth for the profile being configured. This rate is implemented using the following equation – 1 value = 64kbit/sec. (ex. If the user selects a rx rate of 10 then the ingress rate is 640kbit/sec.) The user may select a value between 1-156249 or no limit. The default setting is no limit.

counter [enable | disable] – Use this parameter to enable the counter function. When enabled, this counter will count the number of packets that match the profile stated with this command. If the counter command is enabled using the *flow_meter* command, the counter command here will be overridden and therefore will not count packets. This command is optional and the default setting is *disabled*.

mirror - Selecting *mirror* specifies that packets that match the access profile are mirrored to a port defined in the **config mirror port** command. Port Mirroring must be enabled and a target port must be set.

deny – Specifies that packets that do not match the access profile are not permitted to be forwarded by the Switch and will be filtered.

{time_range <range_name 32>} – Choose this parameter and enter the name of the Time Range settings that has been previously configured using the **config time_range** command. This will set specific times when this access rule will be enabled or disabled on the Switch.

delete access_id <value 1-128> – Use this command to delete a specific rule from the IP profile. Up to 128 rules may be specified for the IP access profile.

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

Example usage:

To configure an access profile by packet content mask:

```
DGS-3627:5#config access_profile profile_id 3 add access_id 1 packet_content
offset_chunk_1 0x11111111 port 3 permit priority 2 replace_priority rx_rate no_limit
counter enable
```

```
Command: config access_profile profile_id 3 add access_id 1 packet_content_mask
offset_chunk_1 0x11111111 port 3 permit priority 2 replace_priority rx_rate no_limit
counter enable
```

Success.

DGS-3627:5#

create access_profile (ipv6)

Purpose	Used to create an access profile on the Switch by examining the IPv6 part of the packet header. 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.
Syntax	create access_profile profile_id <value 1-14> ipv6 {class flowlabel source_ipv6_mask <ipv6mask> destination_ipv6_mask <ipv6mask>}
Description	This command is used to identify various parts of IPv6 packets that enter the Switch so they can be either forwarded or filtered.
Parameters	<p><i>profile_id</i> <value 1-14> - Specifies an index number between 1 and 14 that will identify the access profile being created with this command.</p> <p><i>ipv6</i> – 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. IPv6 packets may be identified by the following:</p> <ul style="list-style-type: none"> • <i>class</i> – Entering this parameter will instruct the Switch to examine the <i>class</i> 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. • <i>flowlabel</i> – Entering this parameter will instruct the Switch to examine the <i>flow label</i> 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. • <i>source_ipv6_mask</i> <ipv6mask> - Specifies an IP address mask for the source IPv6 address. • <i>destination_ipv6_mask</i> <ipv6mask> - Specifies an IP address mask for the destination IPv6 address.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To create an access profile based on IPv6 classification:

```
DGS-3627:5#create access_profile profile_id 4 ipv6 class flowlabel
```

```
Command: create access_profile profile_id 4 ipv6 class flowlabel
```

Success.

DGS-3627:5#

config access_profile profile_id (ipv6)

Purpose	Used to configure the IPv6 access profile on the Switch and to define specific values for the rules 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.
Syntax	config access_profile profile_id <value 1-14> add access_id [auto_assign <value 1-128>] ipv6 {class <value 0-255> flowlabel <hex 0x0-0xffff> source_ipv6 <ipv6addr>

config access_profile profile_id (ipv6)

destination_ipv6 <ipv6addr> port [<portlist> | all] [permit {priority <value 0-7> {replace_priority} | rx_rate {no_limit | <value 1-156249>}} | counter [enable | disable]} | mirror | deny] | {time_range <range_name 32>} delete access_id <value 1-128>]

Description This command is used to define the rules used by the Switch to either filter or forward packets based on the IPv6 part of each packet header.

Parameters *profile_id <value 1-14>* - Enter an integer between 1 and 14 that is 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 lower the profile ID, the higher the priority the rule will be given.

add access_id <value 1-128> - Adds an additional rule to the above specified access profile. The value specifies the relative priority of the additional rule. Up to 128 different rules may be configured for the IPv6 access profile.

- *auto_assign* – Choose this parameter to configure the Switch to automatically assign a numerical value (between 1 and 128) for the rule being configured.

ipv6 - Specifies that the Switch will look into the IPv6 fields in each packet, with emphasis on one or more of the following fields:

- *class <value 0-255>* - 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 <hex 0x0-ffff>* - 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. This field is to be defined by the user in hex form.
- *source_ipv6 <ipv6addr>* - Specifies an IP address mask for the source IPv6 address.
- *destination_ipv6 <ipv6addr>* - Specifies an IP address mask for the destination IPv6 address.

port <portlist> | all - The access profile for Ethernet may be defined for each port on the Switch. Up to 128 rules may be configured for each port. Selecting *all* will configure this rule for all ports on the Switch. The beginning and end of the port list range are separated by a dash. Non-contiguous portlist entries are separated by a comma. (ex: 1-3,7-9)

permit – Specifies that packets that match the access profile are permitted to be forwarded by the Switch.

- *priority <value 0-7>* – This parameter is specified to re-write the 802.1p default priority previously set in the Switch, which is used to determine the CoS queue to which packets are forwarded to. Once this field is specified, packets accepted by the Switch that match this priority are forwarded to the CoS queue specified previously by the user.
- *{replace_priority}* – Enter this parameter to re-write the 802.1p default priority of a packet to the value entered in the Priority field, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being forwarded by the Switch.

deny – Specifies that packets that match the access profile are not permitted to be forwarded by the Switch and will be filtered.

rx_rate - Use this to limit Rx bandwidth for the profile being configured. This rate is implemented using the following equation – 1 value = 64kbit/sec. (ex. If the user selects a rx rate of 10 then the ingress rate is 640kbit/sec.) The user may select a value between 1 and 156249 or no limit. The default setting is no limit.

counter [enable | disable] – Use this parameter to enable the counter function. When enabled, this counter will count the number of packets that match the profile stated with this command. If the counter command is enabled using the *flow_meter* command, the counter command here will be overridden and therefore will not count packets. This command is optional and the default setting is *disabled*.

mirror - Selecting *mirror* specifies that packets that match the access profile are mirrored to a port defined in the **config mirror port** command. Port Mirroring must be enabled and a target port must be set.

config access_profile profile_id (ipv6)

{time_range <range_name 32>} – Choose this parameter and enter the name of the Time Range settings that has been previously configured using the **config time_range** command. This will set specific times when this access rule will be enabled or disabled on the Switch.

delete_access_id <value 1-128> – Use this command to delete a specific rule from the IPv6 profile. Up to 128 rules may be specified for the IPv6 access profile.

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

Example usage:

To configure a previously created access profile based on IPv6 classification:

```
DGS-3627:5#config access_profile profile_id 4 add access_id 1 ipv6
class 1 flowlabel 0xABCD port 4 deny
Command: config access_profile profile_id 4 add access_id 1 ipv6
class 1 flowlabel 0xABCD port 4 deny
```

Success.

```
DGS-3627:5#
```

delete access_profile

Purpose	Used to delete a previously created access profile.
Syntax	delete access_profile [profile_id <value 1-14> all]
Description	The delete access_profile command is used to delete a previously created access profile on the Switch.
Parameters	<i>profile_id <value 1-14></i> – Enter an integer between 1 and 14 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. <i>all</i> – Use this parameter to delete all created access profiles on the Switch.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To delete the access profile with a profile ID of 1:

```
DGS-3400:4# delete access_profile profile_id 1
```

```
Command: delete access_profile profile_id 1
```

Success.

```
DGS-3400:4#
```

show access_profile

Purpose	Used to display the currently configured access profiles on the Switch.
Syntax	show access_profile {profile_id <value 1-14>}
Description	The show access_profile command is used to display the currently configured access profiles.
Parameters	<i>profile_id <value 1-14></i> – Enter an integer between 1 and 14 that is used to identify the access profile that will be viewed with this command. This value is assigned to the access profile when it is created with the create access_profile

show access_profile

command.
 Entering this command without the *profile_id* parameter will command the Switch to display all access profile entries.

Restrictions None.

Example usage:

To display all of the currently configured access profiles on the Switch:

```
DGS-3627:5#show access_profile
Command: show access_profile

Total Unused Rule Entries : 1791
Total Used Rule Entries   : 1

Access Profile ID: 1                TYPE : Packet Contact
=====
Owner       : ACL
MASK Option :
offset_chunk_1 : 1                value : 0x11111111

Access ID : 1                      Mode: Permit      Rx Rate(64Kbps): no_limit
                                           (Replaced)Priority: 2

Ports: 8
Time range: Tiberius
Total Matched Counter : 0
Offset_chunk_1 : 1  value : 0x11111111
=====
Unused Entries : 127

DGS-3627:5#
```

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 config cpu access_profile command, below.
Syntax	create cpu access_profile profile_id <value 1-5> [ethernet {vlan source_mac <macmask 000000000000-ffffffff> destination_mac <macmask 000000000000-ffffffff> ethernet_type } ip {vlan source_ip_mask <netmask> destination_ip_mask <netmask> dscp icmp {type code} igmp {type} tcp { src_port_mask <hex 0x0-0xffff> dst_port_mask <hex 0x0-0xffff>} flag_mask [all {urg ack psh rst syn fin}]} udp { src_port_mask <hex 0x0-0xffff> dst_port_mask <hex 0x0-0xffff>} protocol_id_mask <hex 0x0-0xff>} { user_define_mask <hex 0x0-0xffffffff>}}] packet_content_mask { offset 0-15 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> offset 16-31 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> { offset 32-47 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> { offset 48-63 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> { offset 64-79 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> { offset 80-95 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> ipv6 { class flowlabel source_ipv6_mask <ipv6mask> destination_ipv6_mask <ipv6mask>}}]
Description	The create cpu access_profile 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 config cpu access_profile command, below.
Parameters	<i>ethernet</i> – Specifies that the Switch will examine the layer 2 part of each packet header. <ul style="list-style-type: none"> <i>vlan</i> – Specifies that the Switch will examine the VLAN part of each packet header.

create cpu access_profile

- *source_mac* <macmask> - Specifies to examine the source MAC address mask. MAC address entries may be made in the following format: **000000000000-FFFFFFFFFFFF**
 - *destination_mac* <macmask> - Specifies to examine the destination MAC address mask. MAC address entries may be made in the following format: **000000000000-FFFFFFFFFFFF**
 - *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 Transport 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 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 0x0-0xff> – 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. IPv6 packets may be identified by the following:
- *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

create cpu access_profile

address.

- *destination_ipv6_mask <ipv6mask>* - Specifies an IP address mask for the destination IPv6 address.

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

Example usage:

To create a CPU access profile:

```
DGS-3627:5# 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-3627:5#
```

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	config cpu access_profile profile_id <value 1-5> [add access_id <value 1-100> [ethernet {vlan <vlan_name 32> source_mac <macaddr 000000000000-ffffffff> destination_mac <macaddr 000000000000-ffffffff> ethernet_type <hex 0x0-0xffff>} ip {vlan <vlan_name 32> source_ip <ipaddr> destination_ip <ipaddr> dscp <value 0-63> [icmp {type <value 0-255> code <value 0-255>} igmp {type <value 0-255>} tcp {src_port <value 0-65535> dst_port <value 0-65535> flag [all {urg ack psh rst syn fin}] udp {src_port <value 0-65535> dst_port <value 0-65535>} protocol_id <value 0-255> {user_define <hex 0x0-0xffffffff>}] packet_content {offset_0-15 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> offset_16-31 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> offset_32-47 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> offset_48-63 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> offset_64-79 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> } ipv6 [{class <value 0-255> flowlabel <hex 0x0-0xffff> source_ipv6 <ipv6addr> destination_ipv6 <ipv6addr>}]] port [<portlist> all] [permit deny]] {time_range <range_name 32>} delete access_id <value 1-100>]
Description	The config cpu access_profile 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 create cpu access_profile command, above.
Parameters	<p><i>profile_id <value 1-5></i> – 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.</p> <ul style="list-style-type: none"> • <i>add access_id <value 1-100></i> – Adds an additional rule to the above specified access profile. The value is used to index the rule created. <p><i>ethernet</i> – Specifies that the Switch will look only into the layer 2 part of each packet.</p>

config cpu access_profile

- *vlan* <vlan_name 32> – Specifies that the access profile will apply to only to this VLAN.
 - *source_mac* <macaddr> – Specifies that the access profile will apply to this source MAC address. MAC address entries may be made in the following format: **000000000000-FFFFFFFFFFFF**
 - *destination_mac* <macaddr> – Specifies that the access profile will apply to this destination MAC address. MAC address entries may be made in the following format: **000000000000-FFFFFFFFFFFF**
 - *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 examine the IP fields in each packet.
- *vlan* <vlan_name 32> – 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 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.
 - *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 header.
 - *dst_port* <value 0-65535> – Specifies that the access profile will apply only to packets that have this UDP destination port in their 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 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.

Parameters

config cpu access_profile

- *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 - Specifies that the Switch will look into the IPv6 fields in each packet, with emphasis on one or more of the following fields:

- *class <value 0-255>* - 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 <hex 0x0-ffff>* - 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. This field is to be defined by the user in hex form.
- *source_ipv6 <ipv6addr>* - Specifies an IP address mask for the source IPv6 address.
- *destination_ipv6 <ipv6addr>* - Specifies an IP address mask for the destination IPv6 address.

port <portlist> | all - The access profile for Ethernet may be defined for each port on the Switch. Up to 128 rules may be configured for each port. Selecting *all* will configure this rule for all ports on the Switch. The beginning and end of the port list range are separated by a dash. Non-contiguous portlist entries are separated by a comma. (ex: 1-3,7-9)

permit - Specifies that packets that match the access profile are permitted to be forwarded by the Switch.

deny - Specifies that packets that match the access profile are not permitted to be forwarded by the Switch and will be filtered.

{time_range <range_name 32>} - Choose this parameter and enter the name of the Time Range settings that has been previously configured using the **config time_range** command. This will set specific times when this access rule will be enabled or disabled on the Switch.

delete access_id <value 1-100> - Use this to remove a previously created access rule in a profile ID.

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

Example usage:

To configure CPU access list entry:

```
DGS-3627:5#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-3627:5#
```

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	The delete cpu access_profile command is used to delete a previously created CPU access profile.
Parameters	<p><i>profile_id <value 1-5></i> - 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.</p> <p><i>all</i> - Using this parameter will delete all configured CPU access profiles.</p>

delete cpu access_profile

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

Example usage:

To delete the CPU access profile with a profile ID of 1:

```
DGS-3627:5#delete cpu access_profile profile_id 1
Command: delete cpu access_profile profile_id 1

Success.

DGS-3627:5#
```

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	The config cpu_interface_filtering state command is used view the current CPU interface filtering entries set on the Switch.
Parameters	<i>profile_id <value 1-5></i> – 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. Entering this command without the profile ID parameter will display all configured CPU access profiles.
Restrictions	None.

Example usage:

To show the CPU filtering state on the Switch:

```
DGS-3627:5#show cpu access_profile
Command: show cpu access_profile

CPU Interface Filtering State: Disabled

CPU Interface Access Profile Table

Access Profile ID: 1                TYPE : Ethernet
=====
MASK Option :
VLAN
-----
Access ID: 2           Mode: Permit
Ports: 1
-----
default
=====
Total Entries: 1

DGS-3627:5#
```


TIME RANGE COMMANDS

The Time Range commands are used in conjunction with the Access Profile commands listed in the previous chapter to determine a starting point and an ending point, based on days of the week, when an Access Profile configuration will be enabled on the Switch. Once configured here, the time range are to be applied to an access profile rule using the **config access_profile profile_id** command.



NOTE: The Time Range commands are based on the time settings of the Switch. Make sure to configure the time for the Switch appropriately for these commands using commands listed in the Time and SNTP Commands chapter later in this manual.

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

Command	Parameters
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	

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

config time_range

Purpose	Used to configure a time range in which an access profile rule is to be enabled.
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 is to be used in conjunction with an access profile rule to determine a period of time when an access profile and an associated rule are to be enabled on the Switch. Remember, this time range can only be applied to one period of time and also, it is based on the time set on the Switch.
Parameters	<p><i>range_name 32</i> – Enter a name of no more than 32 alphanumeric characters that will be used to identify this time range on the Switch. This range name will be used in the config access_profile profile_id command to identify the access profile and associated rule to be enabled for this time range.</p> <p><i>hours</i> – This parameter is used to set the time in the day that this time range is to be set using the following parameters:</p> <ul style="list-style-type: none"> <i>start_time <time hh:mm:ss></i> - Use this parameter to identify the starting time of the time range, in hours, minutes and seconds, based on the 24-hour time system. <i>end_time <time hh:mm:ss></i> - Use this parameter to identify the ending time of the time range, in hours, minutes and seconds, based on the 24-hour time system. <p><i>weekdays</i> – Use this parameter to determine the days of the week to set this time range.</p> <ul style="list-style-type: none"> <i><daylist></i> - The user may set the days of the week here to set this time range in the three letter format (mon, tue, wed...). To specify a day range, separate the daylist using a dash (mon-fri would mean Monday through Friday). To specify a list of days in a week, separate the daylist using a comma, with no spaces (mon,tue,fri would mean Monday, Tuesday and Friday). <p><i>delete</i> – Use this parameter to delete a previously configured time range from the system.</p>
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To configure the time range time1 to be between 6:30 a.m. and 9:40 p.m., Monday to Friday:

```
DGS-3627:5#config time_range time1 hours start_time 6:30:00 end_time
21:40:00 weekdays mon-fri
Command: config time_range time1 hours start_time 6:30:00 end_time
21:40:00 weekdays mon-fri

Success.

DGS-3627:5#
```

show time_range

Purpose	To view the current configurations of the time range set on the Switch.
Syntax	show time_range
Description	This command is used to display the currently configured time range(s) set on the Switch.
Parameters	None.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To view the current time range settings.

```
DGS-3627:5#show time_range
Command: show time_range

Time Range information
-----
Range name   : time1
Weekdays    : Mon, Tue, Wed, Thu, Fri
Start time   : 06:30:00
End time     : 21:40:00

Total entries: 1

DGS-3627:5#
```

ACL FLOW METERING COMMANDS

Before configuring the ACL Flow Meter, here is a list of acronyms and terms users will need to know.

trTCM – Two Rate Three Color Marker. This, along with the srTCM, are two methods available on the switch for metering and marking packet flow. The trTCM meters and IP flow and marks it as a color based on the flow's surpassing of two rates, the CIR and the PIR.

CIR – Committed Information Rate. Common to both the trTCM and the srTCM, the CIR is measured in bytes of IP packets. IP packet bytes are measured by taking the size of the IP header but not the link specific headers. For the trTCM, the packet flow is marked green if it doesn't exceed the CIR and yellow if it does. The configured rate of the CIR must not exceed that of the PIR. The CIR can also be configured for unexpected packet bursts using the CBS and PBS fields.

CBS – Committed Burst Size. Measured in bytes, the CBS is associated with the CIR and is used to identify packets that exceed the normal boundaries of packet size. The CBS should be configured to accept the biggest IP packet that is expected in the IP flow.

PIR – Peak Information Rate. This rate is measured in bytes of IP packets. IP packet bytes are measured by taking the size of the IP header but not the link specific headers. If the packet flow exceeds the PIR, that packet flow is marked red. The PIR must be configured to be equal or more than that of the CIR.

PBS – Peak Burst Size. Measured in bytes, the PBS is associated with the PIR and is used to identify packets that exceed the normal boundaries of packet size. The PBS should be configured to accept the biggest IP packet that is expected in the IP flow.

srTCM – Single Rate Three Color Marker. This, along with the trTCM, are two methods available on the switch for metering and marking packet flow. The srTCM marks its IP packet flow based on the configured CBS and EBS. A packet flow that does not reach the CBS is marked green, if it exceeds the CBS but not the EBS its marked yellow, and if it exceeds the EBS its marked red.

CBS – Committed Burst Size. Measured in bytes, the CBS is associated with the CIR and is used to identify packets that exceed the normal boundaries of packet size. The CBS should be configured to accept the biggest IP packet that is expected in the IP flow.

EBS – Excess Burst Size. Measured in bytes, the EBS is associated with the CIR and is used to identify packets that exceed the boundaries of the CBS packet size. The EBS is to be configured for an equal or larger rate than the CBS.

DSCP – Differentiated Services Code Point. The part of the packet header where the color will be added. Users may change the DSCP field of incoming packets.

The ACL Flow Meter function will allow users to color code IP packet flows based on the rate of incoming packets. Users have two types of Flow metering to choose from, trTCM and srTCM, as explained previously. When a packet flow is placed in a color code, the user can choose what to do with packets that have exceeded that color-coded rate.

Green – When an IP flow is in the green mode, its configurable parameters can be set in the Conform field, where the packets can have their DSCP field changed. This is an acceptable flow rate for the ACL Flow Meter function.

Yellow – When an IP flow is in the yellow mode, its configurable parameters can be set in the Exceed field. Users may choose to either **Permit** or **Drop** exceeded packets. Users may also choose to change the DSCP field of the packets.

Red – When an IP flow is in the red mode, its configurable parameters can be set in the Exceed field. Users may choose to either **Permit** or **Drop** exceeded packets. Users may also choose to change the DSCP field of the packets.

Users may also choose to count exceeded packets by clicking the **Counter** check box. If the counter is enabled, the counter setting in the access profile will be disabled.

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

Command	Parameters
config flow_meter profile_id	<value 1-14> access_id <value 1-128> [[tr_tcm cir <value 1-156249> {cbs <value 1-16384>} pir <value 1-156249> {pbs <value 1-16384>} sr_tcm cir <value 1-156249> cbs <value 1-16384> ebs <value 1-16384>] {conform [permit replace_dscp <value 0-63>] {counter [enable disable]}} exceed [permit replace_dscp <value 0-63> drop] {counter [enable disable]} violate [permit replace_dscp <value 0-63> drop] {counter [enable disable]} delete]
show flow_meter	{profile_id <value 1-14> {access_id <value 1-128>}}

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

config flow_meter profile_id	
Purpose	Used to configure the flow metering function for ACL..
Syntax	config flow_meter profile_id <value 1-14> access_id <value 1-128> [[tr_tcm cir <value 1-156249> {cbs <value 1-16384>} pir <value 1-156249> {pbs <value 1-16384>} sr_tcm cir <value 1-156249> cbs <value 1-16384> ebs <value 1-16384>] {conform [permit replace_dscp <value 0-63>] {counter [enable disable]}} exceed [permit replace_dscp <value 0-63> drop] {counter [enable disable]} violate [permit replace_dscp <value 0-63> drop] {counter [enable disable]} delete]
Description	This command is used to configure the parameters for the flow metering function for ACL entries created on the switch.
Parameters	<p><i>profile_id <value 1-14></i> - Enter the pre-configured Profile ID for which to configure the ACL Flow Metering parameters.</p> <p><i>access_id <value 1-128></i> - Enter the pre-configured Access ID for which to configure the ACL Flow Metering parameters.</p> <p><i>tr_tcm</i> - Choosing this field will allow users to employ the Two Rate Three Color Mode and set the following parameters to determine the color rate of the IP packet flow.</p> <ul style="list-style-type: none"> • <i>cir <value 1-156249></i> – The Committed Information Rate can be set between 1 and 156249. IP flow rates at or below this level will be considered <i>green</i>. IP flow rates that exceed this rate but not the PIR rate are considered <i>yellow</i>. • <i>cbs <value 1-16384></i> - The Committed Burst Size. Used to gauge packets that are larger than the normal IP packets. This field does not have to be set for this feature to function properly but is to be used in conjunction with the CIR setting. The CBS should be configured to accept the biggest IP packet that is expected in the IP flow. • <i>pir <value 1-16384></i> - The Peak information Rate. IP flow rates that exceed this setting will be considered as <i>red</i>. This field must be set at an equal or higher value than the CIR. • <i>pbs <value 1-16384></i> - The Peak Burst Size. This optional field is to be used in conjunction with the PIR. The PBS should be configured to accept the biggest IP packet that is expected in the IP flow. <p><i>sr_tcm</i> - Choosing this field will allow users to employ the Single Rate Three Color Mode and set the following parameters to determine the color rate of the IP packet flow.</p> <ul style="list-style-type: none"> • <i>cir <value 1-156249></i> – The Committed Information Rate can be set between 1-156249. The color rates are based on the following two fields which are used in conjunction with the CIR. • <i>cbs <value 1-16384></i> - Committed Burst Size. Measured in bytes, the CBS is associated with the CIR and is used to identify packets that exceed the normal boundaries of packet size. The CBS should be configured to accept the biggest IP packet that is expected in the IP flow. Packet flows which are lower than this configured value are marked green. Packet flows which exceed this value but are less than the EBS value are marked yellow.

config flow_meter profile_id

- *ebs* <value 1-16384> - Excess Burst Size. Measured in bytes, the EBS is associated with the CIR and is used to identify packets that exceed the boundaries of the CBS packet size. The EBS is to be configured for an equal or larger rate than the CBS. Packet flows that exceed this value are marked as red.

conform - This field denotes the *green* packet flow. Green packet flows may have their DSCP field rewritten to a value stated in this field. Users may also choose to count green packets by checking the Counter check box.

- *permit* – Enter this parameter to allow packet flows that are in the green flow.
- *replace_dscp* <value 0-63> - Packets that are in the green flow may have their DSCP field rewritten using this parameter and entering the DSCP value to replace.
- *counter* [*enable* | *disable*] – Use this parameter to enable or disable the packet counter for the specified ACL entry in the green flow.

exceed - This field denotes the *yellow* packet flow. Yellow packet flows may have excess packets permitted through or dropped. Users may replace the DSCP field of these packets by checking its radio button and entering a new DSCP value in the allotted field.

- *permit* – Enter this parameter to allow packet flows that are in the yellow flow.
- *replace_dscp* <value 0-63> - Packets that are in the yellow flow may have their DSCP field rewritten using this parameter and entering the DSCP value to replace.
- *drop* – Enter this parameter to drop packets that are in the yellow flow.
- *counter* [*enable* | *disable*] – Use this parameter to enable or disable the packet counter for the specified ACL entry in the yellow flow.

violate - This field denotes the *red* packet flow. Red packet flows may have excess packets permitted through or dropped. Users may replace the DSCP field of these packets by checking its radio button and entering a new DSCP value in the allotted field.

- *permit* – Enter this parameter to allow packet flows that are in the red flow.
- *replace_dscp* <value 0-63> - Packets that are in the red flow may have their DSCP field rewritten using this parameter and entering the DSCP value to replace.
- *drop* – Enter this parameter to drop packets that are in the red flow.
- *counter* [*enable* | *disable*] – Use this parameter to enable or disable the packet counter for the specified ACL entry in the red flow.

delete – Use this parameter to delete the specified flow meter.

Restrictions

Only administrator-level and operator-level users can issue this command. Only two counters may be enabled at any given time.

Example usage:

To enable the sFlow function:

```
DGS-3627:5#config flow_meter profile_id 1 access_id 1 tr_tcm cir 1000 cbs
200 pir 2000 pbs 200 exceed replace_dscp 21 violate drop
Command: config flow_meter profile_id 1 access_id 1 tr_tcm cir 1000 cbs 200
pir 2000 pbs 200 exceed replace_dscp 21 violate drop

Success.

DGS-3627:5#
```

show flow_meter

Purpose	Used to display the ACL flow meter parameters set on the switch.
Syntax	show flow_meter {profile_id <value 1-14> {access_id <value 1-128>}}
Description	This command will display the flow meter parameters set on the switch.
Parameters	<i>profile_id <value 1-14></i> - Enter the profile ID of the ACL entry to be viewed for flow metering. <i>access_id <value 1-128></i> - Enter the access ID corresponding to the ACL entry to be viewed.
Restrictions	None.

Example usage:

To enable the sFlow function:

```
DGS-3627:5# show flow_meter profile_id 1 access_id 1
Command: show flow_meter profile_id 1 access_id 1

Profile ID : 1   Access ID : 1   Mode: trTCM
CIR: 1000(64kbps)   CBS: 200(Kbyte)   PIR: 2000(64kbps)   PBS : 200(Kbyte)
Action:
  Conform : Permit           Counter : Disabled
  Exceed  : Permit   Replace DSCP: 21   Counter : Disabled
  Violate  : Drop           Counter : Disabled

Total Entries : 1

DGS-3627:5#
```

sFLOW

sFlow is a feature that allows users to monitor network traffic running through the switch to identify network problems through packet sampling and packet counter information of the Switch. The Switch itself is the sFlow agent where packet data is retrieved and sent to an sFlow Analyzer where it can be scrutinized and utilized to resolve the problem.

The Switch can configure the settings for the sFlow Analyzer but the remote sFlow Analyzer device must have an sFlow utility running on it to retrieve and analyze the data it receives from the sFlow agent.

The Switch will take sample packets from the normal running traffic of the Switch based on a sampling interval configured by the user. Once this information has been gathered by the switch, it is packaged into a packet called an sFlow datagram, which is then sent to the sFlow Analyzer for analysis.

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	
create sflow analyzer_server	<value 1-4> owner <name 16> {timeout <sec 1-2000000 collectoraddress <ipaddr> collectorPort <udp_port_number 1-65535> maxdatagramsize <value 300-1400>}
config sflow analyzer_server	<value 1-4> {timeout <sec 1-2000000 collectoraddress <ipaddr> collectorPort <udp_port_number 1-65535> maxdatagramsize <value 300-1400>}
delete sflow analyzer_server	<value 1-4>
show sflow analyzer_server	
create sflow counter_poller ports	[<portlist> all] analyzer_server_id <value 1-4> {internal [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 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>}
delete sflow flow_sampler ports	[<portlist> all]
show sflow flow_sampler	
show sflow	

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

enable sflow

Purpose	Used to enable the sFlow function on the switch.
Syntax	enable sflow
Description	This command, along with the disable sflow command, is used to enable the sFlow function on the switch without altering configurations.
Parameters	None.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To enable the sFlow function:

```
DGS-3627:5#enable sflow
Command:enable sflow

Success.

DGS-3627:5#
```

disable sflow

Purpose	Used to disable the sFlow function on the switch.
Syntax	disable sflow
Description	This command, along with the enable sflow command, is used to disable the sFlow function on the switch without altering configurations.
Parameters	None.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To disable the sFlow:

```
DGS-3627:5#disable sflow
Command:disable sflow

Success.

DGS-3627:5#
```

create sflow analyzer_server

Purpose	Used to create the analyzer server for the sFlow functions.
Syntax	create sflow analyzer_server <value 1-4> owner <name 16> {timeout <sec 1-200000 collectoraddress <ipaddr> collectorport <udp_port_number 1-65535> maxdatagramsize <value 300-1400>}
Description	This command is used to create the remote sFlow Analyzer (collector) that will be used to gather and analyze sFlow Datagrams

create sflow analyzer_server

	that originate from the Switch. Users must have the proper sFlow software set on the Analyzer in order to receive datagrams from the switch to be analyzed, and to analyze these datagrams. Users may specify up to four unique analyzers to receive datagrams, yet the virtual port used must be unique to each entry.
Parameters	<p><i><value 1-4></i> - Enter a value from 1 to 4 to identify the sFlow server being created here.</p> <p><i>owner <name 16></i> - Enter the owner of the entry made here. The user that added this sFlow analyzer configures this name.</p> <p><i>timeout <sec 1-2000000></i> - Used to specify the timeout for the Analyzer server. When the server times out, all sFlow samples and counter polls associated with this server will be deleted. The user may set a time between 1 and 2000000 seconds with a default setting of 400 seconds.</p> <p><i>collectoraddress <ipaddr></i> - The IP address of the sFlow Analyzer Server. If this field is not specified, the entry will become 0.0.0.0 and therefore the entry will be inactive. Users must set this field.</p> <p><i>collectorport <udp_port_number 1-65535></i> - The destination UDP port where sFlow datagrams will be sent. The default setting for this field is 6343. Only one Analyzer Server address can be set for one UDP Collector Port.</p> <p><i>maxdatagramsize <value 300-1400></i> - This field will specify the maximum number of data bytes that can be packaged into a single sFlow datagram. Users may select a value between 300 and 1400 bytes with a default setting of 1400 bytes.</p>
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To create the sFlow server:

```
DGS-3627:5# create sflow analyzer_server 1 owner monitor
Command: create sflow analyzer_server 1 owner monitor

Success.

DGS-3627:5#
```

config sflow analyzer_server

Purpose	Used to configure the analyzer server for the sFlow functions.
Syntax	config sflow analyzer_server <value 1-4> {timeout <sec 1-2000000 collectoraddress <ipaddr> collectorport <udp_port_number 1-65535> maxdatagramsize <value 300-1400>}
Description	This command is used to configure the settings for the remote sFlow Analyzer (collector) that will be used to gather and analyze sFlow Datagrams that originate from the Switch. Users must have the proper sFlow software set on the Analyzer in order to receive datagrams from the switch to be analyzed, and to analyze these datagrams. Users may specify up to four unique analyzers to receive datagrams, yet the virtual port used must be unique to each entry.
Parameters	<i><value 1-4></i> - Enter a value from 1 to 4 to identify the sFlow server being configured here.

config sflow analyzer_server

timeout <sec 1-2000000> - Used to specify the timeout for the Analyzer server. When the server times out, all sFlow samples and counter polls associated with this server will be deleted. The user may set a time between 1 and 2000000 seconds with a default setting of 400 seconds.

collectoraddress <ipaddr> - The IP address of the sFlow Analyzer Server. If this field is not specified, the entry will become 0.0.0.0 and therefore the entry will be inactive. Users must set this field.

collectorport <udp_port_number 1-65535> - The destination UDP port where sFlow datagrams will be sent. The default setting for this field is 6343. Only one Analyzer Server address can be set for one UDP Collector Port.

maxdatagramsize <value 300-1400> - This field will specify the maximum number of data bytes that can be packaged into a single sFlow datagram. Users may select a value between 300 to 1400 bytes with a default setting of 1400 bytes.

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

Example usage:

To configure the sFlow server:

```
DGS-3627:5# config sflow analyzer_server collectoraddress 10.90.90.9
Command: config sflow analyzer_server collectoraddress 10.90.90.9

Success.

DGS-3627:5#
```

delete sflow analyzer_server

Purpose	Used to delete an sFlow analyzer server set on the switch.
Syntax	delete sflow analyzer_server <value 1-4>
Description	This command will delete a previously created sFlow analyzer server.
Parameters	<i><value 1-4></i> - Enter the value identifying the analyzer to be deleted here.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To delete an sFlow analyzer server:

```
DGS-3627:5# delete sflow analyzer_server 1
Command: delete sflow analyzer_server 1

Success.

DGS-3627:5#
```

show sflow analyzer_server

Purpose	Used to display the settings of the sFlow analyzer server set on the switch.
Syntax	show sflow analyzer_server
Description	This command will display the settings for a previously created sFlow analyzer server.
Parameters	None.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To display the sFlow analyzer server settings:

```
DGS-3627:5# show sflow analyzer_server
```

```
Command: show sflow analyzer_server
```

```
SFlow Analyzer Server Information
```

```
-----
Server ID           :1
Owner              : ctsnow
Timeout            : 2000
Current Countdown Time : 2000
Collector Address   : 10.1.2.23
Collector Port      : 6343
Max Datagram Size  : 1400
```

```
Total Entries : 1
```

```
DGS-3627:5#
```

create sflow counter_poller ports

Purpose	Used to create the counter poller for the sFlow function of the switch.
Syntax	create sflow counter_poller ports [<portlist> all] analyzer_server_id <value 1-4> {interval [disable <sec 20-120>]}
Description	This command will allow the user to configure the settings for the Switch's counter poller. This mechanism will take a poll of the IF counters of the Switch and then package them with the other previously mentioned data into a datagram which will be sent to the sFlow Analyzer Server for examination.
Parameters	<p><i><portlist></i> - Use this parameter to set the ports that will be mined for sFlow information.</p> <p><i>all</i> - Use this parameter to set all ports to be mined for sFlow information.</p> <p><i>analyzer_server_id <value 1-4></i> - Enter a value from 1 to 4 to identify the sFlow server where this information will be sent.</p> <p><i>interval [disable <sec 20-120>]</i> - Users may configure the Polling Interval here. The switch will take a poll of the IF counters every time this interval reaches 0, and this information will be included in the sFlow datagrams that will be sent to the sFlow Analyzer for examination. Choosing the disabled parameter will disable the counter polling for this entry.</p>
Restrictions	Only administrator-level and operator-level users can issue this

create sflow counter_poller ports

command.

Example usage:

To create the sFlow counter poller:

```
DGS-3627:5# create sflow counter_poller ports 1 analyzer_server_id 1 interval 20
Command: create sflow counter_poller ports 1 analyzer_server_id 1 interval 20

Success.

DGS-3627:5#
```

config sflow counter_poller ports

Purpose	Used to configure the counter poller for the sFlow function of the switch.
Syntax	create sflow counter_poller ports [<portlist> all] {interval [disable <sec 20-120>]}
Description	This command will allow the user to configure the settings for the Switch's counter poller. This mechanism will take a poll of the IF counters of the Switch and then package them with the other previously mentioned data into a datagram which will be sent to the sFlow Analyzer Server for examination.
Parameters	<p><i><portlist></i> - Use this parameter to set the ports that will be mined for sFlow information.</p> <p><i>all</i> - Use this parameter to set all ports to be mined for sFlow information.</p> <p><i>interval [disable <sec 20-120>]</i> - Users may configure the Polling Interval here. The switch will take a poll of the IF counters every time this interval reaches 0, and this information will be included in the sFlow datagrams that will be sent to the sFlow Analyzer for examination. Choosing the disabled parameter will disable the counter polling for this entry.</p>
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To configure the sFlow counter poller settings:

```
DGS-3627:5# config sflow counter_poller ports 1 interval 50
Command: create sflow counter_poller ports 1 interval 50

Success.

DGS-3627:5#
```

delete sflow counter_poller ports

Purpose	Used to delete the counter poller for the sFlow function of the switch.
Syntax	delete sflow counter_poller ports [<portlist> all]
Description	This command will allow the user to delete the Switch's counter poller.

delete sflow counter_poller ports

Parameters	<i><portlist></i> - Use this parameter to delete the ports that will be mined for sFlow information. <i>all</i> - Use this parameter to delete all ports to be mined for sFlow information.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To delete the sFlow counter poller settings:

```
DGS-3627:5#delete sflow counter_poller ports all
Command:delete sflow counter_poller ports all

Success.

DGS-3627:5#
```

show sflow counter_poller

Purpose	Used to display the counter poller for the sFlow function of the switch.
Syntax	show sflow counter_poller
Description	This command will allow the user to display the Switch's counter poller.
Parameters	None.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To show the sFlow counter poller settings:

```
DGS-3627:5#show sflow counter_poller
Command:show sflow counter_poller

Port      Analyzer Server ID  Polling Interval
-----
1         1                   20

Total Entries : 1

DGS-3627:5#
```

create sflow flow_sampler ports

Purpose	Used to configure the flow sampler settings for the sFlow function.
Syntax	create sflow flow_sampler ports [<i><portlist></i> <i>all</i>] analyzer_server_id <i><value 1-4></i> {rate <i><value 0-65535></i> maxheadersize <i><value 18-256></i>}
Description	This command will allow users to configure the Switch's settings for taking sample packets from the network, including the sampling rate and the amount of the packet header to be extracted.

create sflow flow_sampler ports

Parameters	<p><i><portlist></i> - Use this parameter to set the ports that will be mined for sFlow information.</p> <p><i>all</i> - Use this parameter to set all ports to be mined for sFlow information.</p> <p><i>analyzer_server_id <value 1-4></i> - Enter a value from 1 to 4 to identify the sFlow server where this information will be sent.</p> <p><i>rate <value 0-65535></i> - Users can set the rate of packet sampling here. The value entered here is to be multiplied by 256 to get the percentage of packets sampled. For example, if the user enters a figure of 20 into this field, the switch will sample one out of every 5120 packets (20 x 256 = 5120) that pass through the individual port. Users may enter a value between 1 and 65535. An entry of 0 disables the packet sampling. Since this is the default setting, users are reminded to configure a rate here or this function will not function.</p> <p><i>maxheadersize <value 18-256></i> - This field will set the number of leading bytes of the sampled packet header. This sampled header will be encapsulated with the datagram to be forwarded to the Analyzer Server. The user may set a value between 18 and 256 bytes. The default setting is 128 bytes.</p>
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To create the sFlow flow sampler:

```
DGS-3627:5#create sflow flow_sampler ports 1 analyzer_server_id 1 rate 10000
maxheadersize 128
Command: create sflow flow_sampler ports 1 analyzer_server_id 1 rate 10000
maxheadersize 128
Success.
DGS-3627:5#
```

config sflow flow_sampler ports

Purpose	Used to configure the flow sampler settings for the sFlow function.
Syntax	config sflow flow_sampler ports [<portlist> all] {rate <value 0-65535> maxheadersize <value 18-256>
Description	This command will allow users to configure the Switch's settings for taking sample packets from the network, including the sampling rate and the amount of the packet header to be extracted.
Parameters	<p><i><portlist></i> - Use this parameter to set the ports that will be mined for sFlow information.</p> <p><i>all</i> - Use this parameter to set all ports to be mined for sFlow information.</p> <p><i>rate <value 0-65535></i> - Users can set the rate of packet sampling here. The value entered here is to be multiplied by 256 to get the percentage of packets sampled. For example, if the user enters a figure of 20 into this field, the switch will sample one out of every 5120 packets (20 x 256 = 5120) that pass through the individual port. Users may enter a value between 1 and 65535. An entry of 0 disables the packet sampling. Since this is the default setting, users are reminded to configure a rate here or this function will not function.</p>

config sflow flow_sampler ports

maxheadersize <value 18-256> - This field will set the number of leading bytes of the sampled packet header. This sampled header will be encapsulated with the datagram to be forwarded to the Analyzer Server. The user may set a value between 18 and 256 bytes. The default setting is 128 bytes.

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

Example usage:

To configure the sflow flow sampler:

```
DGS-3627:5#config sflow flow_sampler ports 1 rate 20000 maxheadersize 128
Command: config sflow flow_sampler ports 1 rate 20000 maxheadersize 128
```

Success.

```
DGS-3627:5#
```

delete sflow flow_sampler ports

Purpose Used to delete the flow sampler for the sFlow function of the switch.

Syntax **delete sflow sflow_sampler ports [<portlist> | all]**

Description This command will allow the user to delete the Switch's flow sampler settings.

Parameters <portlist> - Use this parameter to delete the ports that will be mined for sFlow information.

all - Use this parameter to delete all ports to be mined for sFlow information.

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

Example usage:

To delete the sFlow flow sampler settings:

```
DGS-3627:5#delete sflow flow_sampler ports all
```

```
Command: delete sflow flow_sampler ports all
```

Success.

```
DGS-3627:5#
```

show sflow flow_sampler

Purpose	Used to display the sFlow sampler information for the sFlow function of the switch.
Syntax	show sflow flow_sampler
Description	This command will allow the user to display the Switch's sFlow flow sampler information.
Parameters	None.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To show the sFlow flow sampler settings:

```
DGS-3627:5#show sflow flow_sampler
Command:show sflow flow_sampler

Port      Analyzer Server ID  Configured Rate  Active Rate  Max Header Size
-----
1         1                   10000           0            128

Total Entries : 1

DGS-3627:5#
```

show sflow

Purpose	Used to display the sflow settings configured on the switch
Syntax	show sflow
Description	This command will allow the user to display the Switch's sFlow settings.
Parameters	None.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To show the sFlow settings:

```
DGS-3627:5#show sflow
Command:show sflow

SFlow Version   : 1.00
SFlow Address   :10.53.13.199
SFlow State     : Enabled

DGS-3627:5#
```


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>}
show sntp	
enable sntp	
disable sntp	
config time	<date ddmthyyyy> <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>}
Description	Use this command to configure SNTP service from an SNTP server. SNTP must be enabled for this command to function (See <i>enable sntp</i>).
Parameters	<p><i>primary</i> – This is the primary server the SNTP information will be taken from.</p> <ul style="list-style-type: none"> • <i><ipaddr></i> – The IP address of the primary server. <p><i>secondary</i> – This is the secondary server the SNTP information will be taken from in the event the primary server is unavailable.</p> <ul style="list-style-type: none"> • <i><ipaddr></i> – The IP address for the secondary server. <p><i>poll-interval <int 30-99999></i> – This is the interval between requests for updated SNTP information. The polling interval ranges from 30 to 99,999 seconds.</p>
Restrictions	Only administrator-level 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-3627:5#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-3627:5#
```

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-3627:5#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    : 720 sec

DGS-3627:5#
```

enable sntp

Purpose	To enable SNTP server support.
Syntax	enable sntp
Description	This 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-level 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-3627:5#enable sntp
```

```
Command: enable sntp
```

```
Success.
```

```
DGS-3627:5#
```

disable sntp

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

Example:

To disable SNTP support:

```
DGS-3627:5#disable sntp
```

```
Command: disable sntp
```

```
Success.
```

```
DGS-3627:5#
```

config time

Purpose	Used to manually configure system time and date settings.
Syntax	config time <date ddmthyyy> <time hh:mm:ss>
Description	This will configure the system time and date settings. These will be overridden if SNTP is configured and enabled.
Parameters	<p><i>date</i> – 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.</p> <p><i>time</i> – 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.</p>
Restrictions	Only administrator-level 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-3627:5#config time 30jun2003 16:30:30
```

```
Command: config time 30jun2003 16:30:30
```

```
Success.
```

```
DGS-3627:5#
```

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 will adjust system clock settings according to the time zone. Time zone settings will adjust SNTP information accordingly.
Parameters	<i>operator</i> – Choose to add (+) or subtract (-) time to adjust for time zone relative to GMT. <i>hour</i> – Select the number of hours different from GMT. <i>min</i> – Select the number of minutes difference added or subtracted to adjust the time zone.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To configure time zone settings:

```
DGS-3627:5#config time_zone operator + hour 2 min 30
```

```
Command: config time_zone operator + hour 2 min 30
```

```
Success.
```

```
DGS-3627:5#
```

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	DST can be enabled and configured using this command. 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.

config dst

Parameters	<p><i>disable</i> - Disable the DST seasonal time adjustment for the Switch.</p> <p><i>repeating</i> - 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.</p> <p><i>annual</i> - 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.</p> <p><i>s_week</i> - Configure the week of the month in which DST begins.</p> <p><i><start_week 1-4,last></i> - 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.</p> <p><i>e_week</i> - Configure the week of the month in which DST ends.</p> <ul style="list-style-type: none"> • <i><end_week 1-4,last></i> - 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. <p><i>s_day</i> - Configure the day of the week in which DST begins.</p> <ul style="list-style-type: none"> • <i><start_day sun-sat></i> - The day of the week in which DST begins expressed using a three character abbreviation (sun, mon, tue, wed, thu, fri, sat) <p><i>e_day</i> - Configure the day of the week in which DST ends.</p> <ul style="list-style-type: none"> • <i><end_day sun-sat></i> - The day of the week in which DST ends expressed using a three character abbreviation (sun, mon, tue, wed, thu, fri, sat) <p><i>s_mth</i> - Configure the month in which DST begins.</p> <ul style="list-style-type: none"> • <i><start_mth 1-12></i> - The month to begin DST expressed as a number. <p><i>e_mth</i> - Configure the month in which DST ends.</p> <ul style="list-style-type: none"> • <i><end_mth 1-12></i> - The month to end DST expressed as a number. <p><i>s_time</i> - Configure the time of day to begin DST.</p> <ul style="list-style-type: none"> • <i><start_time hh:mm></i> - Time is expressed using a 24-hour clock, in hours and minutes. <p><i>e_time</i> - Configure the time of day to end DST.</p> <ul style="list-style-type: none"> • <i><end_time hh:mm></i> - Time is expressed using a 24-hour clock, in hours and minutes. <p><i>s_date</i> - Configure the specific date (day of the month) to begin DST.</p> <ul style="list-style-type: none"> • <i><start_date 1-31></i> - The start date is expressed numerically. <p><i>e_date</i> - Configure the specific date (day of the month) to begin DST.</p> <ul style="list-style-type: none"> • <i><end_date 1-31></i> - The end date is expressed numerically. <p><i>offset [30 60 90 120]</i> - Indicates number of minutes to add or to subtract during the summertime. The possible offset times are 30, 60, 90, and 120. The default value is 60.</p>
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To configure daylight savings time on the Switch:

```
DGS-3627:5#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-3627:5#
```

show time

Purpose	Used to display the current time settings and status.
Syntax	show time
Description	This 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-3627:5#show time
Command: show time

Current Time Source : System Clock
Boot Time           : 23 Aug 2006 09:44:18
Current Time        : 23 Aug 2006 15:42:52
Time Zone           : GMT +02:30
Daylight Saving Time : Repeating
Offset in Minutes   : 30
  Repeating From    : Apr 2nd Tue 15:00
                   To      : Oct 2nd Wed 15:30
  Annual From      : 29 Apr 00:00
                   To      : 12 Oct 00:00

DGS-3627:5#
```

POLICY ROUTE COMMANDS

Policy Based routing is a method used by the Switch to give specified devices a cleaner path to the Internet. Used in conjunction with the Access Profile feature, the Switch will identify traffic originating from a specified IP address and forward it on to a next hop router that has a less congested connection to the Internet than the normal routing scheme of your network.

The steps needed to set up policy-based routing on the switch are as follows:

1. Create an access profile using the **create access_profile** command which specifies information that will identify the device to be given a policy route.
2. Modify the rule regarding this access profile using the **config access_profile** command. (Remember not to add the deny parameter to this rule, or packets will be dropped and the policy route will not take effect.)
3. Name the policy route to be used by configuring the **create policy_route** command.
4. Bind the access profile (profile_id) and its rule (access_id) to this policy route using the **config policy_route** command. This command must also be used to add the next hop IP address of the device that will be connected directly to the gateway router. When the time is ready to deploy the policy route, the administrator must enable this function here as well (state [enable | disable]).

Once completed, the Switch will identify the device to be given a policy route using the access profile function, recognize that it has a Policy Based route, and then forward the information on to the specified next hop router, that will, in turn, relay packets to the gateway router. Thus, the new, cleaner path to the Internet has been formed.

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

Command	Parameters
create policy_route	name <policyroute_name 32>
config policy_route	name <policyroute_name 32> acl profile_id <value 1-14> access_id <value 1-128> nexthop <ipaddr> state [enable disable]
delete policy_route	name <policyroute_name 32>
show policy_route	

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

create policy_route

Purpose	Used to create a name to identify a policy route.
Syntax	create policy_route name <policyroute_name 32>
Description	This command is used to create a policy route name which will identify the policy route.
Parameters	<i>name <policyroute_name 32></i> - Enter an alphanumeric name of no more than 32 characters to identify this policy route.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To create the policy route name “manager”:

```
DGS-3627:5#create policy_route name manager
Command: create policy_route name manager

Success.

DGS-3627:5#
```

config policy_route

Purpose	Used to configure the parameters to set the policy route on the Switch.
Syntax	config policy_route name <policyroute_name 32> acl profile_id <value 1-14> access_id <value 1-128> nexthop <ipaddr> state [enable disable]
Description	This command is used to configure the policy route settings for a policy route created with the create policy_route command. The administrator must have previously created an access profile with an accompanying access rule using the create access_profile profile_id and config access_profile profile_id mentioned previously in this manual. The next hop router IP address must also be specified using this command.
Parameters	<p><i>name <policyroute_name 32></i> - Enter an alphanumeric name of no more than 32 characters which identifies this policy route.</p> <p><i>acl</i> – This parameter is used to denote the access profile that will be used with this command, by identifying the following parameters:</p> <ul style="list-style-type: none"> <i>profile_id <value 1-14></i> - Enter the ID number of the previously created access profile that is to be associated with this policy route. <i>access_id <value 1-128></i> - Enter the previously created access ID that has been created in conjunction with the access profile ID mentioned previously, that is to be associated with this policy route. <p><i>nexthop <ipaddr></i> - Enter the IP address of the net hop router that will be connected to the gateway router. This field must be set or no policy routing will take place.</p> <p><i>state [enable disable]</i> – Used to enable or disable this policy route on the Switch.</p>
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To configure the policy route name “manager”:

```
DGS-3627:5#config policy_route name manager acl profile_id 1 access_id 2 next
hop 10.2.2.2 state enable
Command: config policy_route name manager acl profile_id 1 access_id 2 next
hop 10.2.2.2 state enable

Success.

DGS-3627:5#
```

delete policy_route

Purpose	Used to delete a policy route setting.
Syntax	delete policy_route name <policyroute_name 32>
Description	This command is used to delete a policy route setting.
Parameters	<i>name <policyroute_name 32></i> - Enter an alphanumeric name of no more than 32 characters to identify this policy route to be deleted.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To delete the policy route name “manager”:

```
DGS-3627:5#delete policy_route name manager
Command: delete policy_route name manager

Success.

DGS-3627:5#
```

show policy_route

Purpose	Used to display policy route settings.
Syntax	show policy_route
Description	This command is used to display policy route settings.
Parameters	None.
Restrictions	None.

Example usage:

To display the policy route settings:

```
DGS-3627:5# show policy_route
Command: show policy_route

Name      Profile ID  Access ID  Next Hop  State
-----
manager   1           1          10.3.3.3  Enabled

Total Entries: 1

DGS-3627:5#
```

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:

1. It will limit bandwidth of receiving ARP packets. The user may implement this in two ways, by using the **config safeguard_engine** command.
 - a. When *strict* is chosen, the Switch will stop receiving ARP packets not destined for the Switch. This will eliminate all unnecessary ARP packets while allowing the essential ARP packets to pass through to the Switch's CPU.
 - b. When *fuzzy* is chosen, the Switch will minimize the ARP packet bandwidth received by the switch by adjusting the bandwidth for all ARP packets, whether destined for the Switch or not. The Switch uses an internal algorithm to filter ARP packets through, with a higher percentage set aside for ARP packets destined for the Switch.
2. It will limit the bandwidth of IP packets received by the Switch. The user may implement this in two ways, by using the **config safeguard_engine** command.
 - a. When *strict* is chosen, the Switch will stop receiving all unnecessary broadcast IP packets, even if the high CPU utilization is not caused by the high reception rate of broadcast IP packets.
 - b. When *fuzzy* is chosen, the Switch will minimize the IP packet bandwidth received by the Switch by adjusting the bandwidth for all IP packets, by setting a acceptable bandwidth for both unicast and broadcast IP packets. The Switch uses an internal algorithm to filter IP packets through while adjusting the bandwidth dynamically.

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>} trap_log [enable disable] mode [strict fuzzy]}
show safeguard_engine	

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

config safeguard_engine

Purpose	To config ARP storm control for system.
Syntax	config safeguard_engine {state [enable disable] utilization {rising <value 20-100> falling <value 20-100>} trap_log [enable disable] mode [strict fuzzy]}
Description	Use this command to configure Safeguard Engine to minimize the effects of an ARP storm.

config safeguard_engine

Parameters	<p><i>state [enable disable]</i> – Select the running state of the Safeguard Engine function as enable or disable.</p> <p><i>utilization</i> – Select this option to trigger the Safeguard Engine function to enable based on the following determinates:</p> <ul style="list-style-type: none"> • <i>rising <value 20-100></i> - 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. • <i>falling <value 20-100></i> - 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. <p><i>trap_log [enable disable]</i> – 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.</p> <p><i>mode</i> - 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:</p> <ul style="list-style-type: none"> • <i>strict</i> – 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. • <i>fuzzy</i> - 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.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To configure the safeguard engine for the Switch:

```
DGS-3627:5#config safeguard_engine state enable utilization rising 45
Command: config safeguard_engine state enable utilization rising 45

Success.

DGS-3627:5#
```

show safeguard_engine

Purpose	Used to display current Safeguard Engine settings.
Syntax	show safeguard_engine
Description	This will 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-3627:5#show safeguard_engine
Command: show safeguard_engine

Safeguard engine state      : Disabled
Safeguard engine current status : normal mode
=====
CPU utilization information:
Rising      : 30%
Falling     : 20%
Trap/Log state : Disabled
Mode        : Fuzzy

DGS-3627:5#
```

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> 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> forward_list [null all <portlist>]
Description	The config traffic_segmentation command is used to configure traffic segmentation on the Switch.
Parameters	<p><i><portlist></i> – Specifies a port or range of ports that will be configured for traffic segmentation. The beginning and end of the port list range are separated by a dash. Non-contiguous portlist entries are separated by a comma. (ex: 1-3,7-9)</p> <p><i>forward_list</i> – Specifies a range of ports that will receive forwarded frames from the ports specified in the portlist, above.</p> <ul style="list-style-type: none"> • <i>null</i> – No ports are specified. • <i>all</i> – All ports are specified. • <i><portlist></i> – 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 <i><portlist></i> specified above for config traffic_segmentation). The beginning and end of the port list range are separated by a dash. Non-contiguous portlist entries are separated by a comma. (ex:1-3,7-9)
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To configure ports 1 through 5 to be able to forward frames to port 6 through 10:

```
DGS-3627:5# config traffic_segmentation 1-5 forward_list 6-10
Command: config traffic_segmentation 1-5 forward_list 6-10

Success.

DGS-3627:5#
```

show traffic_segmentation

Purpose	Used to display the current traffic segmentation configuration on the Switch.
Syntax	show traffic_segmentation {<portlist>}
Description	The show traffic_segmentation command is used to display the current traffic segmentation configuration on the Switch.
Parameters	<p><i><portlist></i> – Specifies a port or range of ports for which the current traffic segmentation configuration on the Switch will be displayed. The beginning and end of the port list range are separated by a</p>

show traffic_segmentation

	dash. Non-contiguous portlist entries are separated by a comma. (ex: 1-3,7-9)
Restrictions	The port lists for segmentation and the forward list must be on the same Switch.

Example usage:

To display the current traffic segmentation configuration on the Switch.

```
DGS-3627:5#show traffic_segmentation
Command: show traffic_segmentation

Traffic Segmentation Table

Port  Forward Portlist
-----
1     1-27
2     1-27
3     1-27
4     1-27
5     1-27
6     1-27
7     1-27
8     1-27
9     1-27
10    1-27
11    1-27
12    1-27
13    1-27
14    1-27
15    1-27
16    1-27
17    1-27
18    1-27
CTRL+C | ESC | q Quit | SPACE | n Next Page | Enter Next Entry | a All
```

ARP AND GRATUITOUS 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>
delete arpentry	[<ipaddr> all]
show arpentry	{ipif <ipif_name 12> ipaddress <ipaddr> static}
config arp_aging time	<value 0-65535>
clear arptable	
config arpentry	<ipaddr> <macaddr>
config gratuitous_arp send ipif_status_up	[enable disable]
config gratuitous_arp send dup_ip_detected	[enable disable]
config gratuitous_arp learning	[enable disable]
enable gratuitous_arp	{ipif <ipif_name 12>} {trap log }
disable gratuitous_arp	{ipif <ipif_name 12>} {trap log}
config gratuitous_arp send periodically ipif	<ipif_name 12> interval <value 0-65535>
show gratuitous_arp	{ipif <ipif_name 12>}

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-level 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-3627:5#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-3627:5#
```

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 <i>all</i> clears the Switch's ARP table.
Parameters	<i><ipaddr></i> – The IP address of the end node or station. <i>all</i> – Deletes all ARP entries.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example Usage:

To delete an entry of IP address 10.48.74.121.125 from the ARP table:

```
DGS-3627:5#delete arpentry 10.48.74.121
Command: delete arpentry 10.48.74.121

Success.

DGS-3627:5#
```

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	<i>time <value 0-65535></i> – 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-level and operator-level users can issue this command.

Example usage:

To configure ARP aging time:

```
DGS-3627:5#config arp_aging time 30
Command: config arp_aging time 30

Success.

DGS-3627:5#
```

show arpentry

Purpose	Used to display the ARP table.
Syntax	show arpentry {ipif <ipif_name 12> ipaddress <ipaddr> static}

show arpentry

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

Example usage:

To display the ARP table:

```
DGS-3627:5#show arpentry
Command: show arpentry

ARP Aging Time : 30

Interface      IP Address      MAC Address      Type
-----
System         10.0.0.0        FF-FF-FF-FF-FF-FF  Local/Broadcast
System         10.1.1.169      00-50-BA-70-E4-4E  Dynamic
System         10.1.1.254      00-01-30-FA-5F-00  Dynamic
System         10.9.68.1       00-A0-C9-A4-22-5B  Dynamic
System         10.9.68.4       00-80-C8-2E-C7-45  Dynamic
System         10.10.27.51     00-80-C8-48-DF-AB  Dynamic
System         10.11.22.145   00-80-C8-93-05-6B  Dynamic
System         10.11.94.10    00-10-83-F9-37-6E  Dynamic
System         10.14.82.24    00-50-BA-90-37-10  Dynamic
System         10.15.1.60     00-80-C8-17-42-55  Dynamic
System         10.17.42.153   00-80-C8-4D-4E-0A  Dynamic
System         10.19.72.100   00-50-BA-38-7D-5E  Dynamic
System         10.21.32.203   00-80-C8-40-C1-06  Dynamic
System         10.40.44.60    00-50-BA-6B-2A-1E  Dynamic
System         10.42.73.221   00-01-02-03-04-00  Dynamic
System         10.44.67.1     00-50-BA-DA-02-51  Dynamic
System         10.47.65.25    00-50-BA-DA-03-2B  Dynamic
System         10.50.8.7      00-E0-18-45-C7-28  Dynamic
System         10.90.90.90    00-01-02-03-04-00  Local
System         10.255.255.255 FF-FF-FF-FF-FF-FF  Local/Broadcast

Total Entries: 20

DGS-3627:5#
```

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-level and operator-level users can issue this command.

Example Usage:

To remove dynamic entries in the ARP table:

```
DGS-3627:5#clear arptable
```

```
Command: clear arptable
```

```
Success.
```

```
DGS-3627:5#
```

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 above.
Restrictions	Only administrator-level 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-3627:5#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-3627:5#
```

config gratuitous_arp send ipif_status_up

Purpose	Used to enable/disable the sending of gratuitous ARP requests while the IP interface status comes up.
Syntax	config gratuitous_arp send ipif_status_up [enable disable]
Description	The command is used to enable/disable sending of gratuitous ARP request packets while the IPIF interface comes up. This is used to automatically announce the interface's IP address to other nodes. By default, the state is enabled, and only one ARP packet will be broadcast.
Parameters	<i>enable</i> – Enable sending of gratuitous ARP when IPIF status comes up. <i>disable</i> – Disable sending of gratuitous ARP when IPIF status comes up.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To enable send gratuitous ARP request in a normal situation:

```
DGS-3627:5#config gratuitous_arp send ipif_status_up enable
Command: config gratuitous_arp send ipif_status_up enable

Success.

DGS-3627:5#
```

config gratuitous_arp send dup_ip_detected

Purpose	Used to enable/disable the sending of gratuitous ARP requests while a duplicate IP address is being detected.
Syntax	config gratuitous_arp send duplicate_ip_detected [enable disable]
Description	The command is used to enable/disable sending of gratuitous ARP request packets while a duplicate IP is being detected. By default, the state is enabled. For this command, the duplicate IP detected means that the system received an ARP request packet that is sent by an IP address that matches the system's own IP address. In this case, the system knows that somebody is using an IP address that is in conflict with the system. In order to reclaim the correct host of this IP address, the system can send out the gratuitous ARP request packet for this duplicate IP address.
Parameters	<i>enable</i> – Enable sending of gratuitous ARP when a duplicate IP is detected. <i>disable</i> – Disable sending of gratuitous ARP when a duplicate IP is detected.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example Usage:

To enable send a gratuitous ARP request when a duplicate IP is detected:

```
DGS-3627:5#config gratuitous_arp duplicate_ip_detected enable
Command: config gratuitous_arp duplicate_ip_detected enable
```

Success.

DGS-3627:5#

config gratuitous_arp learning

Purpose	Used to enable/disable learning of ARP entries in the ARP cache based on the received gratuitous ARP packets.
Syntax	config gratuitous_arp learning [enable disable]
Description	The command is used to enable/disable updating the ARP cache based on the received gratuitous ARP packets. If the switch receives a gratuitous ARP packet and the sender's IP address in its ARP table, it should update the ARP aging timer. By default, the state is disabled.
Parameters	<i>enable</i> – Enable learning of ARP entry based on the received gratuitous ARP packet. <i>disable</i> – Disable learning of ARP entry based on the received gratuitous ARP packet.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To enable learning of ARP entry based on the received gratuitous ARP packet:

DGS-3627:5#config gratuitous_arp learning enable
Command: config gratuitous_arp learning enable

Success.

DGS-3627:5#

enable gratuitous_arp trap & log

Purpose	Used to enable gratuitous ARP trap and log state.
Syntax	enable gratuitous_arp {ipif <ipif_name 12>} {trap log }
Description	The command is used to enable gratuitous ARP trap and log state. The switch can trap and log the IP conflict event to inform the administrator. By default, trap is disabled and event log is enabled.
Parameters	<i>ipif <ipif_name 12></i> – The name of the IP interface the end node or station for which the ARP table entry was made, resides on. <i>{trap log}</i> – Select gratuitous ARP trap and/or log state.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To enable system interface's gratuitous ARP log and trap:

DGS-3627:5#enable gratuitous_arp System trap log
Command: enable gratuitous_arp System trap log

Success.

DGS-3627:5#

disable gratuitous_arp trap & log

Purpose	Used to disable gratuitous ARP trap and log state.
Syntax	disable gratuitous_arp {ipif <ipif_name 12>} {trap log }
Description	This command is used to disable gratuitous ARP trap and log state. When the trap and log are disabled, the switch won't trap and log IP conflict events to inform the administrator.
Parameters	<i>ipif <ipif_name 12></i> – The name of the IP interface the end node or station for which the ARP table entry was made, resides on. <i>{trap log}</i> – Select gratuitous ARP trap and/or log state.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example Usage:

To disable the system interface's gratuitous ARP log and trap:

```
DGS-3627:5#disable gratuitous_arp System trap log
Command: disable gratuitous_arp System trap log

Success.

DGS-3627:5#
```

config gratuitous_arp send periodically

Purpose	Used to configure the interval for periodical sending of gratuitous ARP request packet.
Syntax	config gratuitous_arp send periodically ipif <ipif_name 12> interval <value 0-65535>
Description	The command is used to configure the interval for the periodic sending of gratuitous ARP request packets. By default, the interval is 0.
Parameters	<i><ipif_name 12></i> – The name of the Layer 3 interface. <i><value 0-65535></i> – Periodically send gratuitous ARP interval time in seconds. 0 - means not to send gratuitous ARP periodically.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To configure gratuitous ARP interval to 5 for IPIF System:

```
DGS-3627:5#config gratuitous_arp send periodically ipif
System interval 5
Command: config gratuitous_arp send periodically ipif System
interval 5

Success.

DGS-3627:5#
```

show gratuitous arp

Purpose	Used to display gratuitous ARP configuration.
Syntax	show gratuitous_arp {ipif <ipif_name>}
Description	This command is used to display gratuitous ARP configuration.
Parameters	<ipif_name 12> – The interface name of the Layer 3 device.
Restrictions	None.

Example usage:

To display gratuitous ARP log and trap state:

```
DGS-3627:5#show gratuitous_arp
Command: show gratuitous_arp

Send on IPIF status up           : Enabled
Send on Duplicate_IP_Detected    : Disabled
Gratuitous ARP Learning          : Enabled

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

IP Interface Name : ip1
  Gratuitous ARP Trap           : Disabled
  Gratuitous ARP Log            : Enabled
  Gratuitous ARP Periodical Send Interval : 6

DGS-3627:5#
```

VRRP COMMANDS

VRRP or Virtual Routing Redundancy Protocol is a function on the Switch that dynamically assigns responsibility for a virtual router to one of the VRRP routers on a LAN. The VRRP router that controls the IP address associated with a virtual router is called the Master, and will forward packets sent to this IP address. This will allow any Virtual Router IP address on the LAN to be used as the default first hop router by end hosts. Utilizing VRRP, the administrator can achieve a higher available default path cost without needing to configure every end host for dynamic routing or routing discovery protocols.

Statically configured default routes on the LAN are prone to a single point of failure. VRRP is designed to eliminate these failures by setting an election protocol that will assign a responsibility for a virtual router to one of the VRRP routers on the LAN. When a virtual router fails, the election protocol will select a virtual router with the highest priority to be the Master router on the LAN. This retains the link and the connection is kept alive, regardless of the point of failure.

To configure VRRP for virtual routers on the Switch, an IP interface must be present on the system and it must be a part of a VLAN. VRRP IP interfaces may be assigned to every VLAN, and therefore IP interface, on the Switch. VRRP routers within the same VRRP group must be consistent in configuration settings for this protocol to function optimally.

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

Command	Parameters
enable vrrp	{ping}
disable vrrp	{ping}
create vrrp vrid	<vrid 1-255> ipif <ipif_name 12> ipaddress <ipaddr> {state [enable disable] priority <int 1-254> advertisement_interval <int 1-255> preempt [true false] critical_ip <ipaddr> critical_ip_state [enable disable]}
config vrrp vrid	<vrid 1-255> ipif <ipif_name 12> {state [enable disable] priority <int 1-254> ipaddress <ipaddr> advertisement_interval <int 1-255> preempt [true false] critical_ip <ipaddr> critical_ip_state [enable disable]}
config vrrp ipif	<ipif_name 12> [authtype [none simple authdata <string 8> ip authdata <string 16>]]
show vrrp	{ipif <ipif_name 12> {vrid <vrid 1-255>}}
delete vrrp	{vrid <vrid 1-255> ipif <ipif_name 12>}

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

enable vrrp	
Purpose	To enable the VRRP function on the Switch.
Syntax	enable vrrp {ping}
Description	This command will enable the VRRP function on the Switch.
Parameters	{ping} – Adding this parameter to the command will allow the virtual IP address to be pinged from other host end nodes to verify connectivity. This will only enable the ping connectivity check function. To enable the VRRP protocol on the Switch, omit this parameter. This command is disabled by default.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example Usage:

To enable VRRP globally on the Switch:

```
DGS-3627:5#enable vrrp
Command: enable vrrp

Success.

DGS-3627:5#
```

Example usage:

To enable the virtual IP address to be pinged:

```
DGS-3627:5#enable vrrp ping
Command: enable vrrp ping

Success.

DGS-3627:5#
```

disable vrrp

Purpose	To disable the VRRP function on the Switch.
Syntax	disable vrrp {ping}
Description	This command will disable the VRRP function on the Switch.
Parameters	<i>{ping}</i> - Adding this parameter to the command will stop the virtual IP address from being pinged from other host end nodes to verify connectivity. This will only disable the ping connectivity check function. To disable the VRRP protocol on the Switch, omit this parameter.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To disable the VRRP function globally on the Switch:

```
DGS-3627:5#disable vrrp
Command: disable vrrp

Success.

DGS-3627:5#
```

Example usage:

To disable the virtual IP address from being pinged:

```
DGS-3627:5#disable vrrp ping
Command: disable vrrp ping

Success.

DGS-3627:5#
```


create vrrp vrid

Purpose	To create a VRRP router on the Switch.
Syntax	vrid <vrid 1-255> ipif <ipif_name 12> ipaddress <ipaddr> {state [enable disable] priority <int 1-254> advertisement_interval <int 1-255> preempt [true false] critical_ip <ipaddr> critical_ip_state [enable disable]}
Description	This command is used to create a VRRP interface on the Switch.
Parameters	<p><i>vrid <vrid 1-255></i> - Enter a value between 1 and 255 to uniquely identify this VRRP group on the Switch. All routers participating in this group must be assigned the same <i>vrid</i> value. This value MUST be different from other VRRP groups set on the Switch.</p> <p><i>ipif <ipif_name 12></i> - Enter the name of a previously configured IP interface for which to create a VRRP entry. This IP interface must be assigned to a VLAN on the Switch.</p> <p><i>ipaddress <ipaddr></i> - Enter the IP address that will be assigned to the VRRP router. This IP address is also the default gateway that will be statically assigned to end hosts and must be set for all routers that participate in this group.</p> <p><i>state [enable disable]</i> - Used to enable and disable the VRRP router on the Switch.</p> <p><i>priority <int 1-254></i> - Enter a value between 1 and 254 to indicate the router priority. The VRRP Priority value may determine if a higher priority VRRP router overrides a lower priority VRRP router. A higher priority will increase the probability that this router will become the Master router of the group. A lower priority will increase the probability that this router will become the backup router. VRRP routers that are assigned the same priority value will elect the highest physical IP address as the Master router. The default value is 100. (The value of 255 is reserved for the router that owns the IP address associated with the virtual router and is therefore set automatically.)</p> <p><i>advertisement_interval <int 1-255></i> - Enter a time interval value, in seconds, for sending VRRP message packets. This value must be consistent with all routers participating within the same VRRP group. The default is 1 second.</p> <p><i>preempt [true false]</i> - This entry will determine the behavior of backup routers within the VRRP group by controlling whether a higher priority backup router will preempt a lower priority Master router. A true entry, along with having the backup router's priority set higher than the masters priority, will set the backup router as the Master router. A false entry will disable the backup router from becoming the Master router. This setting must be consistent with all routers participating within the same VRRP group. The default setting is true.</p> <p><i>critical_ip <ipaddr></i> - Enter the IP address of the physical device that will provide the most direct route to the Internet or other critical network connections from this virtual router. This must be a real IP address of a real device on the network. If the connection from the virtual router to this IP address fails, the virtual router will be disabled automatically. A new master will be elected from the backup routers participating in the VRRP group. Different critical IP addresses may be assigned to different routers participating in the VRRP group, and can therefore define multiple routes to the Internet or other critical network connections.</p> <p><i>critical_ip_state [enable disable]</i> - This parameter is used to enable or disable the critical IP address entered above. The default is disable.</p>
Restrictions	Only administrator-level and operator-level users can issue this

create vrrp vrid

command.

Example usage:

To create a VRRP entry:

```
DGS-3627:5#create vrrp vrid 1 ipif Tiberius ipaddress 11.1.1.1 state enable
priority 200 advertisement_interval 1 preempt true critical_ip 10.53.13.224
critical_ip_state enable
```

```
Command: create vrrp vrid 1 ipif Tiberius ipaddress 11.1.1.1 state enable
priority 200 advertisement_interval 1 preempt true critical_ip 10.53.13.224
critical_ip_state enable
```

Success.

```
DGS-3627:5#
```

config vrrp vrid

Purpose	To configure a VRRP router set on the Switch.
Syntax	config vrrp vrid <vrid 1-255> ipif <ipif_name 12> {state [enable disable] priority <int 1-254> ipaddress <ipaddr> advertisement_interval <int 1-255> preempt [true false] critical_ip <ipaddr> critical_ip_state [enable disable]}
Description	This command is used to configure a previously created VRRP interface on the Switch.
Parameters	<p><i>vrid <vrid 1-255></i> - Enter a value between 1 and 255 that uniquely identifies the VRRP group to configure. All routers participating in this group must be assigned the same <i>vrid</i> value. This value MUST be different from other VRRP groups set on the Switch.</p> <p><i>ipif <ipif_name 12></i> - Enter the name of a previously configured IP interface to configure a VRRP entry for. This IP interface must be assigned to a VLAN on the Switch.</p> <p><i>state [enable disable]</i> – Used to enable and disable the VRRP router on the Switch.</p> <p><i>priority <int 1-254></i> - Enter a value between 1 and 254 to indicate the router priority. The VRRP Priority value may determine if a higher priority VRRP router overrides a lower priority VRRP router. A higher priority will increase the probability that this router will become the Master router of the group. A lower priority will increase the probability that this router will become the backup router. VRRP routers that are assigned the same priority value will elect the highest physical IP address as the Master router. The default value is 100. (The value of 255 is reserved for the router that owns the IP address associated with the virtual router and is therefore set automatically.)</p> <p><i>ipaddress <ipaddr></i> - Enter the virtual IP address that will be assigned to the VRRP entry. This IP address is also the default gateway that will be statically assigned to end hosts and must be set for all routers that participate in this group.</p> <p><i>advertisement_interval <int 1-255></i> - Enter a time interval value, in seconds, for sending VRRP message packets. This value must be consistent with all routers participating within the same VRRP group. The default is 1 second.</p> <p><i>preempt [true false]</i> – This entry will determine the behavior of backup routers within the VRRP group by controlling whether a higher priority backup router will preempt a lower priority Master</p>

config vrrp vrid

router. A true entry, along with having the backup router's priority set higher than the masters priority, will set the backup router as the Master router. A false entry will disable the backup router from becoming the Master router. This setting must be consistent with all routers participating within the same VRRP group. The default setting is *true*.

critical_ip <ipaddr> - Enter the IP address of the physical device that will provide the most direct route to the Internet or other critical network connections from this virtual router. This must be a real IP address of a real device on the network. If the connection from the virtual router to this IP address fails, the virtual router will be disabled automatically. A new master will be elected from the backup routers participating in the VRRP group. Different critical IP addresses may be assigned to different routers participating in the VRRP group, and can therefore define multiple routes to the Internet or other critical network connections.

critical_ip_state [enable | disable] – This parameter is used to enable or disable the critical IP address entered above. The default is *disable*.

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

Example usage:

To configure a VRRP entry:

```
DGS-3627:5#config vrrp vrid 1 ipif Zira state enable priority 100 advertisement_interval 2
Command: config vrrp vrid 1 ipif Zira state enable priority 100 advertisement_interval 2
```

Success.

```
DGS-3627:5#
```

config vrrp ipif

Purpose To configure the authentication type for the VRRP routers of an IP interface.

Syntax **config vrrp ipif <ipif_name 12> [authtype [none | simple authdata <string 8> | ip authdata <string 16>]**

Description This command is used to set the authentication type for the VRRP routers of an IP interface.

Parameters *ipif <ipif_name 12>* - Enter the name of a previously configured IP interface for which to configure the VRRP entry. This IP interface must be assigned to a VLAN on the Switch.

authtype – Specifies the type of authentication used. The authtype must be consistent with all routers participating within the VRRP group. The user may choose between:

- *none* – Entering this parameter indicates that VRRP protocol exchanges will not be authenticated.
- *simple authdata <string 8>* - This parameter, along with an alphanumeric string of no more than eight characters, to set a simple password for comparing VRRP message packets received by a router. If the two passwords are not exactly the same, the packet will be dropped.

ip authdata <string 16> - This parameter will require the user to set

config vrrp ipif

	an alphanumeric authentication string of no more than 16 characters to generate a MD5 message digest for authentication in comparing VRRP messages received by the router. If the two values are inconsistent, the packet will be dropped.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To set the authentication type for a VRRP entry:

```
DGS-3627:5#config vrrp ipif Zira authtype simple authdata tomato
Command: config vrrp ipif Zira authtype simple authdata tomato
```

Success.

```
DGS-3627:5#
```

show vrrp

Purpose	To view the VRRP settings set on the Switch.
Syntax	show vrrp ipif <ipif_name 12> vrid <vrid 1-255>
Description	This command is used to view current VRRP settings of the VRRP Operations table.
Parameters	<i>ipif <ipif_name 12></i> - Enter the name of a previously configured IP interface for which to view the VRRP settings. This IP interface must be assigned to a VLAN on the Switch. <i>vrid <vrid 1-255></i> - Enter the VRRP ID of a VRRP entry for which to view these settings.
Restrictions	None.

Example Usage:

To view the global VRRP settings currently implemented on the Switch (VRRP Enabled):

```
DGS-3627:5#show vrrp
Command: show vrrp

Global VRRP           : Enabled
Non-owner response PING : Disabled

Interface Name       : System
Authentication type  : No Authentication

  VRID                : 2
  Virtual IP Address   : 10.53.13.3
  Virtual MAC Address  : 00-00-5E-00-01-02
  Virtual Router State : Master
  State                : Enabled
  Priority              : 255
  Master IP Address    : 10.53.13.3
  Critical IP Address  : 0.0.0.0
  Checking Critical IP : Disabled
  Advertisement Interval : 1 secs
  Preempt Mode         : True
  Virtual Router Up Time : 2754089 centi-secs
Total Entries : 1
```

```
DGS-3627:5#
```

delete vrrp

Purpose	Used to delete a VRRP entry from the switch.
Syntax	delete vrrp {vrid <vrid 1-255> ipif <ipif_name 12>}
Description	This command is used to remove a VRRP router running on a local device.
Parameters	<i>vrid <vrid 1-255></i> - Enter the VRRP ID of the virtual router to be deleted. Not entering this parameter will delete all VRRP entries on the Switch. <i>ipif <ipif_name 12></i> - Enter the name of the IP interface which holds the VRRP router to delete.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To delete a VRRP entry:

```
DGS-3627:5#delete vrrp vrid 2 ipif Zira
```

```
Command: delete vrrp vrid 2 ipif Zira
```

```
Success.
```

```
DGS-3627:5#
```

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 <network_address>] [null0 <ipaddr> {<metric 1-65535>} {[primary backup weight <value 1-4>]}]
delete iproute	[default <network_address>] [null0 <ipaddr>]
show iproute	{[<network_address> <ipaddr>]} {[static rip ospf]}
create ipv6route	[default <ipv6networkaddr>] [<ipif_name 12> <ipv6addr> <ipv6addr> {<metric 1-65535>} {[primary backup]}]
delete ipv6route	[[default <ipv6networkaddr>] [<ipif_name 12> <ipv6addr> <ipv6addr>] all]
show ipv6route	{<ipv6networkaddr>}

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

create iproute

Purpose	Used to create IP route entries to the Switch's IP routing table.
Syntax	create iproute [default <network_address>] [null0 <ipaddr> {<metric 1-65535>} {[primary backup weight <value 1-4>]}]
Description	This command is used to create an IP route entry to the Switch's IP routing table. This route may be primary, backup or weighted multipath.
Parameters	<p><i>default</i> – Use this parameter to create a default static IP route entry to the Switch's IP routing table.</p> <p><i><network_address></i> – IP address and netmask of the IP interface that is the destination of the route. The address and mask information can be specified using the traditional format (for example, 10.1.2.3/255.0.0.0 or in CIDR format, 10.1.2.3/8).</p> <p><i>null0</i> – Specify the null interface as the next hop.</p> <p><i><ipaddr></i> – The gateway IP address for the next hop router.</p> <p><i><metric 1-65535></i> – 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.</p> <p><i>[primary backup]</i> - The user may choose between Primary and Backup. If the Primary Static/Default Route fails, the Backup Route will support the entry. Please take note that the Primary and Backup entries cannot have the same Gateway.</p> <p><i>weight <value 1-4></i> - This field is used to add a weight to the IP route. The rate will determine the ratio for forwarding data packets to a destination.</p>
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To add a single static address 10.48.74.121, mask 255.0.0.0 and gateway 10.1.1.254 to the routing table:

```
DGS-3627:5#create iproute 10.48.74.121/255.0.0.0 10.1.1.254 1
Command: create iproute 10.48.74.121/8 10.1.1.254 1
```

```
Success.
```

```
DGS-3627:5#
```

To create a static route with Null interface as the next hop:

```
DGS-3627:5#create iproute 10.48.74.121/255.0.0.0 Null0
Command: create iproute 10.48.74.121/8 Null0
```

```
Success.
```

```
DGS-3627:5#
```

delete iproute

Purpose	Used to delete an IP route entry from the Switch's IP routing table.
Syntax	delete iproute [default <network_address>] [null0 <ipaddr>]
Description	This command will delete an existing entry from the Switch's IP routing table.
Parameters	<p><i>default</i> – Use this parameter to delete a default static IP route entry from the Switch's IP routing table.</p> <p><network_address> – IP address and netmask of the IP interface that is the destination of the route. The address and mask information can be specified using the traditional format (for example, 10.1.2.3/255.0.0.0 or in CIDR format, 10.1.2.3/8).</p> <p><i>null0</i> – Specify the null interface as the next hop.</p> <p><ipaddr> – The gateway IP address for the next hop router.</p>
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To delete a backup static address 10.48.75.121, mask 255.0.0.0 and gateway (ipaddr) entry of 10.1.1.254 from the routing table:

```
DGS-3627:5#delete iproute 10.48.74.121/8 10.1.1.254
Command: delete iproute 10.48.74.121/8 10.1.1.254
```

```
Success.
```

```
DGS-3627:5#
```

To delete a static route whose next hop is Null interface:

```
DGS-3627:5#delete iproute 10.48.74.121/8 Null0
Command: delete iproute 10.48.74.121/8 Null0
```

```
Success.
```

```
DGS-3627:5#
```

show iproute

Purpose	Used to display the Switch's current IP routing table.
Syntax	show iproute {[<network_address> <ipaddr>]} {[static rip ospf]}
Description	This command will display the Switch's current IP routing table.
Parameters	<network_address> – IP address and netmask of the IP interface that is

show iproute

the destination of the route. The address and mask information can be specified using the traditional format (for example, 10.1.2.3/255.0.0.0 or in CIDR format, 10.1.2.3/8).

<ipaddr> – The gateway IP address for the next hop router to be displayed.

static | rip | ospf – Enter one of these parameters to show that corresponding IP route.

Restrictions None.

Example usage:

To display the contents of the IP routing table:

```
DGS-3627:5#show iproute
Command: show iproute

Routing Table

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

Total Entries : 1

DGS-3627:5#
```

create ipv6route

Purpose	Used to create IPv6 route entries to the Switch's IP routing table.
Syntax	create ipv6route [default <ipv6networkaddr>] [<ipif_name 12 <ipv6addr> <ipv6addr>] {<metric 1-65535>} {[primary backup]}
Description	This command is used to create a primary and backup IP route entry to the Switch's IP routing table.
Parameters	<p><i>default</i> – Use this parameter to create a default static IPv6 route entry to the Switch's IP routing table.</p> <p><i><ipv6networkaddr></i> – IPv6 address and netmask of the IP interface that is the destination of the route. Specify the address and mask information using the format as ipv6address / prefix_length (ipv6address is hexadecimal number, prefix length is decimal number, for example 1234::5D7F/32).</p> <p><i>ipif_name 12</i> – Enter the corresponding ipif name of the IPv6 address.</p> <p><i><ipv6addr></i> – IPv6 address for the next hop router.</p> <p><i><metric 1-65535></i> – 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.</p> <p><i>[primary backup]</i> - The user may choose between Primary and Backup. If the Primary Static/Default Route fails, the Backup Route will support the entry. Please take note that the Primary and Backup entries cannot have the same Gateway.</p>
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To add a single static IPv6 entry in IPv6 format:


```
DGS-3627:5#create ipv6route 1234::5D7F/32 2D30::AC21
Command:create ipv6route 1234::5D7F/32 2D30::AC21

Success.

DGS-3627:5#
```

delete ipv6route

Purpose	Used to delete an static IPv6 route entry from the Switch's IP routing table.
Syntax	delete ipv6route [[default <ipv6networkaddr>] [<ipif_name 12> <ipv6addr> <ipv6addr>] all]
Description	This command will delete an existing static IPv6 entry from the Switch's IP routing table.
Parameters	<p><i>default</i> – Use this parameter to delete a default static IPv6 route entry to the Switch's IP routing table.</p> <p><i><ipv6networkaddr></i> – IPv6 address and netmask of the IP interface that is the destination of the route. Specify the address and mask information using the format as ipv6address / prefix_length (ipv6address is hexadecimal number, prefix length is decimal number, for example 1234::5D7F/32).</p> <p><i><ipif_name 12></i> - Enter the corresponding IP interface name of the IPv6 address to be deleted here.</p> <p><i><ipv6addr></i> – IPv6 address for the next hop router.</p> <p><i>all</i> – This will delete all IPv6 static entries.</p>
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To delete a static IPv6 entry from the routing table:

```
DGS-3627:5# delete ipv6route 1234::5D7F/32 2D30::AC21
Command: delete ipv6route 1234::5D7F/32 2D30::AC21

Success.

DGS-3627:5#
```

show ipv6route

Purpose	Used to display the Switch's current static IPv6 routing table or a specified IPv6 address.
Syntax	show ipv6route { <ipv6networkaddr> }
Description	This command will display the Switch's current static IPv6 routing table or a specific IPv6 entry.
Parameters	<i><ipv6networkaddr></i> – IPv6 address and netmask of the IP interface that is the destination of the route. Specify the address and mask information using the format as ipv6address / prefix_length (ipv6address is hexadecimal number, prefix length is decimal number, for example 1234::5D7F/32).
Restrictions	None.

Example usage:

To display the static IPv6 entries in the routing table:

DGS-3627:5# show ipv6route

Command: show ipv6route

IPv6 Prefix	: ::/0	Protocol	: Static	Metric: 65535
Next Hop	: 3003::30	IPIF	: ip3	
Backup	: Backup	Status	: Active	
Total Entries	: 1			

DGS-3627:5#

ROUTE REDISTRIBUTION COMMANDS

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

Command	Parameters
create route redistribute dst ospf src	[static rip local] {mettype [1 2] metric <value 0-16777214>}
create route redistribute dst rip src	[local static ospf [all internal external type_1 type_2 inter+e1 inter+e2]] {metric <value 0-16>}
config route redistribute dst ospf src	[static rip local] {mettype [1 2] metric <value 0-16777214>}
config route redistribute dst rip src	[local static ospf [all internal external type_1 type_2 inter+e1 inter+e2]] {metric <value 0-16>}
delete route redistribute	[dst [rip ospf] src [rip static local ospf]]
show route redistribute	{dst [rip ospf] src [rip static local ospf]}

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

create route redistribute dst ospf src

Purpose	Used to add route redistribution settings for the exchange of RIP routes to OSPF routes on the Switch.
Syntax	create route redistribute dst ospf src [static rip local] {mettype [1 2] metric <value 0-16777214>}
Description	This command will redistribute routing information between the OSPF and RIP routing protocols to all routers on the network that are running OSPF or RIP. Routing information entered into the Static Routing Table on the local xStack switch is also redistributed.
Parameters	<p><i>src</i> [static rip local] – Allows for the selection of the protocol for the source device.</p> <p><i>mettype</i> [1 2] – Allows for the selection of one of two methods of calculating the metric value.</p> <ul style="list-style-type: none"> Type-1 calculates (for RIP to OSPF) by adding the destination's interface cost to the metric entered in the Metric field. Type-2 uses the metric entered in the Metric field without change. This field applies only when the destination field is OSPF. <p><i>metric</i> <value 0-16777214> – Allows the entry of an OSPF interface cost. This is analogous to a Hop Count in the RIP routing protocol.</p>
Restrictions	Only administrator-level and operator-level users can issue this command.

Routing information source – RIP, the Static Route table, and the Local interface routing information. Routing information will be redistributed to OSPF.

Route Source	Metric	Metric Type
RIP	0 to 16777214	mettype 1 mettype 2
Static	0 to 16777214	mettype 1 mettype 2
Local	0 to 16777214	mettype 1 mettype 2

Allowed Metric Type combinations are mettype 1 or mettype 2. The metric value 0 above will be redistributed in OSPF as the metric 20.

Example usage:

To add route redistribution settings:

```
DGS-3627:5#create route redistribute dst ospf src rip
Command: create route redistribute dst ospf src rip

Success.

DGS-3627:5#
```

create route redistribute dst rip src	
Purpose	Used to add route redistribution settings for the exchange of OSPF routes to RIP routes on the Switch.
Syntax	create route redistribute dst rip src [local static ospf [all internal external type_1 type_2 inter+e1 inter+e2]] {metric <value 0-16>}
Description	This command will redistribute routing information between the OSPF and RIP routing protocols to all routers on the network that are running OSPF or RIP. Routing information entered into the Static Routing Table on the local xStack switch is also redistributed
Parameters	<p><i>src</i> – Allows the selection of the protocol of the source device, as being either local, static or OSPF. After selecting the source device, the user may set the following parameters for that source device from the following options:</p> <ul style="list-style-type: none"> • <i>all</i> – Specifies both internal an external. • <i>internal</i> – Specifies the internal protocol of the source device. • <i>external</i> - Specifies the external protocol of the source device. • <i>type_1</i> - Calculates the metric (for RIP to OSPF) by adding the destination’s interface cost to the metric entered in the Metric field. • <i>type_2</i> - Uses the metric entered in the Metric field without change. This field applies only when the destination field is OSPF. • <i>inter+e1</i> – Specifies the internal protocol AND type 1 of the external protocol. • <i>inter+e2</i> – Specifies the internal protocol AND type 2 of the external protocol. <p><i>metric <value 0-16></i> – Allows the entry of an OSPF interface cost. This is analogous to a HOP Count in the RIP routing protocol.</p>
Restrictions	Only administrator-level and operator-level users can issue this command.

Routing information source – OSPF and the Static Route table. Routing information will be redistributed to RIP. The following table lists the allowed values for the routing metrics and the types (or forms) of the routing information that will be redistributed.

Route Source	Metric	Type
OSPF	0 to 16	all type_1 type_2 inter+e1 inter+e2 external internal
Static	0 to 16	not applicable
Local	0 to 16	route source

Entering the Type combination – **Internal, ExtType_1, ExtType_2** is functionally equivalent to **All**. Entering the combination **ExtType_1, ExtType_2** is functionally equivalent to **External**. Entering the combination **Internal, External** is functionally equivalent to **All**.

Entering the metric 0 specifies transparency.

Example usage:

To add route redistribution settings

```
DGS-3627:5#create route redistribute dst rip src ospf all metric 2
Command: create route redistribute dst rip src ospf all metric 2

Success.

DGS-3627:5#
```

config route redistribute dst ospf src

Purpose	Used configure route redistribution settings for the exchange of RIP routes to OSPF routes on the Switch.
Syntax	config route redistribute dst ospf src [static rip local] {mettype [1 2] metric <value 0-16777214>}
Description	Route redistribution allows routers on the network – that are running different routing protocols to exchange routing information. This is accomplished by comparing the routes stored in the various router's routing tables and assigning appropriate metrics. This information is then exchanged among the various routers according to the individual router's current routing protocol. The switch can redistribute routing information between the OSPF and RIP routing protocols to all routers on the network that are running OSPF or RIP. Routing information entered into the Static Routing Table on the local switch is also redistributed.
Parameters	<p><i>src [static rip local]</i> – Allows the selection of the protocol of the source device.</p> <p><i>mettype</i> – allows the selection of one of the methods for calculating the metric value.</p> <ul style="list-style-type: none"> • Type - 1 calculates the metric (for RIP to OSPF) by adding the destination's interface cost to the metric entered in the Metric field. • Type - 2 uses the metric entered in the Metric field without change. This field applies only when the destination field is OSPF. <p><i>metric <value 0-16777214></i> – Allows the entry of an OSPF interface cost. This is analogous to a Hop Count in the RIP routing protocol.</p>
Restrictions	Only administrator-level and operator-level users can issue this command.

Routing information source – RIP: the Static Route table, and the Local interface routing information. Routing information will be redistributed to OSPF. The following table lists the allowed values for the routing metrics and the types (or forms) of the routing information that will be redistributed.

Route Source	Metric	Metric Type
RIP	0 to 16777214	mettype 1 mettype 2
Static	0 to 16777214	mettype 1 mettype 2
Local	0 to 16777214	mettype 1 mettype 2

Allowed Metric Type combinations are mettype 1 or mettype 2. The metric value 0 above will be redistributed in OSPF as the metric 20.

Example usage:

To configure route redistributions:

```
DGS-3627:5#config route redistribute dst ospf src all metric 2
Command: config route redistribute dst ospf src all metric 2

Success.

DGS-3627:5#
```

config route redistribute dst rip src	
Purpose	Used configure route redistribution settings for the exchange of RIP routes to OSPF routes on the Switch.
Syntax	config route redistribute dst rip src [local static ospf [all internal external type_1 type_2 inter+e1 inter+e2]] {metric <value 0-16>}
Description	Route redistribution allows routers on the network that are running different routing protocols to exchange routing information. This is accomplished by comparing the routes stored in the various router's routing tables and assigning appropriate metrics. This information is then exchanged among the various routers according to the individual routers current routing protocol. The Switch can redistribute routing information between the OSPF and RIP routing protocols to all routers on the network that are running OSPF or RIP. Routing information entered into the Static Routing Table on the local switch is also redistributed.
Parameters	<p><i>src</i> - Allows the selection of the protocol of the source device, as being either local, static or OSPF. After selecting the source device, the user may set the following parameters for that source device from the following options:</p> <ul style="list-style-type: none"> • <i>all</i> – Specifies both internal an external. • <i>internal</i> – Specifies the internal protocol of the source device. • <i>external</i> - Specifies the external protocol of the source device. • <i>type_1</i> - Calculates the metric (for RIP to OSPF) by adding the destination's interface cost to the metric entered in the Metric field. • <i>type_2</i> - Uses the metric entered in the Metric field without change. This field applies only when the destination field is OSPF. • <i>inter+e1</i> – Specifies the internal protocol AND type 1 of the external protocol. • <i>inter+e2</i> – Specifies the internal protocol AND type 2 of the external protocol. <p><i>metric <value 0-16></i> – Allows the entry of an OSPF interface cost. This is analogous to a Hop Count in the RIP routing protocol.</p>
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To configure route redistributions:

```
DGS-3627:5#config route redistribute dst ospf src rip mettype type_1 metric 2
Command: config route redistribute dst ospf src rip mettype type_1 metric 2

Success.
```

DGS-3627:5#

delete route redistribute

Purpose	Used to delete an existing route redistribute configuration on the Switch.
Syntax	delete route redistribute {dst [rip ospf] src [rip static local ospf]}
Description	This command will delete the route redistribution settings on this switch.
Parameters	<i>dst [rip ospf]</i> – Allows the selection of the protocol on the destination device. The user may choose between RIP and OSPF. <i>src [rip static local ospf]</i> – Allows the selection of the protocol on the source device. The user may choose between RIP, static, local or OSPF.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To delete route redistribution settings:

```
DGS-3627:5#delete route redistribute dst rip src ospf
Command: delete route redistribute dst rip src ospf

Success.

DGS-3627:5#
```

show route redistribute

Purpose	Used to display the route redistribution on the Switch.
Syntax	show route redistribute {dst [rip ospf] src [rip static local ospf]}
Description	Displays the current route redistribution settings on the Switch.
Parameters	<i>src [rip static local ospf]</i> – Allows the selection of the routing protocol on the source device. The user may choose between RIP, static, local or OSPF. <i>dst [rip ospf]</i> – Allows the selection of the routing protocol on the destination device. The user may choose between RIP and OSPF.
Restrictions	None.

Example Usage:

To display route redistributions:

```
DGS-3627:5#show route redistribute
Command: show route redistribute

Source  Destination Type      Metric
Protocol Protocol
-----
STATIC  RIP       All       1
LOCAL   OSPF      Type-2    20

Total Entries : 2

DGS-3627:5#
```

DNS COMMANDS

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

Command	Parameters
config dnsm	[[primary secondary] nameserver <ipaddr> [add delete] static <domain_name 32> <ipaddr>]
enable dnsm	{[cache static]}
disable dnsm	{[cache static]}
show dnsm	{static}

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

config dnsm	
Purpose	Used to configure the DNS relay function.
Syntax	config dnsm [[primary secondary] nameserver <ipaddr> [add delete] static <domain_name 32> <ipaddr>]
Description	This command is used to configure the DNS relay function on the Switch.
Parameters	<p><i>primary</i> – Indicates that the IP address below is the address of the primary DNS server.</p> <p><i>secondary</i> – Indicates that the IP address below is the address of the secondary DNS server.</p> <p><i>nameserver <ipaddr></i> – The IP address of the DNS nameserver.</p> <p><i>[add delete]</i> – Indicates whether to add or delete the DNS relay function.</p> <p><i><domain_name 32></i> – The domain name of the entry.</p> <p><i><ipaddr></i> – The IP address of the entry.</p>
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To set IP address 10.43.21.12 of primary.

```
DGS-3627:5#config dnsm primary 10.43.21.12
Command: config dnsm primary 10.43.21.12

Success

DGS-3627:5#
```

Example usage:

To add an entry domain name dns1, IP address 10.43.21.12 to DNS static table:

```
DGS-3627:5#config dnsm add static dns1 10.43.21.12
Command: config dnsm add static dns1 10.43.21.12

Success.

DGS-3627:5#
```


Example usage:

To delete an entry domain name dns1, IP address 10.43.21.12 from DNS static table.

```
DGS-3627:5#config dnsr delete static dns1 10.43.21.12
Command: config dnsr delete static dns1 10.43.21.12

Success.

DGS-3627:5#
```

enable dnsr

Purpose	Used to enable DNS relay.
Syntax	enable dnsr {[cache static]}
Description	This command is used, in combination with the disable dnsr command below, to enable and disable DNS Relay on the Switch.
Parameters	<i>cache</i> - This parameter will allow the user to enable the cache lookup for the DNS relay on the Switch. <i>static</i> - This parameter will allow the user to enable the static table lookup for the DNS relay on the Switch.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To enable status of DNS relay:

```
DGS-3627:5#enable dnsr
Command: enable dnsr

Success.

DGS-3627:5#
```

Example usage:

To enable cache lookup for DNS relay.

```
DGS-3627:5#enable dnsr cache
Command: enable dnsr cache

Success.

DGS-3627:5#
```

Example usage:

To enable static table lookup for DNS relay.

```
DGS-3627:5#enable dnsr static
Command: enable dnsr static

Success.

DGS-3627:5#
```

disable dnsr

Purpose	Used to disable DNS relay on the Switch.
Syntax	disable dnsr {[cache static]}
Description	This command is used, in combination with the enable dnsr command above, to enable and disable DNS Relay on the Switch.
Parameters	<i>cache</i> – This parameter will allow the user to disable the cache lookup for the DNS relay on the Switch. <i>static</i> – This parameter will allow the user to disable the static table lookup for the DNS relay on the Switch.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To disable status of DNS relay.

```
DGS-3627:5#disable dnsr
Command: disable dnsr

Success.

DGS-3627:5#
```

Example usage:

To disable cache lookup for DNS relay.

```
DGS-3627:5#disable dnsr cache
Command: disable dnsr cache

Success.

DGS-3627:5#
```

Example usage:

To disable static table lookup for DNS relay.

```
DGS-3627:5#disable dnsr static
Command: disable dnsr static

Success.

DGS-3627:5#
```

show dnsr

Purpose	Used to display the current DNS relay status.
Syntax	show dnsr {static}
Description	This command is used to display the current DNS relay status.
Parameters	<i>static</i> – Allows the display of only the static entries into the DNS relay table. If this parameter is omitted, the entire DNS relay table will be displayed.
Restrictions	None.

Example usage:

To display DNS relay status:

```
DGS-3627:5#show dnsr
Command: show dnsr

DNSR Status           : Disabled
Primary Name Server   : 0.0.0.0
Secondary Name Server : 0.0.0.0
DNSR Cache Status     : Disabled
DNSR Static Cache Table Status : Disabled

DNS Relay Static Table

Domain Name           IP Address
-----
www.123.com.tw        10.12.12.123
bbs.ntu.edu.tw        140.112.1.23

Total Entries: 2

DGS-3627:5#
```

RIP COMMANDS

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

Command	Parameters
config rip	[ipif <ipif_name 12> all] {authentication [enable <password 16> disable] tx_mode [disable v1_only v1_compatible v2_only] rx_mode [v1_only v2_only v1_or_v2 disable] state [enable disable]}
enable rip	
disable rip	
show rip	ipif <ipif_name 12>

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

config rip	
Purpose	Used to configure RIP on the Switch.
Syntax	config rip [ipif <ipif_name 12> all] {authentication [enable <password 16> disable] tx_mode [disable v1_only v1_compatible v2_only] rx_mode [v1_only v2_only v1_or_v2 disable] state [enable disable]}
Description	This command is used to configure RIP on the Switch.
Parameters	<p><ipif_name 12> – The name of the IP interface.</p> <p><i>all</i> – To configure all RIP receiving mode for all IP interfaces.</p> <p><i>authentication [enable disable]</i> – Enables or disables authentication for RIP on the Switch.</p> <ul style="list-style-type: none"> • <password 16> – Allows the specification of a case-sensitive password. <p><i>tx_mode</i> – Determines how received RIP packets will be interpreted – as RIP version <i>V1 only</i>, <i>V2 Only</i>, or <i>V1 Compatible (V1 and V2)</i>. This entry specifies which version of the RIP protocol will be used to transfer RIP packets. The disabled entry prevents the reception of RIP packets.</p> <ul style="list-style-type: none"> • <i>disable</i> – Prevents the transmission of RIP packets. • <i>v1_only</i> – Specifies that only RIP v1 packets will be transmitted. • <i>v1_compatible</i> – Specifies that only RIP v1 compatible packets will be transmitted. • <i>v2_only</i> - Specifies that only RIP v2 packets will be transmitted. <p><i>rx_mode</i> – Determines how received RIP packets will be interpreted – as RIP version <i>V1 only</i>, <i>V2 Only</i>, or <i>V1 or V2</i>. This entry specifies which version of the RIP protocol will be used to receive RIP packets. The <i>disable</i> entry prevents the reception of RIP packets.</p> <ul style="list-style-type: none"> • <i>v1_only</i> – Specifies that only RIP v1 packets will be transmitted. • <i>v2_only</i> - Specifies that only RIP v2 packets will be transmitted. • <i>v1_or_v2</i> - Specifies that only RIP v1 or v2 packets will be transmitted. <p><i>state [enable disable]</i> – Allows RIP to be enabled and disabled on the Switch.</p>
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To change the RIP receive mode for the IP interface System:

```
DGS-3627:5#config rip ipif System rx_mode v1_only
Command: config rip ipif System rx_mode v1_only

Success.

DGS-3627:5#
```

enable rip

Purpose	Used to enable RIP.
Syntax	enable rip
Description	This command is used to enable RIP on the Switch.
Parameters	None.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example Usage:

To enable RIP:

```
DGS-3627:5#enable rip
Command: enable rip

Success.

DGS-3627:5#
```

disable rip

Purpose	Used to disable RIP.
Syntax	disable rip
Description	This command is used to disable RIP on the Switch.
Parameters	None.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To disable RIP:

```
DGS-3627:5#disable rip
Command: disable rip

Success.

DGS-3627:5#
```

show rip

Purpose	Used to display the RIP configuration and statistics for the Switch.
Syntax	show rip {ipif <ipif_name 12>}
Description	This command will display the RIP configuration and statistics for a given IP interface or for all IP interfaces.
Parameters	<i>ipif <ipif_name 12></i> – The name of the IP interface for which to display the RIP configuration and settings. If this parameter is not specified, the show rip command will display the global RIP configuration for the Switch.
Restrictions	None.

Example usage:

To display RIP configuration:

```
DGS-3627:5#show rip
Command: show rip

RIP Global State : Disabled

RIP Interface Settings

Interface  IP Address      TX Mode  RX Mode  Authen-  State
-----  -
System    10.41.44.33/8   Disabled Disabled  Disabled Disabled

Total Entries : 1

DGS-3627:5#
```

Example usage:

To display RIP configurations by IP interface:

```
DGS-3627:5#show rip ipif System
Command: show rip ipif System

RIP Interface Settings

Interface Name: System          IP Address: 10.53.13.33/8 (Link Up)
Interface Metric: 1             Administrative State: Disabled
TX Mode: V2 Only                RX Mode: V1 or V2
Authentication: Disabled

Total Entries: 1

DGS-3627:5#
```

DVMRP COMMANDS

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

Command	Parameters
config dvmrp	[ipif <ipif_name 12> all] {metric <value 1-31> probe <sec 1-65535> neighbor_timeout <sec 1-65535> state [enable disable]}
enable dvmrp	
disable dvmrp	
show dvmrp neighbor	{ipif <ipif_name 12> ipaddress <network_address>}
show dvmrp nexthop	{ipaddress <network_address> ipif <ipif_name 12>}
show dvmrp routing_table	{ipaddress <network_address>}
show dvmrp	{ipif <ipif_name 12>}

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

config dvmrp	
Purpose	Used to configure DVMRP on the Switch.
Syntax	config dvmrp [ipif <ipif_name 12> all] {metric <value 1-31> probe <sec 1-65535> neighbor_timeout <sec 1-65535> state [enable disable]}
Description	This command is used to configure DVMRP on the Switch.
Parameters	<p><i>ipif <ipif_name 12></i> – The name of the IP interface for which DVMRP is to be configured.</p> <p><i>all</i> – Specifies that DVMRP is to be configured for all IP interfaces on the Switch.</p> <p><i>metric <value 1-31></i> – Allows the assignment of a DVMRP route cost to the above IP interface. A DVMRP route cost is a relative number that represents the real cost of using this route in the construction of a multicast delivery tree. It is similar to, but not defined as, the hop count in RIP. The default is 1.</p> <p><i>probe <second 1-65535></i> – DVMRP defined an extension to IGMP that allows routers to query other routers to determine if a DVMRP neighbor is present on a given subnetwork or not. This is referred to as a 'probe'. This entry will set an intermittent probe (in seconds) on the device that will transmit dvmrp messages, depending on the time specified. This probe is also used to "keep alive" the connection between DVMRP enabled devices. The default value is 10 seconds.</p> <p><i>neighbor_timeout <second 1-65535></i> – The time period for which DVMRP will hold Neighbor Router reports before issuing poison route messages. The default value is 35 seconds.</p> <p><i>state [enable disable]</i> – Allows DVMRP to be enabled or disabled.</p>
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To configure DVMRP configurations of IP interface System:

```
DGS-3627:5#config dvmrp ipif System neighbor_timeout 30 metric 1 probe 5
Command: config dvmrp ipif System neighbor_timeout 30 metric 1 probe 5

Success

DGS-3627:5#
```

enable dvmrp

Purpose	Used to enable DVMRP.
Syntax	enable dvmrp
Description	This command, in combination with the disable dvmrp command below, is used to enable and disable DVMRP on the Switch.
Parameters	None.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To enable DVMRP:

```
DGS-3627:5#enable dvmrp
Command: enable dvmrp

Success.

DGS-3627:5#
```

disable dvmrp

Purpose	Used to disable DVMRP.
Syntax	disable dvmrp
Description	This command is used, in combination with the enable dvmrp command above, is used to enable and disable DVMRP on the Switch.
Parameters	None.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To disable DVMRP:

```
DGS-3627:5#disable dvmrp
Command: disable dvmrp

Success.

DGS-3627:5#
```

show dvmrp routing_table

Purpose	Used to display the current DVMRP routing table.
Syntax	show dvmrp routing table [ipaddress <network_address>]

show dvmrp routing_table

Description	The command is used to display the current DVMRP routing table.
Parameters	<i>ipaddress <network_address></i> – The IP address and netmask of the destination. The address and mask information can be specified using the traditional format (for example, 10.1.2.3/255.0.0.0 or in CIDR format, 10.1.2.3/8).
Restrictions	None.

Example usage:

To display DVMRP routing table:

```
DGS-3627:5#show dvmrp routing_table
Command: show dvmrp routing_table

DVMRP Routing Table
Source Address/Netmask  Upstream Neighbor  Metric  Learned  Interface  Expire
-----
10.0.0.0/8              10.90.90.90        1       Local    System     -
20.0.0.0/8              20.1.1.1           2       Dynamic  ip2        117
30.0.0.0/8              30.1.1.1           2       Dynamic  ip3        106

Total Entries: 3

DGS-3627:5#
```

show dvmrp neighbor

Purpose	Used to display the DVMRP neighbor table.
Syntax	show dvmrp neighbor {ipif <ipif_name 12> ipaddress <network_address>}
Description	This command will display the current DVMRP neighbor table.
Parameters	<i><ipif_name 12></i> – The name of the IP interface for which to display the DVMRP neighbor table. <i>ipaddress <network_address></i> – The IP address and netmask of the destination. The address and mask information can be specified using the traditional format (for example, 10.1.2.3/255.0.0.0 or in CIDR format, 10.1.2.3/8).
Restrictions	None.

Example usage:

To display DVMRP neighbor table:

```
DGS-3627:5#show dvmrp neighbor
Command: show dvmrp neighbor

DVMRP Neighbor Address Table

Interface  Neighbor Address  Generation ID  Expire Time
-----
System     10.2.1.123       2              35

Total Entries: 1

DGS-3627:5#
```

show dvmrp nexthop

Purpose	Used to display the current DVMRP routing next hop table.
Syntax	show dvmrp nexthop {ipaddress <network_address> ipif <ipif_name 12>}
Description	This command will display the DVMRP routing next hop table.
Parameters	<ipif_name 12> – The name of the IP interface for which to display the current DVMRP routing next hop table. ipaddress <network_address> – The IP address and netmask of the destination. The address and mask information can be specified using the traditional format (for example, 10.1.2.3/255.0.0.0 or in CIDR format, 10.1.2.3/8).
Restrictions	None.

Example usage:

To display DVMRP routing next hop table:

```
DGS-3627:5#show dvmrp nexthop
Command: show dvmrp nexthop

Source IP Address/Netmask  Interface Name  Type
-----
10.0.0.0/8                 ip2             Leaf
10.0.0.0/8                 ip3             Leaf
20.0.0.0/8                 System          Leaf
20.0.0.0/8                 ip3             Leaf
30.0.0.0/8                 System          Leaf
30.0.0.0/8                 ip2             Leaf

Total Entries: 6

DGS-3627:5#
```

show dvmrp

Purpose	Used to display the current DVMRP settings on the Switch.
Syntax	show dvmrp {<ipif_name 12>}
Description	The command will display the current DVMRP configurations.
Parameters	<ipif_name 12> – This parameter will allow the user to display DVMRP settings for a specific IP interface.
Restrictions	None.

Example usage:

To show DVMRP configurations:

DGS-3627:5#show dvmrp

Command: show dvmrp

DVMRP Global State : Disabled

Interface	IP Address	Neighbor Timeout	Probe	Metric	State
System	10.90.90.90/8	35	10	1	Disabled
Zira	12.1.1.1/8	35	10	1	Enabled

Total Entries: 2

DGS-3627:5#

PIM COMMANDS

PIM or Protocol Independent Multicast is a method of forwarding traffic to multicast groups over the network using any pre-existing unicast routing protocol, such as RIP or OSPF, set on routers within a multicast network. The xStack DGS-3600 Series supports three types of PIM, Dense Mode (PIM-DM), Sparse Mode (PIM-SM), and Sparse and Dense Mode (PIM-SM-DM).

PIM-SM

PIM-SM or Protocol Independent Multicast – Sparse Mode is a method of forwarding multicast traffic over the network only to multicast routers who actually request this information. Unlike most multicast routing protocols which flood the network with multicast packets, PIM-SM will forward traffic to routers who are explicitly a part of the multicast group through the use of a Rendezvous Point (RP). This RP will take all requests from PIM-SM enabled routers, analyze the information and then returns multicast information it receives from the source, to requesting routers within its configured network. Through this method, a distribution tree is created, with the RP as the root. This distribution tree holds all PIM-SM enabled routers within which information collected from these router is stored by the RP.

Two other types of routers also exist with the PIM-SM configuration. When many routers are a part of a multiple access network, a Designated Router (DR) will be elected. The DR's primary function is to send Join/Prune messages to the RP. The router with the highest priority on the LAN will be selected as the DR. If there is a tie for the highest priority, the router with the higher IP address will be chosen.

The third type of router created in the PIM-SM configuration is the Boot Strap Router (BSR). The goal of the Boot Strap Router is to collect and relay RP information to PIM-SM enabled routers on the LAN. Although the RP can be statically set, the BSR mechanism can also determine the RP. Multiple Candidate BSRs (C-BSR) can be set on the network but only one BSR will be elected to process RP information. If it is not explicitly apparent which C-BSR is to be the BSR, all C-BSRs will emit Boot Strap Messages (BSM) out on the PIM-SM enabled network to determine which C-BSR has the higher priority and once determined, will be elected as the BSR. Once determined, the BSR will collect RP data emanating from candidate RPs on the PIM-SM network, compile it and then send it out on the land using periodic Boot Strap Messages (BSM). All PIM-SM Routers will get the RP information from the Boot Strap Mechanism and then store it in their database.

Discovering and Joining the Multicast Group

Although Hello packets discover PIM-SM routers, these routers can only join or be “pruned” from a multicast group through the use of Join/Prune Messages exchanged between the DR and RP. Join/Prune Messages are packets relayed between routers that effectively state which interfaces are, or are not to be receiving multicast data. These messages can be configured for their frequency to be sent out on the network and are only valid to routers if a Hello packet has first been received. A Hello packet will simply state that the router is present and ready to become a part of the RP's distribution tree. Once a router has accepted a member of the IGMP group and it is PIM-SM enabled, the interested router will then send an explicit Join/Prune message to the RP, which will in turn route multicast data from the source to the interested router, resulting in a unidirectional distribution tree for the group. Multicast packets are then sent out to all nodes on this tree. Once a prune message has been received for a router that is a member of the RP's distribution tree, the router will drop the interface from its distribution tree.

Distribution Trees

Two types of distribution trees can exist within the PIM-SM protocol, a Rendezvous-Point Tree (RPT) and a Shortest Path Tree (SPT). The RP will send out specific multicast data that it receives from the source to all outgoing interfaces enabled to receive multicast data. Yet, once a router has determined the location of its source, an SPT can be created, eliminating hops between the source and the destination, such as the RP. This can be configured by the switch administrator by setting the multicast data rate threshold. Once the threshold has been passed, the data path will switch to the SPT. Therefore, a closer link can be created between the source and destination, eliminating hops previously used and shortening the time a multicast packet is sent from the source to its final destination.

Register and Register Suppression Messages

Multicast sources do not always join the intended receiver group. The first hop router (DR) can send multicast data without being the member of a group or having a designated source, which essentially means it has no information about how to relay this information to the RP distribution tree. This problem is alleviated through Register and Register-Stop messages. The first multicast packet received by the DR is encapsulated and sent on to the RP which in turn removes the encapsulation and sends the packet on down the RP distribution tree. When the route has been established, a SPT can be created to directly connect routers to the source, or the multicast traffic flow can begin, traveling from the DR to the RP. When the latter occurs, the same packet may be sent twice, one type encapsulated, one not. The RP will detect this flaw and then return a Register Suppression message to the DR requesting it to discontinue sending encapsulated packets.

Assert Messages

At times on the PIM-SM enabled network, parallel paths are created from source to receiver, meaning some receivers will receive the same multicast packets twice. To improve this situation, Assert messages are sent from the receiving device to both multicast sources to determine which single router will send the receiver the necessary multicast data. The source with the shortest metric (hop count) will be elected as the primary multicast source. This metric value is included within the Assert message.

PIM-DM

The Protocol Independent Multicast - Dense Mode (PIM-DM) protocol should be used in networks with a low delay (low latency) and high bandwidth as PIM-DM is optimized to guarantee delivery of multicast packets, not to reduce overhead.

The PIM-DM multicast routing protocol assumes that all downstream routers want to receive multicast messages and relies upon explicit prune messages from downstream routers to remove branches from the multicast delivery tree that do not contain multicast group members.

PIM-DM has no explicit 'join' messages. It relies upon periodic flooding of multicast messages to all interfaces and then either waiting for a timer to expire (the Join/Prune Interval) or for the downstream routers to transmit explicit 'prune' messages indicating that there are no multicast members on their respective branches. PIM-DM then removes these branches ('prunes' them) from the multicast delivery tree.

Because a member of a pruned branch of a multicast delivery tree may want to join a multicast delivery group (at some point in the future), the protocol periodically removes the 'prune' information from its database and floods multicast messages to all interfaces on that branch. The interval for removing 'prune' information is the Join/Prune Interval.

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

Command	Parameters
enable pim	
disable pim	
config pim	[[ipif <ipif_name 12> all] {hello <sec 1-18724> jp_interval <sec 1-18724> state [enable disable] mode [dm sm sm-dm] dr_priority <unit 0 – 4294967294>} register_probe_time <value 1-127> register_suppression_time <value 3-255>]
create pim crp group	<network_address> rp <ipif_name 12>
delete pim crp group	<network_address>
config pim crp	{holdtime <value 0-255> priority <value 0-255> wildcard_prefix_cnt [0 1]}
create pim static_rp group	<network_address> rp <ipaddr>
delete pim static_rp group	<network_address>
show pim static_rp	
config pim last_hop_spt_switchover	[never immediately]
show pim rpset	
show pim crp	
config pim cbsr	[ipif <ipif_name 12> {priority [-1 <value 0-255>]} hash_masklen <value 0-32> bootstrap_period <value 1-255>]
show pim cbsr	{ipif <ipif_name 12>}
show pim	{ipif <ipif_name 12>}
show pim neighbor	{ipif <ipif_name 12> ipaddress <network_address>}
show pim ipmroute	
create pim register_checksum_include_data rp_address	<ipaddr>

Command	Parameters
delete pim register_checksum_include_data rp_address	<ipaddr>
show pim register_checksum_include_data_rp_list	

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

enable pim

Purpose	Used to enable the PIM function on the Switch.
Syntax	enable pim
Description	This command will enable PIM for the Switch.
Parameters	None.
Restrictions	Only administrator-level and operator-level users can issue this command.

Usage example:

To enable PIM as previously configured on the Switch:

```
DGS-3627:5#enable pim
Command: enable pim

Success.

DGS-3627:5#
```

disable pim

Purpose	Used to disable PIM function on the Switch.
Syntax	disable pim
Description	This command will disable PIM for the Switch. Any previously configured PIM settings will remain unchanged and may be enabled at a later time with the enable pim command.
Parameters	None.
Restrictions	Only administrator-level and operator-level users can issue this command.

Usage example:

To disable PIM on the Switch:

```
DGS-3627:5#disable pim
Command: disable pim

Success.

DGS-3627:5#
```

config pim

Purpose	Used to configure the parameters for the PIM protocol.
Syntax	config pim [[ipif <ipif_name 12> all] {hello <sec 1-18724> jp_interval <sec 1-18724> state [enable disable] mode [dm sm sm-dm] dr_priority <unit 0 – 4294967294>} register_probe_time <value 1-127> register_suppression_time <value 3-255>]
Description	This command will configure the general settings for the PIM protocol per IP interface, including choice of PIM mode, Designated Router priority and various timers.
Parameters	<p><i>ipif <ipif_name 12></i> - Enter an IP interface for which to configure the PIM settings. This name cannot exceed 12 alphanumeric characters.</p> <p><i>all</i> – Select this parameter to configure PIM settings for all IP interfaces on the Switch.</p> <p><i>hello <sec 1-18724></i> - Used to set the interval time between the sending of Hello Packets from this IP interface to neighboring routers one hop away. These Hello packets are used to discover other PIM enabled routers and state their priority as the Designated Router (DR) on the PIM enabled network. The user may state an interval time between 1 and 18724 seconds with a default interval time of 30 seconds.</p> <p><i>jp_interval <sec 1-18724></i> - This field will set the interval time between the sending of Join/Prune packets stating which multicast groups are to join the PIM enabled network and which are to be removed or “pruned” from that group. The user may state an interval time between 1 and 18724 seconds with a default interval time of 30 seconds.</p> <p><i>state [enable disable]</i> - Used to enable or disable PIM for this IP interface. The default is Disabled.</p> <p><i>mode [dm sm sm-dm]</i> - Used to select the type of PIM protocol to use, Sparse Mode (SM), Dense Mode (DM), or Spare-Dense Mode (SM-DM). The default setting is DM.</p> <p><i>dr_priority <unsigned_int 0 – 4294967294></i> - Enter the priority of this IP interface to become the Designated Router for the multiple access network. The user may enter a DR priority between 0 and 4,294,967,294 with a default setting of 1.</p> <p><i>register_probe_time <value 1-127></i> - Configure this field to set a time to send a probe message from the DR to the RP before the Register Suppression time expires. The user may configure a time between 1and 127 seconds with a default setting of 5 seconds.</p> <p><i>register_suppression_time <value 3-255></i> - <i><value 3-255></i> - The user may set an interval time between 3 and255 with a default setting of 60 seconds for the sending of register suppression time packets. The default value is 60 seconds.</p>
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To configure the PIM settings for an IP interface:

```
DGS-3627:5#config pim ipif Zira hello 60 jp_interval 60 state enable mode sm
```

```
Command: config pim ipif Zira hello 60 jp_interval 60 state enable mode sm
```

Success.

```
DGS-3627:5#
```



NOTE: The Probe time value must be less than half of the Register Suppression Time value. If not, the administrator will be presented with a Fail message.

create pim crp

Purpose	To enable the Switch to become a candidate to be the Rendezvous Point (RP).
Syntax	create pim crp group <network_address> rp <ipif_name 12>
Description	This command will set the parameters for the switch to become a candidate RP. This command is for PIM-SM configurations only.
Parameters	<i>group <network_address></i> - Enter the multicast group address for this switch to become a Candidate RP. This address must be a class D address. <i>rp <ipif_name 12></i> - Enter the name of the PIM-SM enabled interface the switch administrator wishes to become the CRP for this group.
Restrictions	Only administrator-level and operator-level users can issue this command.

Usage example:

To create an IP interface to become a Candidate RP on the Switch:

```
DGS-3627:5#create pim crp group 231.0.0.1/32 rp Zira
Command: create pim crp group 231.0.0.1/32 rp Zira

Success.

DGS-3627:5#
```

delete pim crp

Purpose	To disable the Switch in becoming a possible candidate to be the Rendezvous Point (RP).
Syntax	delete pim crp group <network_address>
Description	This command remove the switch's status of Candidate RP. This command is for PIM-SM configurations only.
Parameters	<i>group <network_address></i> - Enter the multicast group address for this switch to be removed from being a Candidate RP. This address must be a class D address.
Restrictions	Only administrator-level and operator-level users can issue this command.

Usage example:

To delete an IP interface from becoming a Candidate RP on the Switch:

```
DGS-3627:5#delete pim crp group 231.0.0.1/32
Command: delete pim crp group 231.0.0.1/32

Success.

DGS-3627:5#
```


config pim crp

Purpose	To configure the Candidate RP settings that will determine the RP.
Syntax	config pim crp {holdtime <value 0-255> priority <value 0-255> wildcard_prefix_cnt [0 1]}
Description	This command will configure parameters regarding the Candidate RP on the Switch, including hold time, priority and wildcard prefix count. This command is for PIM-SM configurations only.
Parameters	<p><i>holdtime <value 0-255></i> - This field is used to set the time Candidate RP (CRP) advertisements are valid on the PIM-SM enabled network. If CRP advertisements are not received by the BSR within this time frame, the CRP is removed from the list of candidates. The user may set a time between 0 and 255 seconds with a default setting of 150 seconds. An entry of 0 will send out one advertisement that states to the BSR that it should be immediately removed from CRP status on the PIM-SM network.</p> <p><i>priority <value 0-255></i> - Enter a priority value to determine which CRP will become the RP for the distribution tree. This priority value will be included in the router's CRP advertisements. A lower value means a higher priority, yet, if there is a tie for the highest priority, the router having the higher IP address will become the RP. The user may set a priority between 0 and 255 with a default setting of 192.</p> <p><i>wildcard_prefix_cnt [0 1]</i> - The user may set the Prefix Count value of the wildcard group address here by choosing a value between 0 and 1 with a default setting of 0.</p>
Restrictions	Only administrator-level and operator-level users can issue this command.

Usage example:

To configure the Candidate RP settings:

```
DGS-3627:5#config pim crp holdtime 150 priority 2 wildcard_prefix_cnt 0
Command: config pim crp holdtime 150 priority 2 wildcard_prefix_cnt 0

Success.

DGS-3627:5#
```

create pim static_rp

Purpose	Used to enter the multicast group IP address used in identifying the Rendezvous Point (RP).
Syntax	create pim static_rp group <network_address> rp <ipaddr>
Description	This command will enter the multicast group IP address which will be used to identify the RP. This entry must be a class D IP address. This command is for PIM-SM configurations only.
Parameters	<p><i>group <network_address></i> - Enter the multicast group IP address used in determining the Static RP. This address must be a class D IP address.</p> <p><i>rp <ipaddr></i> - Enter the IP address of the RP the switch administrator wishes to become the Static RP for this group.</p>
Restrictions	Only administrator-level and operator-level users can issue this command.

Usage example:

To create the settings to determine a static RP:

```
DGS-3627:5#create pim static_rp group 231.0.0.1/32 rp 11.1.1.1
Command: create pim static_rp group 231.0.0.1/32 rp 11.1.1.1

Success.

DGS-3627:5#
```

delete pim static_rp

Purpose	To remove the multicast group IP address used in identifying the Rendezvous Point (RP).
Syntax	delete pim static_rp group <network_address>
Description	This command will remove the multicast group IP address used in identifying the Rendezvous Point (RP). This command is for PIM-SM configurations only.
Parameters	<i>group <network_address></i> - Enter the multicast group IP address used in identifying the Rendezvous Point (RP). This address must be a class D address.
Restrictions	Only administrator-level and operator-level users can issue this command.

Usage example:

To remove the multicast group IP address used in identifying the Rendezvous Point (RP):

```
DGS-3627:5#delete pim static_rp group 231.0.0.1/32
Command: delete pim static_rp group 231.0.0.1/32

Success.

DGS-3627:5#
```

show pim static_rp

Purpose	To show the Static Rendezvous Point (RP) settings.
Syntax	show pim static_rp
Description	This command will display the Static Rendezvous Point (RP) settings. This command is for PIM-SM configurations only.
Parameters	None.
Restrictions	None.

Usage example:

To display the static RP settings as configured for the multiple access network:

```
DGS-3627:5#show pim static_rp
```

```
Command: show pim static_rp
```

PIM Static RP Table

Group	RP Address
24.0.0.0/4	11.1.1.254
239.0.0.1/32	31.1.1.1
239.0.0.2/32	31.1.1.12
239.0.0.3/32	31.1.1.123

```
Total entries: 4
```

```
DGS-3627:5#
```

config pim last_hop_spt_switchover

Purpose	Used to choose the switchover mode on the last hop router.
Syntax	config pim last_hop_spt_switchover [never immediately]
Description	This command will configure the need to change the last hop router's distribution tree to a SPT. The last hop router will always receive data from the shared tree unless this command is changed to immediately and then the router will always receive multicast data from the shortest path tree. This command is for PIM-SM configurations only.
Parameters	<i>never</i> – Using this command will configure the router to always receive multicast data from the shared tree. <i>immediately</i> – Using this command will configure the router to always receive multicast data from the shortest path tree.
Restrictions	Only administrator-level and operator-level users can issue this command.

Usage example:

To configure the last hop router to immediately switch to SPT:

```
DGS-3627:5#config pim last_hop_spt_switchover immediately
```

```
Command: config pim last_hop_spt_switchover immediately
```

```
Success.
```

```
DGS-3627:5#
```

show pim rpset

Purpose	Used to display the RP Set of the Switch.
Syntax	show pim rpset
Description	This command will display the information regarding the RP Set learned by the BSR. This command is for PIM-SM configurations only.
Parameters	None.
Restrictions	None.

Usage example:

To view the RP Set information:

```
DGS-3627:5# show pim rpset
Command: show pim rpset

PIM RP-Set Table

Bootstrap Router: 12.43.51.81

Group Address      RP Address      Holdtime      Expired Time      Type
-----
224.0.0.0/4       31.43.51.81    150           107               Dynamic

Total Entries: 1

DGS-3627:5#
```

show pim crp	
Purpose	Used to display the Candidate RP settings on the Switch, along with CRP parameters configured for the Switch.
Syntax	show pim crp
Description	This command will display the settings for Candidate RPs that are accessible to the switch. This command is for PIM-SM configurations only.
Parameters	None.
Restrictions	None.

Usage Example:

To view the CRP settings:

```
DGS-3627:5# show pim crp
Command: show pim crp

PIM Candidate-RP Table

C-RP Holdtime      : 150
C-RP Priority       : 2
C-RP Wildcard Prefix Count : 0

Group      Interface
-----
224.0.0.0/4      Zira

DGS-3627:5#
```

config pim cbsr	
Purpose	Used to configure the settings for the Candidate Bootstrap Router and the priority of the selected IP interface to become the Boot Strap Router (BSR) for the PIM-SM network domain.
Syntax	config pim cbsr [ipif <ipif_name 12> {priority [-1 value 0-255>}] hash_masklen <value 0-32> bootstrap_period <value 1-255>]
Description	This command will configure the settings for the Candidate BSR. The Boot Strap Router holds the information which determines which router on the network is to be elected as the RP for the multicast group and then to distribute RP information to other PIM-SM enabled routers. This command is for PIM-SM configurations only.

config pim cbsr

Parameters	<p><i>ipif <ipif_name 12></i> - Enter the ipif name of the interface to become the CBSR.</p> <p><i>priority [-1 value 0-255]</i> - Used to state the Priority of this IP Interface to become the BSR. The user may select a priority between -1 and 255. An entry of -1 states that the interface will be disabled to be the BSR.</p> <p><i>hash_masklen <value 0-32></i> Enter a hash mask length, which will be used with the IP address of the candidate RP and the multicast group address, to calculate the hash algorithm used by the router to determine which CRP on the PIM-SM enabled network will be the RP. The user may select a length between 0 and 32 with a default setting of 30. This parameter must be configured separately from the ipif settings of this command. See the examples below for a better understanding.</p> <p><i>bootstrap_period <value 1-255></i> - Enter a time period between 1 and 255 to determine the interval the Switch will send out Boot Strap Messages (BSM) to the PIM enabled network. The default setting is 60 seconds. This parameter must be configured separately from the ipif settings of this command. See the examples below for a better understanding.</p>
Restrictions	Only administrator-level and operator-level users can issue this command.

Usage example:

To configure the settings for an IP interface to become a CBSR:

```
DGS-3627:5#config pim cbsr ipif Zira priority 4
Command: config pim cbsr ipif Zira priority 4

Success.

DGS-3627:5#
```

Usage example:

To configure the hash mask length for the CBSR:

```
DGS-3627:5#config pim cbsr hash_masklen 30
Command: config pim cbsr hash_masklen 30

Success.

DGS-3627:5#
```

Usage example:

To configure the bootstrap period for the CBSR:

```
DGS-3627:5#config pim cbsr bootstrap_period 60
Command: config pim cbsr bootstrap_period 60

Success.

DGS-3627:5#
```

show pim cbsr

Purpose	Used to display the Candidate BSR settings of the switch, along with CCSR parameters configured for the Switch.
Syntax	show pim cbsr {ipif <ipif_name12>}
Description	This command will display the settings for Candidate BSRs that are accessible to the switch. This command is for PIM-SM configurations only.
Parameters	<ipif_name 12> - Enter the name of the IP interface for which to display settings. Entering no name will display all CCSRs.
Restrictions	None.

Usage example:

To view the CCSR settings:

```
DGS-3627:5# show pim cbsr
Command: show pim cbsr

PIM Candidate-BSR Table

C-BSR Hash Mask Len      : 30
C-BSR Bootstrap Period   : 2

Interface                IP Address                Priority
-----                -
Zira                     11.1.1.1/8                4
System                   10.53.13.30/8             -1 (Disabled)

DGS-3627:5#
```

show pim

Purpose	Used to display the PIM settings, along with PIM parameters configured for the Switch.
Syntax	show pim {ipif <ipif_name12>}
Description	This command will display the settings for the PIM function that are accessible to the switch.
Parameters	<ipif_name 12> - Enter the name of the IP address for which to display settings. Entering no name will display all PIM IP interfaces.
Restrictions	None.

Usage example:

To view the PIM settings:

```
DGS-3627:5# show pim
Command: show pim

PIM Global State           : Enabled
Last Hop SPT Switchover    : Immediately
Register Probe Time        : 5
Register Suppression Time  : 60

PIM Interface Table

Interface      IP Address      Designated   Hello   J/P
-----      -
Zira           11.1.1.1/8      10.53.13.30  30     60
System        10.53.13.30/8   11.1.1.1     60     60
Mode          State
DM            Disabled
SM            Enabled

Total Entries: 2

DGS-3627:5#
```

show pim neighbor

Purpose	Used to display PIM neighbors of the Switch.
Syntax	show pim neighbor {ipif <ipif_name12> ipaddress <network_address>}
Description	This command will display the PIM neighbor table for the Switch.
Parameters	<p><ipif_name 12> - Enter the name of the IP interface for which to display PIM information regarding PIM neighbors.</p> <p>ipaddress <network_address> - Enter the IP address of a PIM neighbor for which to display information.</p> <p>Adding no parameters to this command will display all PIM neighbors that probed the Switch.</p>
Restrictions	None.

Usage example:

To view the PIM neighbors:

```
DGS-3627:5# show pim neighbor
Command: show pim neighbor

PIM Neighbor Address Table

Interface Name      Neighbor Address  Expired Time
-----
n10                 10.20.6.251     79

Total Entries: 1

DGS-3627:5#
```

show pim ipmroute

Purpose	Used to display the PIM IP Multicast Route Table on the Switch.
Syntax	show pim ipmroute
Description	This command will display the PIM IP Multicast Route Table on the Switch. This command is for PIM-SM configurations only.
Parameters	None.
Restrictions	None.

Usage example:

To view the PIM routes:

```
DGS-3627:5# show pim ipmroute
Command: show pim ipmroute

PIM IP Multicast Route Table

UA = Upstream AssertTimer
AM = Assert Metric
AMPref = Assert MetricPref
ARB = Assert RPTBit
```

Group Address	Source Address	UA	AM	AMPref	ARB	Flag	Type
224.0.1.1	31.43.51.81/32	0	0	0	0	RPT	(*G)
224.0.1.24	10.54.81.250/32	0	0	0	0	SPT	(S,G)
224.0.1.24	10.55.68.64/32	0	0	0	0	SPT	(S,G)
224.0.1.24	31.43.51.81/32	0	0	0	0	RPT	(*G)
229.55.150.208	10.6.51.1/32	0	0	0	0	SPT	(S,G)
229.55.150.208	10.38.45.151/32	0	0	0	0	SPT	(S,G)
229.55.150.208	10.38.45.192/32	0	0	0	0	SPT	(S,G)
229.55.150.208	10.50.93.100/32	0	0	0	0	SPT	(S,G)
229.55.150.208	10.51.16.1/32	0	0	0	0	SPT	(S,G)
229.55.150.208	10.59.23.10/32	0	0	0	0	SPT	(S,G)
229.55.150.208	31.43.51.81/32	0	0	0	0	RPT	(*G)
239.192.0.1	31.43.51.81/32	0	0	0	0	RPT	(*G)

```
Total Entries: 12

DGS-3627:5#
```

create pim register_checksum_include_data

Purpose	Used to set the RPs that the Switch will send Register packets to and create checksums to be included with the data in Registered packets.
Syntax	create pim register_checksum_include_data rp_address <ipaddr>
Description	This command will set the RPs that the Switch will send Register packets to and create checksums to be included with the data in Registered packets. This command is for PIM-SM configurations only.
Parameters	<i>rp_address <ipaddr></i> - Enter the IP address of the RP that will verify checksums included with Registered packets.
Restrictions	Only administrator-level and operator-level users can issue this command.

Usage example:

To create an RP to which the Switch will send Register packets to and create checksums to be included with the data in Registered packets:

```
DGS-3627:5# create pim register_checksum_include_data rp_address 11.1.1.1
Command: create pim register_checksum_include_data rp_address 11.1.1.1

Success.

DGS-3627:5#
```

delete pim register_checksum_include_data

Purpose	Used to disable the RPs that the Switch will send Register packets to and create checksums to be included with the data in Registered packets.
Syntax	delete pim register_checksum_include_data rp_address <ipaddr>
Description	This command will disable the RPs that the Switch will send Register packets to and create checksums to be included with the data in Registered packets. This command is for PIM-SM configurations only.
Parameters	<i>rp_address <ipaddr></i> - Enter the IP address of the RP that will discontinue sending Register packets to and create checksums to be included with the data in Registered packets.
Restrictions	Only administrator-level and operator-level users can issue this command.

Usage example:

To delete RPs that the Switch will send Register packets to and create checksums to be included with the data in Registered packets:

```
DGS-3627:5#delete pim register_checksum_include_data rp_address 11.1.1.1
Command: delete pim register_checksum_include_data rp_address 11.1.1.1

Success.

DGS-3627:5#
```

show pim register_checksum_include_data_rp_list

Purpose	Used to display RPs that the Switch will send Register packets to and create checksums to be included with the data in Registered packets.
Syntax	show pim register_checksum_include_data_rp_list
Description	This command will display RPs that the Switch will send Register packets to and create checksums to be included with the data in Registered packets. This command is for PIM-SM configurations only.
Parameters	None.
Restrictions	None

Usage example:

To show the RPs that the Switch will send Register packets to and create checksums to be included with the data in Registered packets:

```
DGS-3627:5#show pim register_checksum_include_data_rp_list
Command: show pim register_checksum_include_data_rp_list
PIM Register Checksum Include Data
RP Address
-----
11.1.1.1
Total Entries: 1
DGS-3627:5#
```

IP MULTICASTING COMMANDS

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

Command	Parameters
show ipmc cache	{group <group>} {ipaddress <network_address>}
show ipmc	{ipif <ipif_name 12> protocol [inactive dvmrp pim]}

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

show ipmc cache

Purpose	Used to display the current IP multicast forwarding cache.
Syntax	show ipmc cache {group <group>} {ipaddress <network_address>}
Description	This command will display the current IP multicast forwarding cache.
Parameters	<i>group <group></i> – The multicast group IP address. <i>ipaddress <network_address></i> – The IP address and netmask of the source. The address and mask information can be specified using the traditional format (for example, 10.1.2.3/255.0.0.0 or in CIDR format, 10.1.2.3/8).
Restrictions	None.

Usage example:

To display the current IP multicast forwarding cache:

```
DGS-3627:5#show ipmc cache
Command: show ipmc cache
```

Multicast Group	Source Address/Netmask	Upstream Neighbor	Expire Time	Routing Protocol
224.1.1.1	10.48.74.121/32	10.48.75.63	30	DVMRP
224.1.1.1	20.48.74.25 /32	20.48.75.25	20	DVMRP
224.1.2.3	10.48.75.3 /3	10.48.76.6	30	DVMRP

```
Total Entries: 3

DGS-3627:5#
```

show ipmc

Purpose	Used to display the IP multicast interface table.
Syntax	show ipmc {ipif <ipif_name 12> protocol [inactive dvmrp pim]}
Description	This command will display the current IP multicast interface table.
Parameters	<i><ipif_name 12></i> – The name of the IP interface for which to display the IP multicast interface table for. <i>protocol</i> – Allows the user to specify whether or not to use one of the available protocols to display the IP multicast interface table. For example, if DVMRP is specified, the table will display only those entries that are related to the DVMRP protocol.

show ipmc

- *inactive* – Specifying this parameter will display entries that are currently inactive.
- *dvmrp* – Specifying this parameter will display only those entries that are related to the DVMRP protocol.
- *pim* - Specifying this parameter will display only those entries that are related to the PIM protocol.

Restrictions None.

Usage example

To display the current IP multicast interface table by DVMRP entry:

```
DGS-3627:5#show ipmc protocol dvmrp
Command: show ipmc protocol dvmrp

Interface Name  IP Address  Multicast Routing
-----
Triton         11.1.1.1   DVMRP

Total Entries: 1

DGS-3627:5#
```

MD5 COMMANDS

The MD5 configuration commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameters
create md5 key	<key_id 1-255> <password 16>
config md5 key	<key_id 1-255> <password 16>
delete md5 key	<key_id 1-255>
show md5	{key <key_id 1-255>}

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

create md5 key

Purpose	Used to create a new entry in the MD5 key table.
Syntax	create md5 key <key_id 1-255> <password 16>
Description	This command is used to create an entry for the MD5 key table.
Parameters	<key_id 1-255> – The MD5 key ID. The user may enter a key ranging from 1 to 255. <password> – An MD5 password of up to 16 bytes.
Restrictions	Only administrator-level and operator-level users can issue this command.

Usage example

To create an entry in the MD5 key table:

```
DGS-3627:5# create md5 key 1 dlink
Command: create md5 key 1 dlink

Success.

DGS-3627:5#
```

config md5 key

Purpose	Used to enter configure the password for an MD5 key.
Syntax	config md5 key <key_id 1-255> <password 16>
Description	This command is used to configure an MD5 key and password.
Parameters	<key_id 1-255> – The previously defined MD5 key ID. <password 16> – The user may change the MD5 password for the md5 key. A new password of up to 16 characters can be created.
Restrictions	Only administrator-level and operator-level users can issue this command.

Usage example

To configure an MD5 Key password:

```
DGS-3627:5#config md5 key 1 taboo
Command: config md5 key 1 taboo

Success.

DGS-3627:5#
```

delete md5 key

Purpose	Used to delete an entry in the MD5 key table.
Syntax	delete md5 key <key_id 1-255>
Description	This command is used to delete a specific entry in the MD5 key table.
Parameters	<key_id 1-255> – The MD5 key ID to delete.
Restrictions	Only administrator-level and operator-level users can issue this command.

Usage example

The delete an entry in the MD5 key table:

```
DGS-3627:5# delete md5 key 1
Command: delete md5 key 1

Success.

DGS-3627:5#
```

show md5

Purpose	Used to display an MD5 key table.
Syntax	show md5 {key <key_id 1-255>}
Description	This command will display the current MD5 key table.
Parameters	<key_id 1-255> – The MD5 key ID to be displayed.
Restrictions	None.

Usage example

To display the current MD5 key:

```
DGS-3627:5#show md5
Command: show md5

MD5 Key Table Configurations

Key-ID   Key
-----  -
1        dlink
2        develop
3        fireball
4        intelligent

Total Entries: 4

DGS-3627:5#
```

OSPF CONFIGURATION COMMANDS

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

Command	Parameters
config ospf router_id	<ipaddr>
enable ospf	
disable ospf	
show ospf	{ipif <ipif_name 12> all}
create ospf area	<area_id> type [normal [stub nssa {translate [enable disable]}] {stub_summary [enable disable] metric <value 0-65535>}]
delete ospf area	<area_id>
config ospf area	<area_id> type [normal [stub nssa {translate [enable disable]}] {stub_summary [enable disable] metric <value 0-65535>}]
show ospf area	{<area_id>}
create ospf host_route	<ipaddr> {area <area_id> metric <value 1-65535>}
delete ospf host_route	<ipaddr>
config ospf host_route	<ipaddr> {area <area_id> metric <value 1-65535>}
show ospf host_route	<ipaddr>
create ospf aggregation	<area_id> <network_address> lsdb_type [summary {advertise [enable disable]} nssa_ext {advertise [enable disable]}]
delete ospf aggregation	<area_id> <network_address> lsdb_type [summary nssa_ext]
config ospf aggregation	<area_id> <network_address> lsdb_type [summary {advertise [enable disable]} nssa_ext {advertise [enable disable]}]
show ospf aggregation	{<area_id>}
show ospf lsdb	{area <area_id> advertise_router <ipaddr> type [rtrlink netlink summary assummary asexmlink nssa_ext]}
show ospf neighbor	{<ipaddr>}
show ospf virtual_neighbor	{<area_id> <neighbor_id>}
config ospf ipif	[ipif <ipif_name 12> all] {area <area_id> priority <value> hello_interval <sec 1-65535> dead_interval <sec 1-65535> authentication [none simple <password 8> md5 <key_id 1-255>] metric <value 1-65535> state [enable disable] passive [enable disable]}
create ospf virtual_link	<area_id> <neighbor_id> {hello_interval <sec 1-65535> dead_interval <sec 1-65535> authentication [none simple <password 8> md5 <key_id 1-255>]}
config ospf virtual_link	<area_id> <neighbor_id> {hello_interval <sec 1-65535> dead_interval <sec 1-65535> authentication [none simple <password 8> md5 <key_id 1-255>]}
delete ospf virtual_link	<area_id> <neighbor_id>
show ospf virtual_link	{<area_id> <neighbor_id>}

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

config ospf router_id

Purpose	Used to configure the OSPF router ID.
Syntax	config ospf router_id <ipaddr>
Description	This command is used to configure the OSPF router ID.
Parameters	<ipaddr> – The IP address of the OSPF router.
Restrictions	Only administrator-level and operator-level users can issue this command.

Usage example

To configure the OSPF router ID:

```
DGS-3627:5#config ospf router_id 10.48.74.122
Command: config ospf router_id 10.48.74.122

Success.

DGS-3627:5#
```

enable ospf

Purpose	Used to enable OSPF on the Switch.
Syntax	enable ospf
Description	This command, in combination with the disable ospf command below, is used to enable and disable OSPF on the Switch.
Parameters	None.
Restrictions	Only administrator-level and operator-level users can issue this command.

Usage example

To enable OSPF on the Switch:

```
DGS-3627:5#enable ospf
Command: enable ospf

Success.

DGS-3627:5#
```

disable ospf

Purpose	Used to disable OSPF on the Switch.
Syntax	disable ospf
Description	This command, in combination with the enable ospf command above, is used to enable and disable OSPF on the Switch.
Parameters	None.
Restrictions	Only administrator-level and operator-level users can issue this command.

Usage example

To disable OSPF on the Switch:


```
DGS-3627:5#disable ospf
Command: disable ospf

Success.

DGS-3627:5#
```

show ospf

Purpose	Used to display the current OSPF state on the Switch.
Syntax	show ospf
Description	This command will display the current state of OSPF on the Switch, divided into the following categories: General OSPF settings OSPF Interface settings OSPF Area settings OSPF Virtual Interface settings OSPF Area Aggregation settings OSPF Host Route settings
Parameters	None.
Restrictions	None.

Usage example:

To show OSPF state:

```
DGS-3627:5#show ospf
Command: show ospf

OSPF Router ID   : 10.1.1.2
State            : Enabled

OSPF Interface Settings

Interface  IP Address   Area ID  State   Link Status   Metric
-----  -
System    10.90.90.90/8  0.0.0.0  Disabled Link DOWN     1
ip2       20.1.1.1/8    0.0.0.0  Disabled Link DOWN     1
ip3       30.1.1.1/8    0.0.0.0  Disabled Link DOWN     1

Total Entries : 3

OSPF Area Settings

Area ID   Type   Stub Import Summary LSA  Stub Default Cost  Translate
-----  -
0.0.0.0   Normal None                       None                None
10.0.0.0  Normal None                       None                None
244.0.0.6 NSSA  Enabled                    2                   Enabled

Total Entries : 3

Virtual Interface Configuration

Transit  Virtual      Hello  Dead  Authentication  Link
Area ID  Neighbor Router Interval Interval          Status
-----  -

```

10.0.0.0	20.0.0.0	10	60	None	DOWN
10.1.1.1	20.1.1.1	10	60	None	DOWN
Total Entries : 2					
OSPF Area Aggregation Settings					
Area ID	Aggregated Network Address	LSDB Type	Advertise		
-----	-----	-----	-----		
244.0.0.6	11.0.0.0/8	NSSA-EXT	Disabled		
Total Entries : 1					
OSPF Host Route Settings					
Host Address	Metric	Area ID			
-----	-----	-----			
10.3.3.3	1	10.1.1.1			
Total Entries : 1					
DGS-3627:5#					

create ospf area

Purpose	Used to create an OSPF area.
Syntax	create ospf area <area_id> type [normal stub nssa {translate [enable disable]}] {stub_summary [enable disable] metric <value 0-65535>}
Description	This command is used to create an OSPF area and configure its settings.
Parameters	<p><area_id> – The OSPF area ID. The user may enter a 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.</p> <p>type – The OSPF area mode of operation – the user has three choices to choose from to define the area created here.</p> <ul style="list-style-type: none"> • <i>normal</i> – Choosing this parameter will define the OSPF area created here as a normal area. • <i>stub</i> – Choosing this parameter will define the OSPF area created here as a stub area. • <i>nssa</i> – Choosing this parameter will define the OSPF area created here as an NSSA (Not So Stubby Area) area. <ul style="list-style-type: none"> • <i>translate [enable disable]</i> – Enable this parameter to translate Type-7 LSAs into Type-5 LSAs, so that they can be distributed outside of the NSSA. The default is Disabled. This field can only be configured if <i>nssa</i> is chosen in the <i>type</i> field. <p>stub_summary [enable disable] – Enables or disables the OSPF area to import summary LSA advertisements.</p> <p>metric <value 0-65535> – The OSPF area cost between 0 and 65535. 0 denotes that the value will be automatically assigned. The default setting is 0. For NSSA areas, the metric field determines the cost of traffic entering the NSSA area.</p>
Restrictions	Only administrator-level and operator-level users can issue this command.

Usage example:

To create an OSPF area:

```
DGS-3627:5#create ospf area 10.48.74.122 type normal
Command: create ospf area 10.48.74.122 type normal

Success.

DGS-3627:5#
```

To create an OSPF NSSA area:

```
DGS-3627:5#create ospf area 11.1.1.1 type nssa translate enable metric 5 stub_summary enable
Command: create ospf area 11.1.1.1 type nssa translate enable metric 5 stub_summary enable

Success.

DGS-3627:5#
```

delete ospf area

Purpose	Used to delete an OSPF area.
Syntax	delete ospf area <area_id>
Description	This command is used to delete an OSPF area.
Parameters	<area_id> – A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.
Restrictions	Only administrator-level and operator-level users can issue this command.

Usage example:

To delete an OSPF area:

```
DGS-3627:5#delete ospf area 10.48.74.122
Command: delete ospf area 10.48.74.122

Success.

DGS-3627:5#
```

config ospf area

Purpose	Used to configure an OSPF area's settings.
Syntax	config ospf area <area_id> type [normal stub nssa {translate [enable disable]}] {stub_summary [enable disable] metric <value 0-65535>}
Description	This command is used to configure an OSPF area's settings.
Parameters	<p><area_id> – The OSPF area ID. The user may enter a 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.</p> <p>type – The OSPF area mode of operation – the user has three choices to choose from to define the area configured here.</p> <ul style="list-style-type: none"> • <i>normal</i> – Choosing this parameter will define the OSPF area

config ospf area

configured here as a normal area.

- *stub* – Choosing this parameter will define the OSPF area configured here as a stub area.
- *nssa* – Choosing this parameter will define the OSPF area configured here as an NSSA (Not So Stubby Area) area.
 - *translate [enable | disable]* – Enable this parameter to translate Type-7 LSAs into Type-5 LSAs, so that they can be distributed outside of the NSSA. The default is Disabled. This field can only be configured if *nssa* is chosen in the type field.

stub_summary [enable | disable] – Allows the OSPF area import of LSA advertisements to be enabled or disabled.

metric <value 0-65535> – The OSPF area stub default cost.

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

Usage example

To configure an OSPF area's settings:

```
DGS-3627:5#config ospf area 10.48.74.122 type stub stub_summary enable metric 1
Command: config ospf area 10.48.74.122 type stub stub_summary enable metric 1

Success.

DGS-3627:5#
```

show ospf area

Purpose	Used to display an OSPF area's configuration.
Syntax	show ospf area {<area_id>}
Description	This command will display the current OSPF area configuration.
Parameters	<area_id> – A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.
Restrictions	None.

Usage example

To display an OSPF area's settings:

```
DGS-3627:5#show ospf area
Command: show ospf area
```

Area ID	Type	Stub	Import Summary LSA	Stub Default Cost	Translate
0.0.0.0	Normal	None		None	None
10.48.74.122	Stub	Enabled		Enabled	None
244.0.0.6	NSSA	Enabled		5	Enabled

```
Total Entries: 3

DGS-3627:5#
```

create ospf host_route

Purpose	Used to configure OSPF host route settings.
Syntax	create ospf host_route <ipaddr> {area <area_id> metric <value 1-65535>}
Description	This command is used to configure the OSPF host route settings.
Parameters	<p><ipaddr> – The host's IP address.</p> <p><area_id> – A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.</p> <p>metric <value 1-65535> – A metric between 1 and 65535, which will be advertised.</p>
Restrictions	Only administrator-level and operator-level users can issue this command.

Usage example

To configure the OSPF host route settings:

```
DGS-3627:5#create ospf host_route 10.48.74.122 area 10.1.1.1 metric 2
Command: create ospf host_route 10.48.74.122 area 10.1.1.1 metric 2

Success.

DGS-3627:5#
```

delete ospf host_route

Purpose	Used to delete an OSPF host route.
Syntax	delete ospf host_route <ipaddr>
Description	This command is used to delete an OSPF host route.
Parameters	<ipaddr> – The IP address of the OSPF host.
Restrictions	Only administrator-level and operator-level users can issue this command.

Usage example

To delete an OSPF host route:

```
DGS-3627:5#delete ospf host_route 10.48.74.122
Command: delete ospf host_route 10.48.74.122

Success.

DGS-3627:5#
```

config ospf host_route

Purpose	Used to configure OSPF host route settings.
Syntax	config ospf host_route <ipaddr> {area <area_id> metric <value>}
Description	This command is used to configure an OSPF host route settings.
Parameters	<p><ipaddr> – The IP address of the host.</p> <p><area_id> – A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.</p> <p><value> – A metric between 1 and 65535 that will be advertised for the route.</p>

config ospf host_route

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

Usage example

To configure an OSPF host route:

```
DGS-3627:5#config ospf host_route 10.48.74.122 area 10.1.1.1 metric 2
Command: config ospf host_route 10.48.74.122 area 10.1.1.1 metric 2

Success.

DGS-3627:5#
```

show ospf host_route

Purpose	Used to display the current OSPF host route table.
Syntax	show ospf host_route {<ipaddr>}
Description	This command will display the current OSPF host route table.
Parameters	<ipaddr> – The IP address of the host.
Restrictions	None.

Usage example:

To display the current OSPF host route table:

```
DGS-3627:5#show ospf host_route
Command: show ospf host_route

Host Address   Metric   Area_ID
-----
10.48.73.21    2        10.1.1.1
10.48.74.122  1        10.1.1.1

Total Entries: 2

DGS-3627:5#
```

create ospf aggregation

Purpose	Used to configure OSPF area aggregation settings.
Syntax	create ospf aggregation <area_id> <network_address> lsdb_type [summary {advertise [enable disable]} nssa_ext {advertise [enable disable]}]
Description	This command is used to create an OSPF area aggregation.
Parameters	<p><area_id> – A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.</p> <p><network_address> – The 32-bit number in the form of an IP address that uniquely identifies the network that corresponds to the OSPF Area.</p> <p>lsdb_type – The type of address aggregation. The user has two choices for the LSDB type:</p> <ul style="list-style-type: none"> • <i>summary</i> – Choosing this LSDB type will summarize routes that

create ospf aggregation

are entering the OSPF area by redistribution.

- *advertise [enable | disable]* – Allows for the advertisement trigger to be enabled or disabled.
- *nssa_ext* – Choosing this LSDB type will summarize routes that are entering the OSPF NSSA from an external source.
 - *advertise [enable | disable]* – Allows for the advertisement trigger to be enabled or disabled.

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

Usage example:

To create an OSPF area aggregation:

```
DGS-3627:5#create ospf aggregation 10.1.1.1 10.48.76.122/16
lsdb_type summary advertise enable
Command: create ospf aggregation 10.1.1.1 10.48.76.122/16
lsdb_type summary advertise enable

Success.

DGS-3627:5#
```

delete ospf aggregation

Purpose	Used to delete an OSPF area aggregation configuration.
Syntax	delete ospf aggregation <area_id> <network_address> lsdb_type [summary nssa_ext]
Description	This command is used to delete an OSPF area aggregation configuration.
Parameters	<p><i><area_id></i> – A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.</p> <p><i><network_address></i> – The 32-bit number in the form of an IP address that uniquely identifies the network that corresponds to the OSPF Area.</p> <p><i>lsdb_type summary</i> – Specifies the type of address aggregation to be deleted. Choose either <i>summary</i> or <i>nssa_ext</i>.</p>
Restrictions	Only administrator-level and operator-level users can issue this command.

Usage example

To configure the OSPF area aggregation settings:

```
DGS-3627:5#delete ospf aggregation 10.1.1.1 10.48.76.122/16 lsdb_type summary
Command: delete ospf aggregation 10.1.1.1 10.48.76..122/16 lsdb_type summary

Success.

DGS-3627:5#
```

config ospf aggregation

Purpose	Used to configure the OSPF area aggregation settings.
Syntax	config ospf aggregation <area_id> <network_address> lsdb_type [summary {advertise [enable disable]} nssa_ext {advertise [enable disable]}]

config ospf aggregation

Description	This command is used to configure the OSPF area aggregation settings.
Parameters	<p><area_id> – A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.</p> <p><network_address> – The 32-bit number in the form of an IP address that uniquely identifies the network that corresponds to the OSPF Area.</p> <p>lsdb_type – The type of address aggregation. The user has two choices for the LSDB type:</p> <ul style="list-style-type: none"> summary – Choosing this LSDB type will summarize routes that are entering the OSPF area by redistribution. <ul style="list-style-type: none"> advertise [enable disable] – Allows for the advertisement trigger to be enabled or disabled. nssa_ext – Choosing this LSDB type will summarize routes that are entering the OSPF NSSA from an external source. <ul style="list-style-type: none"> advertise [enable disable] – Allows for the advertisement trigger to be enabled or disabled.
Restrictions	Only administrator-level and operator-level users can issue this command.

Usage example

To configure the OSPF area aggregation settings:

```
DGS-3627:5#config ospf aggregation 10.1.1.1 10.48.76.122/16 lsdb_type
summary advertise enable
Command: config ospf aggregation 10.1.1.1 10.48.76.122/16 lsdb_type
summary advertise enable

Success.

DGS-3627:5#
```

show ospf aggregation

Purpose	Used to display the current OSPF area aggregation settings.
Syntax	show ospf aggregation {<area_id>}
Description	This command will display the current OSPF area aggregation settings.
Parameters	<area_id> – Enter this parameter to view this table by a specific OSPF area ID.
Restrictions	None.

Usage example:

To display OSPF area aggregation settings:

```
DGS-3627:5#show ospf aggregation
Command: show ospf aggregation

OSPF Area Aggregation Settings

Area ID      Aggregated      LSDB           Advertise
-----      -
10.1.1.1     10.0.0.0/8      Summary        Enabled
244.0.0.6    11.0.0.0/8      NSSA-Ext       Enabled
```


Total Entries: 2

DGS-3627:5#

show ospf lsdb

Purpose	Used to display the OSPF Link State Database (LSDB).
Syntax	show ospf lsdb {area_id <area_id> advertise_router <ipaddr> type [rtrlink netlink summary assummary asexmlink nssa_ext]}
Description	This command will display the current OSPF Link State Database (LSDB).
Parameters	<i>area_id <area_id></i> – A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain. <i>advertise_router <ipaddr></i> – The router ID of the advertising router. <i>type [rtrlink netlink summary assummary asexmlink nssa_ext]</i> – The type of link.
Restrictions	None.



NOTE: When this command displays a "*" (a star symbol) in the OSPF LSDB table for the *area_id* or the *Cost*, this is interpreted as "no area ID" for external LSAs, and as "no cost given" for the advertised link.

Usage example:

To display the link state database of OSPF:

```
DGS-3627:5#show ospf lsdb
Command: show ospf lsdb
```

Area ID	LSDB Type	Advertising Router ID	Link State ID	Cost	Sequence Number
0.0.0.0	RTRLink	50.48.75.73	50.48.75.73	*	0x80000002
0.0.0.0	Summary	50.48.75.73	10.0.0.0/8	1	0x80000001
1.0.0.0	RTRLink	50.48.75.73	50.48.75.73	*	0x80000001
1.0.0.0	Summary	50.48.75.73	40.0.0.0/8	1	0x80000001
1.0.0.0	Summary	50.48.75.73	50.0.0.0/8	1	0x80000001
*	ASExtLink	50.48.75.73	1.2.0.0/16	20	0x80000001

```
Total Entries: 5
DGS-3627:5#
```

show ospf neighbor

Purpose	Used to display the current OSPF neighbor router table.
Syntax	show ospf neighbor {<ipaddr>}
Description	This command will display the current OSPF neighbor router table.
Parameters	<i><ipaddr></i> – The IP address of the neighbor router.
Restrictions	None.

Usage example

To display the current OSPF neighbor router table:

```
DGS-3627:5#show ospf neighbor
Command: show ospf neighbor

IP Address of Neighbor   Router ID of Neighbor   Neighbor Priority   Neighbor State
-----
10.48.74.122             10.2.2.2                1                   Initial

Total Entries: 1

DGS-3627:5#
```

show ospf virtual_neighbor

Purpose	Used to display the current OSPF virtual neighbor router table.
Syntax	show ospf virtual_neighbor {<area_id> <neighbor id>}
Description	This command will display the current OSPF virtual neighbor router table.
Parameters	<p><area_id> – A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.</p> <p><neighbor_id> – The OSPF router ID for the neighbor. This is a 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the remote area's Area Border Router.</p>
Restrictions	None.

Usage example

To display the current OSPF virtual neighbor table:

```
DGS-3627:5#show ospf virtual_neighbor
Command: show ospf virtual_neighbor

Transit Area ID   Router ID of Virtual Neighbor   IP Address of Virtual Neighbor   Virtual Neighbor State
-----
10.1.1.1         10.2.3.4                        10.48.74.111                     Exchange

Total Entries : 1

DGS-3627:5#
```

config ospf ipif

Purpose	Used to configure the OSPF interface settings.
Syntax	config ospf [ipif <ipif_name 12> all] {area <area_id> priority <value> hello_interval <sec 1-65535> dead_interval <sec 1-65535> authentication [none simple <password 8> md5 <key_id 1-255>] metric <value 1-65535> state [enable disable] passive [enable disable]}
Description	This command is used to configure the OSPF interface settings.
Parameters	<p><ipif_name 12> – The name of the IP interface.</p> <p>all - All IP interfaces.</p> <p>area <area_id> - A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.</p> <p>priority <value> – The priority used in the election of the Designated Router (DR).</p>

config ospf ipif

A number between 0 and 255.

hello_interval <sec 1-65535> – Allows the specification of the interval between the transmission of OSPF Hello packets, in seconds. Between 1 and 65535 seconds can be specified. The Hello Interval, Dead Interval, Authorization Type, and Authorization Key should be the same for all routers on the same network.

dead_interval <sec 1-65535> – Allows the specification of the length of time between the receipt of Hello packets from a neighbor router before the selected area declares that router down. An interval between 1 and 65535 seconds can be specified. The Dead Interval must be evenly divisible by the Hello Interval.

metric <value 1-65535 > – The interface metric (1 to 65535). Entering a 0 will allow automatic calculation of the metric.

authentication – Enter the type of authentication preferred. The user may choose between:

- *none* – Choosing this parameter will require no authentication.
- *simple* <password 8> – Choosing this parameter will set a simple authentication which includes a case-sensitive password of no more than 8 characters.
- *md5* <key_id 1-255> – Choosing this parameter will set authentication based on md5 encryption. A previously configured MD5 key ID (1 to 255) is required.

metric <value 1-65535> – This field allows the entry of a number between 1 and 65,535 that is representative of the OSPF cost of reaching the selected OSPF interface. The default metric is 1.

state [enable | disable] – Used to enable or disable this function.

passive [enable | disable] – The user may select Active or Passive for this OSPF interface. Active interfaces actively advertise OSPF to routers on other Intranets that are not part of this specific OSPF group. Passive interface will not advertise to any other routers than those within its OSPF intranet. When this field is disabled, it denotes an active interface. The default setting is *disable*. (active)

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

Usage example

To configure OSPF interface settings:

```
DGS-3627:5#config ospf ipif System priority 2 hello_interval 15 metric 2 state enable
Command: config ospf ipif System priority 2 hello_interval 15 metric 2 state enable
```

```
Success.
```

```
DGS-3627:5#
```

show ospf ipif

Purpose	Used to display the current OSPF interface settings for the specified interface name.
Syntax	show ospf ipif {<ipif_name 12> all}
Description	This command will display the current OSPF interface settings for the specified interface name.
Parameters	<ipif_name 12> – The IP interface name for which to display the current OSPF interface settings. all – Choosing this parameter will display the OSPF settings for all IP interfaces on the Switch.
Restrictions	None.

Usage example:

To display the current OSPF interface settings, for a specific OSPF interface:

```
DGS-3627:5#show ospf ipif ipif2
Command: show ospf ipif ipif2

Interface Name: ipif2                IP Address: 123.234.12.34/24 ((Link Up))
Network Medium Type: BROADCAST      Metric: 1
Area ID: 1.0.0.0                    Administrative State: Enabled
Priority: 1                           DR State: DR
DR Address: 123.234.12.34           Backup DR Address: None
Hello Interval: 10                   Dead Interval: 40
Transmit Delay: 1                    Retransmit Time: 5
Authentication: None
Passive Mode : Disabled

Total Entries: 1

DGS-3627:5#
```

show ospf all	
Purpose	Used to display the current OSPF settings of all the OSPF interfaces on the Switch.
Syntax	show ospf all
Description	This command will display the current OSPF settings for all OSPF interfaces on the Switch.
Parameters	None.
Restrictions	None.

Usage example:

To display the current OSPF interface settings, for all OSPF interfaces on the Switch:

```
DGS-3627:5#show ospf all
Command: show ospf all

Interface Name: System                IP Address: 10.42.73.10/8 (Link Up)
Network Medium Type: BROADCAST      Metric: 1
Area ID: 0.0.0.0                    Administrative State: Enabled
Priority: 1                           DR State: DR
DR Address: 10.42.73.10             Backup DR Address: None
Hello Interval: 10                   Dead Interval: 40
Transmit Delay: 1                    Retransmit Time: 5
Authentication: None

Interface Name: ipif2                IP Address: 123.234.12.34/24 ((Link Up))
Network Medium Type: BROADCAST      Metric: 1
Area ID: 1.0.0.0                    Administrative State: Enabled
Priority: 1                           DR State: DR
DR Address: 123.234.12.34           Backup DR Address: None
Hello Interval: 10                   Dead Interval: 40
Transmit Delay: 1                    Retransmit Time: 5
Authentication: None

Total Entries: 2

DGS-3627:5#
```

create ospf virtual_link

Purpose	Used to create an OSPF virtual interface.
Syntax	create ospf virtual_link <area_id> <neighbor_id> {hello_interval <sec 1-65535> dead_interval <sec 1-65535> authentication [none simple <password 8> md5 <key_id 1-255>]}
Description	This command is used to create an OSPF virtual interface.
Parameters	<p><i><area_id></i> – A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.</p> <p><i><neighbor_id></i> – The OSPF router ID for the remote area. This is a 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the remote area's Area Border Router. The router ID of the neighbor router.</p> <p><i>hello_interval <sec 1-65535></i> – Allows the specification of the interval between the transmission of OSPF Hello packets, in seconds. Between 1 and 65535 seconds can be specified. The Hello Interval, Dead Interval, Authorization Type, and Authorization Key should be the same for all routers on the same network.</p> <p><i>dead_interval <sec 1-65535></i> – Allows the specification of the length of time between the receipt of Hello packets from a neighbor router before the selected area declares that router down. An interval between 1 and 65535 seconds can be specified. The Dead Interval must be evenly divisible by the Hello Interval.</p> <p><i>authentication</i> – Enter the type of authentication preferred. The user may choose between:</p> <ul style="list-style-type: none"> • <i>none</i> – Choosing this parameter will require no authentication. • <i>simple <password 8></i> – Choosing this parameter will set a simple authentication which includes a case-sensitive password of no more than 8 characters. • <i>md5 <key_id 1-255></i> – Choosing this parameter will set authentication based on md5 encryption. A previously configured MD5 key ID (1 to 255) is required.
Restrictions	Only administrator-level and operator-level users can issue this command.

Usage example

To create an OSPF virtual interface:

```
DGS-3627:5#create ospf virtual_link 10.1.12 20.1.1.1 hello_interval 10
Command: create ospf virtual_link 10.1.12 20.1.1.1 hello_interval 10

Success.

DGS-3627:5#
```

config ospf virtual_link

Purpose	Used to configure the OSPF virtual interface settings.
Syntax	config ospf virtual_link <area_id> <neighbor_id> {hello_interval <sec 1-65535> dead_interval <sec 1-65535> authentication [none simple <password 8> md5 <key_id 1-255>]}
Description	This command is used to configure the OSPF virtual interface settings.
Parameters	<i><area_id></i> – A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx)

config ospf virtual_link

that uniquely identifies the OSPF area in the OSPF domain.

<neighbor_id> – The OSPF router ID for the remote area. This is a 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the remote area's Area Border Router.

hello_interval <sec 1-65535> – Allows the specification of the interval between the transmission of OSPF Hello packets, in seconds. Between 1 and 65535 seconds can be specified. The Hello Interval, Dead Interval, Authorization Type, and Authorization Key should be the same for all routers on the same network.

dead_interval <sec 1-65535> – Allows the specification of the length of time between the receipt of Hello packets from a neighbor router before the selected area declares that router down. An interval between 1 and 65535 seconds can be specified. The Dead Interval must be evenly divisible by the Hello Interval.

authentication – Enter the type of authentication preferred. The user may choose between:

- *none* – Choosing this parameter will require no authentication.
- *simple <password 8>* – Choosing this parameter will set a simple authentication which includes a case-sensitive password of no more than 8 characters.
- *md5 <key_id 1-255>* – Choosing this parameter will set authentication based on md5 encryption. A previously configured MD5 key ID (1 to 255) is required.

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

Usage example

To configure the OSPF virtual interface settings:

```
DGS-3627:5#config ospf virtual_link 10.1.1.2 20.1.1.1 hello_interval 10
Command: config ospf virtual_link 10.1.1.2 20.1.1.1 hello_interval 10

Success.

DGS-3627:5#
```

delete ospf virtual_link

Purpose	Used to delete an OSPF virtual interface.
Syntax	delete ospf virtual_link <area_id> <neighbor_id>
Description	This command will delete an OSPF virtual interface from the Switch.
Parameters	<p><i><area_id></i> – A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.</p> <p><i><neighbor_id></i> – The OSPF router ID for the remote area. This is a 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the remote area's Area Border Router. The router ID of the neighbor router.</p>
Restrictions	Only administrator-level and operator-level users can issue this command.

Usage example:

To delete an OSPF virtual interface from the Switch:

```
DGS-3627:5#delete ospf virtual_link 10.1.12 20.1.1.1
```

Command: delete ospf virtual_link 10.1.12 20.1.1.1

Success.

DGS-3627:5#

show ospf virtual_link

Purpose	Used to display the current OSPF virtual interface configuration.
Syntax	show ospf virtual_link {<area_id> <neighbor_id>}
Description	This command will display the current OSPF virtual interface configuration.
Parameters	<p><area_id> – A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.</p> <p><neighbor_id> – The OSPF router ID for the remote area. This is a 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the remote area's Area Border Router. This is the router ID of the neighbor router.</p>
Restrictions	None.

Usage example:

To display the current OSPF virtual interface configuration:

```

DGS-3627:5#show ospf virtual_link
Command: show ospf virtual_link

Virtual Interface Configuration

Transit   Virtual   Hello   Dead   Authentication   Link
Area ID   Neighbor Router Interval Interval ----- Status
-----
10.0.0.0  20.0.0.0    10      60     None             DOWN

Total Entries: 1
DGS-3627:5#
    
```

ROUTE PREFERENCE COMMANDS

Route Preference is a way for routers to select the best path when there are two or more different routes to the same destination from two different routing protocols. The majority of routing protocols are not compatible when used in conjunction with each other. This Switch supports and may be configured for many routing protocols, as a stand alone switch or more importantly, in utilizing the stacking function and Single IP Management of the Switch. Therefore the ability to exchange route information and select the best path is essential to optimal use of the Switch and its capabilities.

The first decision the Switch will make in selecting the best path is to consult the Route Preference Settings table of the Switch. This table can be viewed using the **show route preference** command, and it holds the list of possible routing protocols currently implemented in the Switch, along with a reliability value which determines which routing protocol will be the most dependable to route packets. Below is a list of the default route preferences set on the Switch.

Route Type	Validity Range	Default Value
Local	0 – Permanently set on the Switch and not configurable.	0
Static	1 – 999	60
OSPF Intra	1 – 999	80
OSPF Inter	1 – 999	90
RIP	1 – 999	100
OSPF ExtT1	1 – 999	110
OSPF ExtT2	1 – 999	115

As shown above, Local will always be the first choice for routing purposes and the next most reliable path is Static due to the fact that its has the next lowest value. To set a higher reliability for a route, change its value to a number less than the value of a route preference that has a greater reliability value using the **config route preference** command. For example, if the user wishes to make RIP the most reliable route, the user can change its value to one that is less than the lowest value (Static - 60) or the user could change the other route values to more than 100.

The user should be aware of three points before configuring the route preference.

1. No two route preference values can be the same. Entering the same route preference may cause the Switch to crash due to indecision by the Switch.
2. If the user is not fully aware of all the features and functions of the routing protocols on the Switch, a change in the default route preference value may cause routing loops or black holes.
3. After changing the route preference value for a specific routing protocol, that protocol needs to be restarted because the previously learned routes have been dropped from the Switch. The Switch must learn the routes again before the new settings can take affect.

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

Command	Parameters
config route preference	[static rip ospfIntra ospfInter ospfExt1 ospfExt2] <value 1-999>
show route preference	{[local static rip ospfIntra ospfInter ospfExt1 ospfExt2]}

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

config route preference

Purpose	Used to configure the route preference of each route type.
Syntax	config route preference [static rip ospfIntra ospfInter ospfExt1 ospfExt2] <value 1-999>
Description	This command is used to set the route preference value for each routing protocol listed. A lower value will denote a better chance that the specified protocol is the best path for routing packets.
Parameters	<p>The user may set a preference value for a specific route by first choosing one of the following and then adding an alternate preference value:</p> <ul style="list-style-type: none"> • <i>static</i> – Choose this parameter to configure the preference value for the <i>static</i> route. • <i>rip</i> - Choose this parameter to configure the preference value for the <i>RIP</i> route. • <i>ospfIntra</i> - Choose this parameter to configure the preference value for the <i>OSPF Intra-area</i> route. • <i>ospfInter</i> - Choose this parameter to configure the preference value for the <i>OSPF Inter-area</i> route. • <i>ospfExtT1</i> - Choose this parameter to configure the preference value for the <i>OSPF AS External route type-1</i> route. • <i>ospfExtT2</i> - Choose this parameter to configure the preference value for the <i>AS External route type-2</i> route. <p><value 1-999> - Enter a value between 1 and 999 to set the route preference for a particular route. The lower the value, the higher the chance the specified protocol will be chosen as the best path for routing packets.</p>
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To configure the route preference value for RIP as 50:

```
DGS-3627:5#config route preference rip 50
Command: config route preference rip 50

Success.

DGS-3627:5#
```

show route preference

Purpose	Used to display the route preference of each route type.
Syntax	show route preference {[local static rip ospfIntra ospfInter ospfExt1 ospfExt2]}
Description	This command will display the Route Preference Settings table. The user may view all route preference settings by entering the command without any parameters or choose a specific type by adding the route parameter to the command.
Parameters	<p><i>local</i> – Enter this parameter to view the route preference settings for the <i>local</i> route.</p> <p><i>static</i> - Enter this parameter to view the route preference settings for the <i>static</i> route.</p>

show route preference

rip - Enter this parameter to view the route preference settings for the *RIP* route.

ospfIntra - Enter this parameter to view the route preference settings for the *Ospf Intra-area* route.

ospfInter - Enter this parameter to view the route preference settings for the *OSPF Inter-area* route.

ospfExtT1 - Enter this parameter to view the route preference settings for the *OSPF AS External route type-1*.

ospfExtT2 - Enter this parameter to view the route preference settings for the *OSPF AS External route type-2*.

Entering this command with no parameters will display the route preference for all routes.

Restrictions None.

Example usage:

To view the route preference values for all routes:

```
DGS-3627:5#show route preference
```

```
Command: show route preference
```

```
Route Preference Settings
```

```
Route Type    Preference
```

```
-----
```

RIP	100
OSPF Intra	80
STATIC	60
LOCAL	0
OSPF Inter	90
OSPF ExtT1	110
OSPF ExtT2	115

```
DGS-3627:5#
```

Example usage:

To view the route preference values for the RIP route:

```
DGS-3627:5#show route preference rip
```

```
Command: show route preference rip
```

```
Route Preference Settings
```

```
Route Type    Preference
```

```
-----
```

RIP	100
-----	-----

```
DGS-3627:5#
```

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>}
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-level and operator-level users can issue this command.

Example usage:

To enable MAC notification without changing basic configuration:

```
DGS-3627:5#enable mac_notification
Command: enable mac_notification

Success.

DGS-3627:5#
```

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-level and operator-level users can issue this command.

Example usage:

To disable MAC notification without changing basic configuration:

```
DGS-3627:5#disable mac_notification
Command: disable mac_notification

Success.

DGS-3627:5#
```

config mac_notification

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

Example usage:

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

```
DGS-3627:5#config mac_notification interval 1 historysize 500
Command: config mac_notification interval 1 historysize 500

Success.

DGS-3627:5#
```

config mac_notification ports

Purpose	Used to configure MAC address notification status settings.
Syntax	config mac_notification ports [<portlist> all] [enable disable]
Description	MAC address notification is used to monitor MAC addresses learned and entered into the FDB.
Parameters	<i><portlist></i> - Specify a port or range of ports to be configured. The beginning and end of the port list range are separated by a dash. Non-contiguous portlist entries are separated by a comma. (ex: 1-3,7-9) <i>all</i> - Entering this command will set all ports on the system. <i>[enable disable]</i> - These commands will enable or disable MAC address table notification on the Switch.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To enable port 7 for MAC address table notification:

```
DGS-3627:5#config mac_notification ports 7 enable
Command: config mac_notification ports 7 enable

Success.

DGS-3627:5#
```

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-3627:5#show mac_notification
Command: show mac_notification

Global Mac Notification Settings

State      : Enabled
Interval   : 1
History Size : 1

DGS-3627:5#
```

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. The beginning and end of the port list range are separated by a dash. Non-contiguous portlist entries are separated by a comma. (ex: 1-3,7-9) 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-3627:5#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
13	Disabled
14	Disabled
15	Disabled
16	Disabled
17	Disabled
18	Disabled
19	Disabled
20	Disabled
CTRL+C ESC q Quit SPACE n Next Page Enter Next Entry a All	

WEB-BASED ACCESS CONTROL (WAC) COMMANDS

Web-based Access Control is another port based access control method implemented similarly to the 802.1x port based access control method previously stated. This function will allow user authentication through a RADIUS server or through the local username and password set on the Switch when a user is trying to access the network via the Switch, if the port connected to the user is enabled for this feature.

The user attempting to gain web access will be prompted for a username and password before being allowed to accept HTTP packets from the Switch. Once accepted, the user will be placed in the configured VLAN that has been set for Web-based Access Control. If denied access, no packets will pass through to the user and thus, will be prompted for a username and password again.

Please note that if you choose to use Web-based Access Control, SSL will not be available as the two are mutually exclusive.

The Web-based Access Control (WAC) 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>}
create wac user	<username 15> {vlan <vlan_name 32>}
config wac user	<username 15> vlan <vlan_name 32>
delete wac user	<username 15>
show wac user	
show wac	{ports [<portlist> all]}

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

enable wac	
Purpose	Used to enable the Web-based Access Control on the Switch.
Syntax	enable wac
Description	This command is used to enable Web-based Access Control globally on the Switch.
Parameters	None.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To enable Web-based Access Control globally on the Switch.

```
DGS-3627:5#enable wac
Command: enable wac

Success.

DGS-3627:5#
```

disable wac

Purpose	Used to disable the Web-based Access Control on the Switch.
Syntax	disable wac
Description	This command is used to disable Web-based Access Control globally on the Switch.
Parameters	None.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To enable Web-based Access Control globally on the Switch.

```
DGS-3627:5#disable wac
Command: disable wac

Success.

DGS-3627:5#
```

config wac

Purpose	Used to configure the parameters for the Web-based Access Control feature on this Switch
Syntax	config wac {vlan <vlan_name 32> ports [<portlist> all] state [enable disable] method [local radius] default_redirpath <string 128>}
Description	This command is used to configure the appropriate switch parameters for the Web-based Access Control, including the specification of a VLAN, ports to be enabled for WAC and the method used to authenticate users trying to access the network via the switch
Parameters	<p><i>vlan</i> <vlan_name 32> - Enter the VLAN name which users will be placed when authenticated by the Switch or a RADIUS server. This VLAN should be pre-configured to have limited access rights to web based authenticated users.</p> <p><i>ports</i> – Specify this parameter to add ports to be enabled as Web-based Access Control ports. Only these ports will accept authentication parameters from the user wishing limited access rights through the Switch.</p> <ul style="list-style-type: none"> • <portlist> - Specify a port or range of ports to be set as Web-based Access Control ports. • <i>all</i> – Specify this parameter to set all ports as Web-based Access Control ports. <p><i>state</i> [enable disable] – Choose whether to enable or disable the previously set ports and VLAN as Web-based Access Control ports.</p> <p><i>method</i> – Select this parameter to select a method of authentication for users trying to access the network via the switch. There are two options:</p> <ul style="list-style-type: none"> • <i>local</i> – Choose this parameter to use the local authentication method of the Switch as the authenticating method for users trying to access the network via the switch. This is, in fact, the username and password to access the Switch. • <i>radius</i> – Choose this parameter to use a remote RADIUS server as the authenticating method for users trying to access the network via the switch. This RADIUS server must have

config wac

already been pre-assigned by the administrator using the **config radius** commands located in the 802.1x section.

default_redirpath - Enter the URL of the website that authenticated users placed in the VLAN are directed to once authenticated. This path must be entered into this field before the Web-based Access Control can be enabled.

Restrictions

The WAC VLAN, ports and method can only be configured separately. Only administrator-level and operator-level users can issue this command.

Example usage:

To configure the WAC VLAN:

```
DGS-3627:5#config wac vlan Balkman
Command: config wac vlan Balkman

Success.

DGS-3627:5#
```

Example usage:

To configure the WAC ports:

```
DGS-3627:5#config wac ports 1-7 state enable
Command: config wac ports 1-7 state enable

Success.

DGS-3627:5#
```

Example usage:

To configure the Web-based Access Control method:

```
DGS-3628:4#config wac method local
Command: config wac method local

Success.

DGS-3627:5#
```



NOTE: To enable the Web-based Access Control function, the redirection path field must have the URL of the website that users will be directed to once they enter the limited resource, pre-configured VLAN. Users which attempt Apply settings without the Redirection Page field set will be prompted with an error message and Web-based Access Control will not be enabled. The URL should follow the form `http(s)://www.dlink.com`



NOTE: The subnet of the IP address of the authentication VLAN must be the same as that of the client, or the client will always be denied authentication.

create wac user

Purpose	Used to create a Web-based Access Control user on the switch
Syntax	create wac user <username 15> {vlan <vlan_name 32>}
Description	This command is used to create a Web-based Access Control user on the Switch.
Parameters	<p><i><username 15></i> -Enter a username of up to 15 alphanumeric characters used to authenticate users trying to access the network via the Switch. This username must be identical to the one the user enters to access the Web-based Access Control for the Switch.</p> <p><i>vlan <vlan_name 32></i> - Enter the VLAN name of the VLAN this user will be placed in, once authenticated.</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

To create a WAC user on the Switch.

```
DGS-3627:5#create wac user ctsnow vlan Tiberius
Command: create wac user ctsnow vlan Tiberius

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

Success.

DGS-3627:5#
```

delete wac user

Purpose	Used to delete a Web-based Access Control user on the switch
Syntax	delete wac user <username 15>
Description	This command is used to delete a Web-based Access Control user on the Switch.
Parameters	<p><i><username 15></i> -Enter a username of up to 15 alphanumeric characters used to authenticate users trying to access the network via the Switch. This username must be identical to the one the user enters to access the Web-based Access Control for the Switch.</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

To delete a WAC user on the Switch.

```
DGS-3627:5#delete wac user ctsnow
Command: delete wac user ctsnow

Success.

DGS-3627:5#
```

config wac user

Purpose	Used to configure a previously created Web-based Access Control
---------	---

config wac user

	user on the Switch.
Syntax	config wac user <username 15> vlan <vlan_name 32>
Description	This command is used to configure a previously created Web-based Access Control user on the Switch.
Parameters	<i><username 15></i> - Enter a username of up to 15 alphanumeric characters used to authenticate users trying to access the network via the Switch. This username must be identical to the one the user enters to access the Web-based Access Control for the Switch. <i>vlan <vlan_name 32></i> - Enter the VLAN name of the VLAN this user will be placed in, once authenticated, if a change in VLANs is desired.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure a WAC user on the Switch.

```
DGS-3627:5#config wac user Peter vlan Chandler
Command: config wac user Peter vlan Chandler

Success.

DGS-3627:5#
```

show wac user

Purpose	Used to display the parameters for a previously created Web-based Access Control user on the Switch.
Syntax	show wac user
Description	This command is used to display the parameters for a previously created Web-based Access Control user on the Switch.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To display the parameters for the WAC user:

```
DGS-3627:5#show wac user
Command: show wac user

Current Accounts:
Username      VLAN name
-----
ctsnow       Tiberius

Total Entries : 1

DGS-3627:5#
```

show wac

Purpose	Used to display the parameters for the Web-based Access Control settings currently configured on the Switch.
Syntax	show wac {ports [<portlist> all]}
Description	This command is used to display the parameters for the Web-based Access Control settings currently configured on the Switch.
Parameters	<p><i>ports <portlist></i>- Use this parameter to define ports to be viewed for their Web-based Access Control settings.</p> <p><i>all</i> – Use this parameter to display all ports for their Web-based Access Control settings.</p> <p>Entering no parameters will display the remaining parameters of state, authentication method and Web-based Access Control VLAN currently set on the Switch.</p>
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To display the WAC parameters

```
DGS-3627:5#show wac
Command: show wac

Web Based Access Control
-----
State           : Enable
Method          : Local
VLAN            :
Redirection Page :

DGS-3627:5#
```

Example usage:

To display the WAC enabled ports:

```
DGS-3627:5#show wac ports 1-10
Command: show wac ports 1-10

Port   State
----   -
1      Disabled
2      Disabled
3      Disabled
4      Disabled
5      Disabled
6      Disabled
7      Disabled
8      Disabled
9      Disabled
10     Enabled

DGS-3627:5#
```



NOTE: A successful authentication should direct the client to the stated web page. If the client does not reach this web page, yet does not receive a Fail! message, the client will already be authenticated and therefore should refresh the current browser window or attempt to open a different web page.

ACCESS AUTHENTICATION CONTROL COMMANDS

The TACACS / XTACACS / TACACS+ / RADIUS commands allow users to 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 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}
delete authen_login method_list_name	<string 15>
show authen_login	{default method_list_name <string 15> all}
create authen_enable method_list_name	<string 15>
config authen_enable	[default method_list_name <string 15>] method {tacacs xtacacs tacacs+ radius server_group <string 15> local_enable none}
delete authen_enable method_list_name	<string 15>
show authen_enable	[default method_list_name <string 15> all]
config authen application	{console telnet ssh http all} [login enable] [default method_list_name <string 15>]
show authen application	
create authen server_group	<string 15>
config authen server_group	[tacacs xtacacs tacacs+ radius <string 15>] [add delete] server_host <ipaddr> protocol [tacacs xtacacs tacacs+ radius]
delete authen server_group	<string 15>
show authen server_group	<string 15>
create authen server_host	<ipaddr> protocol [tacacs xtacacs tacacs+ radius] {port <int 1-65535> key [<key_string 254> none] timeout <int 1-255> retransmit <int 1-255>}
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>}
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-3627:5#enable authen_policy
Command: enable authen_policy

Success.

DGS-3627:5#
```

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-3627:5#disable authen_policy
Command: disable authen_policy

Success.

DGS-3627:5#
```

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	None.

Example usage:

To display the system access authentication policy:

```
DGS-3627:5#show authen_policy
Command: show authen_policy

Authentication Policy: Enabled

DGS-3627:5#
```

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 <i>method list</i> .
Restrictions	Only administrator-level users can issue this command.

Example usage:

To create the method list “Trinity.”:

```
DGS-3627:5#create authen_login method_list_name DLee
Command: create authen_login method_list_name DLee

Success.

DGS-3627:5#
```

config authen_login	
Purpose	Used to configure a user-defined or default <i>method list</i> 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}
Description	This command will configure a user-defined or default <i>method list</i> 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 <i>tacacs – xtacacs – local</i> , the Switch will send an authentication request to the first <i>tacacs</i> host in the server group. If no response comes from the server host, the Switch will send an authentication request to the second <i>tacacs</i> 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, <i>xtacacs</i> . If no authentication takes place using the <i>xtacacs</i> list, the <i>local</i> 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

config authen_login

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:

- *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 “DLee” with authentication methods TACACS, XTACACS and local, in that order.

```
DGS-3627:5#config authen_login method_list_name DLee method tacacs xtacacs local
Command: config authen_login method_list_name DLee method tacacs xtacacs local

Success.

DGS-3627:5#
```

Example usage:

To configure the default method list with authentication methods XTACACS, TACACS+ and local, in that order:

```
DGS-3627:5#config authen_login default method xtacacs tacacs+ local
Command: config authen_login default method xtacacs tacacs+ local

Success.

DGS-3627:5#
```

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	<i><string 15></i> - Enter an alphanumeric string of up to 15 characters to define the given <i>method list</i> to delete.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To delete the method list named “DLee”:

```
DGS-3627:5#delete authen_login method_list_name DLee
Command: delete authen_login method_list_name DLee

Success.

DGS-3627:5#
```

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	<i>default</i> – Entering this parameter will display the default method list for users logging on to the Switch. <i>method_list_name <string 15></i> - Enter an alphanumeric string of up to 15 characters to define the given <i>method list</i> to view.

show authen_login

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 None.

Example usage:

To view the authentication login method list named Trinity:

```
DGS-3627:5#show authen_login method_list_name Trinity
Command: show authen_login method_list_name Trinity

Method List Name  Priority  Method Name  Comment
-----
Dlee              1        tacacs+      Built-in Group
                  2        tacacs       Built-in Group
                  3        ctsnow       User-defined Group
                  4        local        Keyword

DGS-3627:5#
```

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 <i>enable method list</i> 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-3627:5#create authen_enable method_list_name Permit
```

```
Command: show authen_login method_list_name Permit
```

```
Success.
```

```
DGS-3627:5#
```

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}
Description	<p>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.</p> <p>The sequence of methods implemented in this command will affect the authentication result. For example, if a user enters a sequence of methods like <i>tacacs – xtacacs – local_enable</i>, 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 <i>local_enable</i> password set in the Switch is used to authenticate the user.</p> <p>Successful authentication using any of these methods will give the user an "Admin" level privilege.</p>
Parameters	<p><i>default</i> – 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 of the following authentication methods:</p> <ul style="list-style-type: none"> ▪ <i>tacacs</i> – Adding this parameter will require the user to be authenticated using the TACACS protocol from the remote TACACS <i>server hosts</i> of the TACACS <i>server group</i> list. ▪ <i>xtacacs</i> – Adding this parameter will require the user to be authenticated using the XTACACS protocol from the remote XTACACS <i>server hosts</i> of the XTACACS <i>server group</i> list. ▪ <i>tacacs+</i> – Adding this parameter will require the user to be authenticated using the TACACS+ protocol from the remote TACACS+ <i>server hosts</i> of the TACACS+ <i>server group</i> list. ▪ <i>radius</i> – Adding this parameter will require the user to be authenticated using the RADIUS protocol from the remote RADIUS <i>server hosts</i> of the RADIUS <i>server group</i> list. ▪ <i>server_group <string 15></i> - Adding this parameter will require the user to be authenticated using a user-defined server group previously configured on the Switch. ▪ <i>local_enable</i> - Adding this parameter will require the user to be authenticated using the local <i>user account</i> database on the Switch. ▪ <i>none</i> – Adding this parameter will require no authentication to access the Switch. <p><i>method_list_name</i> – Enter a previously implemented method list name</p>

config authen_enable

defined by the user (*create authen_enable*). 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_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-3627:5#config authen_enable method_list_name DLee method tacacs xtacacs local
Command: config authen_enable method_list_name DLee method tacacs xtacacs local

Success.

DGS-3627:5#
```

Example usage:

To configure the default method list with authentication methods XTACACS, TACACS+ and local, in that order:

```
DGS-3627:5#config authen_enable default method xtacacs tacacs+ local
Command: config authen_enable default method xtacacs tacacs+ local

Success.

DGS-3627:5#
```

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.

delete authen_enable method_list_name

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	<i><string 15></i> - Enter an alphanumeric string of up to 15 characters to define the given <i>enable method list</i> to delete.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To delete the user-defined method list "Permit"

```
DGS-3627:5#delete authen_enable method_list_name Permit
Command: delete authen_enable method_list_name Permit

Success.

DGS-3627:5#
```

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	<p><i>default</i> – Entering this parameter will display the default method list for users attempting to gain access to Administrator-level privileges on the Switch.</p> <p><i>method_list_name <string 15></i> - Enter an alphanumeric string of up to 15 characters to define the given <i>method list</i> to view.</p> <p><i>all</i> – Entering this parameter will display all the authentication login methods currently configured on the Switch.</p> <p>The window will display the following parameters:</p> <ul style="list-style-type: none"> ▪ 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. <i>User-defined Group</i> refers to <i>server groups</i> defined by the user. <i>Built-in Group</i> refers to the TACACS, XTACACS, TACACS+ and RADIUS security protocols which are permanently set in the Switch. <i>Keyword</i> refers to authentication using a technique INSTEAD of TACACS/XTACACS/TACACS+/RADIUS which are local (authentication through the <i>local_enable</i> 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-3627:5#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	ctsnow	User-defined Group
	4	local	Keyword
default	1	tacacs+	Built-in Group
	2	local	Keyword

```
Total Entries : 2
DGS-3627:5#
```

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, HTTP) for login at the user level and at the administration level (<i>authen_enable</i>) utilizing a previously configured method list.
Parameters	<p><i>application</i> – Choose the application to configure. The user may choose one of the following five options to configure.</p> <ul style="list-style-type: none"> ▪ <i>console</i> – Choose this parameter to configure the command line interface login method. ▪ <i>telnet</i> – Choose this parameter to configure the Telnet login method. ▪ <i>ssh</i> – Choose this parameter to configure the Secure Shell login method. ▪ <i>http</i> – Choose this parameter to configure the web interface login method. ▪ <i>all</i> – Choose this parameter to configure all applications (console, Telnet, SSH, web) login method. <p><i>login</i> – Use this parameter to configure an application for normal login on the user level, using a previously configured method list.</p> <p><i>enable</i> - Use this parameter to configure an application for upgrading a normal user level to administrator privileges, using a previously configured method list.</p> <p><i>default</i> – Use this parameter to configure an application for user authentication using the default method list.</p> <p><i>method_list_name <string 15></i> - 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.</p>
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure the default method list for the web interface:


```
DGS-3627:5#config authen application http login default
Command: config authen application http login default

Success.

DGS-3627:5#
```

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	None.

Example usage:

To display the login and enable method list for all applications on the Switch:

```
DGS-3627:5#show authen application
Command: show authen application
```

Application	Login Method List	Enable Method List
Console	default	default
Telnet	DLee	default
SSH	default	default
HTTP	default	default

```
DGS-3627:5#
```

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	<p><i>server_host</i> <ipaddr> - The IP address of the remote server host to add.</p> <p><i>protocol</i> - The protocol used by the server host. The user may choose one of the following:</p> <ul style="list-style-type: none"> ▪ <i>tacacs</i> - Enter this parameter if the server host utilizes the

create authen server_host

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-3627:5#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-3627:5#
```

config authen server_host

Purpose	Used to configure a user-defined 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 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.

config authen server_host

Parameters	<p><i>server_host</i> <ipaddr> - The IP address of the remote server host the user wishes to alter.</p> <p><i>protocol</i> – The protocol used by the server host. The user may choose one of the following:</p> <ul style="list-style-type: none"> ▪ <i>tacacs</i> – Enter this parameter if the server host utilizes the TACACS protocol. ▪ <i>xtacacs</i> - Enter this parameter if the server host utilizes the XTACACS protocol. ▪ <i>tacacs+</i> - Enter this parameter if the server host utilizes the TACACS+ protocol. ▪ <i>radius</i> - Enter this parameter if the server host utilizes the RADIUS protocol. <p><i>port</i> <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.</p> <p><i>key</i> <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.</p> <p><i>timeout</i> <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.</p> <p><i>retransmit</i> <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.</p>
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-3627:5#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-3627:5#
```

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	<p><i>server_host</i> <ipaddr> - The IP address of the remote server host to be deleted.</p> <p><i>protocol</i> – The protocol used by the server host to delete. The user may choose one of the following:</p> <ul style="list-style-type: none"> ▪ <i>tacacs</i> – Enter this parameter if the server host utilizes the

delete authen server_host

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-3627:5#delete authen server_host 10.1.1.121 protocol tacacs+
Command: delete authen server_host 10.1.1.121 protocol tacacs+

Success.

DGS-3627:5#
```

show authen server_host

Purpose	Used to view a user-defined authentication server host.
Syntax	show authen server_host
Description	<p>This command is used to view user-defined authentication server hosts previously created on the Switch.</p> <p>The following parameters are displayed:</p> <p>IP Address – The IP address of the authentication server host.</p> <p>Protocol – The protocol used by the server host. Possible results will include TACACS, XTACACS, TACACS+ or RADIUS.</p> <p>Port – The virtual port number on the server host. The default value is 49.</p> <p>Timeout - The time in seconds the Switch will wait for the server host to reply to an authentication request.</p> <p>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.</p> <p>Key - Authentication key to be shared with a configured TACACS+ server only.</p>
Parameters	None.
Restrictions	None.

Example usage:

To view authentication server hosts currently set on the Switch:

```
DGS-3627:5#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-3627:5#
```

create authn server_group

Purpose	Used to create a user-defined authentication server group.
Syntax	create authn 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 authn 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-3627:5#create authn server_group group_1
Command: create authn server_group group_1

Success.

DGS-3627:5#
```

config authn server_group

Purpose	Used to configure a user-defined authentication server group.
Syntax	config authn 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	<p><i>server_group</i> - 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 authn server_group command.</p> <ul style="list-style-type: none"> ▪ <i>tacacs</i> – 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. ▪ <i>xtacacs</i> – 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. ▪ <i>tacacs+</i> – 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. ▪ <i>radius</i> – 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. ▪ <i><string 15></i> - 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.

config authn server_group

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-3627:5# config authn server_group group_1 add server_host
10.1.1.121 protocol tacacs+
Command: config authn server_group group_1 add server_host
10.1.1.121 protocol tacacs+

Success.

DGS-3627:5#
```

delete authn server_group

Purpose	Used to delete a user-defined authentication server group.
Syntax	delete authn server_group <string 15>
Description	This command will delete an authentication server group.
Parameters	<i><string 15></i> - 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-3627:5#delete server_group group_1
Command: delete server_group group_1

Success.

DGS-3627:5#
```

show authn server_group

Purpose	Used to view authentication server groups on the Switch.
Syntax	show authn server_group <string 15>

show authen server_group

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	None.

Example usage:

To view authentication server groups currently set on the Switch.

```
DGS-3627:5#show authen server_group
Command: show authen server_group

Group Name  IP Address          Protocol
-----
Darren      10.53.13.2          TACACS
tacacs      10.53.13.94         TACACS
tacacs+
xtacacs
-----

Total Entries : 4

DGS-3627:5#
```

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	<i>response_timeout</i> <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. 0 disables the timeout for the response. The default value is 30 seconds.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure the response timeout for 60 seconds:

```
DGS-3627:5# config authen parameter response_timeout 60
Command: config authen parameter response_timeout 60

Success.

DGS-3627:5#
```

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	<i>parameter attempt <int 1-255></i> - Set the maximum number of attempts the user may try to become authenticated by the Switch, before being locked out.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To set the maximum number of authentication attempts at 5:

```
DGS-3627:5# config authen parameter attempt 5
Command: config authen parameter attempt 5

Success.

DGS-3627:5#
```

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. The default number of attempts for authentication is 3.
Parameters	None.
Restrictions	None.

Example usage:

To view the authentication parameters currently set on the Switch:

```
DGS-3627:5#show authen parameter
Command: show authen parameter

Response timeout : 60 seconds
User attempts    : 5

DGS-3627:5#
```


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 (<i>none</i>). 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	Only user-level users can issue this command.

Example usage:

To enable administrator privileges on the Switch:

```
DGS-3600:3#enable admin
Password: *****

DGS-3627:5#
```

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 “ <i>local_enable</i> ” 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	< <i>password 15</i> > - 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-3627:5#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-3627:5#
```

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:

1. Create a user account with admin-level access using the **create account admin <username> <password>** command. This is identical to creating any other admin-level 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.
2. 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 user** command. There are three choices as to the method SSH will use to authorize the user, and they are password, publickey and hostbased.
3. Configure the encryption algorithm that SSH will use to encrypt and decrypt messages sent between the SSH Client and the SSH Server.
4. Finally, enable SSH on the Switch using the **enable ssh** command.

After following the above steps, you 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]}
show ssh server	
config ssh user	<username> authmode [hostbased [hostname <domain_name> hostname_IP <domain_name> <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-level and operator-level users can issue this command.

Usage example:

To enable SSH:

```
DGS-3627:5#enable ssh
Command: enable ssh

Success.

DGS-3627:5#
```

disable ssh

Purpose	Used to disable SSH.
Syntax	disable ssh
Description	This command allows users to disable SSH on the Switch. Enabling SSH will disable the Telnet-manager on the Switch.
Parameters	None.
Restrictions	Only administrator-level and operator-level users can issue this command.

Usage example:

To disable SSH:

```
DGS-3627:5# disable ssh
Command: disable ssh

Success.

DGS-3627:5#
```

config ssh authmode

Purpose	Used to configure the SSH authentication mode setting.
Syntax	config ssh authmode [password publickey hostbased] [enable disable]
Description	This command will allow users to configure the SSH authentication mode for users attempting to access the Switch.
Parameters	<p><i>password</i> – This parameter may be chosen if the administrator wishes to use a locally configured password for authentication on the Switch.</p> <p><i>publickey</i> - This parameter may be chosen if the administrator wishes to use a publickey configuration set on a SSH server, for authentication.</p> <p><i>hostbased</i> - 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.</p> <p><i>[enable disable]</i> - This allows users to enable or disable SSH authentication on the Switch.</p>
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To enable the SSH authentication mode by password:

```
DGS-3627:5#config ssh authmode password enable
Command: config ssh authmode password enable

Success.

DGS-3627:5#
```

show ssh authmode

Purpose	Used to display the SSH authentication mode setting.
Syntax	show ssh authmode
Description	This command will allow users 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-3627:5#show ssh authmode
Command: show ssh authmode

The SSH authmode:
-----
Password   : Enabled
Publickey  : Enabled
Hostbased  : Enabled

DGS-3627:5#
```

config ssh server

Purpose	Used to configure the SSH server.
Syntax	config ssh server {maxsession <int 1-8> timeout <sec 120-600> authfail <int 2-20> rekey [10min 30min 60min never]}
Description	This command allows you to configure the SSH server.
Parameters	<p><i>maxsession <int 1-8></i> - Allows the user to set the number of users that may simultaneously access the Switch. The default setting is 8.</p> <p><i>timeout <sec 120-600></i> - Allows the user to set the connection timeout. The user may set a time between 120 and 600 seconds. The default is 300 seconds.</p> <p><i>authfail <int 2-20></i> - 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.</p> <p><i>rekey [10min 30min 60min never]</i> - Sets the time period that the Switch will change the security shell encryptions.</p>
Restrictions	Only administrator-level and operator-level users can issue this command.

Usage Example:

To configure the SSH server:

```
DGS-3627:5# config ssh server maxsession 2 contimeout 300 authfail 2
Command: config ssh server maxsession 2 contimeout 300 authfail 2

Success.

DGS-3627:5#
```

show ssh server

Purpose	Used to display the SSH server setting.
Syntax	show ssh server
Description	This command allows users to display the current SSH server setting.
Parameters	None.
Restrictions	None.

Usage Example:

To display the SSH server:

```
DGS-3627:5# show ssh server
Command: show ssh server

SSH Server Status           : Disabled
SSH Max Session             : 8
Connection timeout         : 300
Authenticate failed attempts : 2
Rekey timeout               : never
port                        : 22

DGS-3627:5#
```

config ssh user

Purpose	Used to configure the SSH user.
Syntax	config ssh user <username> authmode [hostbased [hostname <domain_name> hostname_IP <domain_name> <ipaddr>] password publickey]
Description	This command allows configuration of the SSH user authentication method.
Parameters	<p><i><username></i> - Enter a username of no more than 15 characters to identify the SSH user.</p> <p><i>authmode</i> – Specifies the authentication mode of the SSH user wishing to log on to the Switch. The administrator may choose between:</p> <ul style="list-style-type: none"> • <i>hostbased</i> – 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. • <i>hostname <domain_name></i> - Enter an alphanumeric string of up to 32 characters identifying the remote SSH user. • <i>hostname_IP <domain_name> <ipaddr></i> - Enter the hostname and the corresponding IP address of the SSH

config ssh user

user.

password – This parameter should be chosen if the user wishes to use an administrator defined password for authentication. Upon entry of this command, the Switch will prompt the user for a password, and then to retype the password for confirmation.

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-3627:5# config ssh user Tiberius authmode Password
Command: config ssh user Tiberius authmode Password

Enter a case sensitive new password: *****
Enter the new password again for conformation:*****

Success.

DGS-3627:5#
```

show ssh user authmode

Purpose	Used to display the SSH user setting.
Syntax	show ssh user authmode
Description	This command allows you to display the current SSH user setting.
Parameters	None.
Restrictions	None.

Example usage:

To display the SSH user:

```
DGS-3627:5#show ssh user authmode
Command: show ssh user authmode

Current Accounts:
UserName            AuthMode            Hostname            HostIP
-----
Tiberius            Hostbased            Zlra                11.1.1.1

DGS-3627:5#
```



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 user 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 allows users to configure the desired type of SSH algorithm used for authentication encryption.
Parameters	<p><i>3DES</i> – This parameter will enable or disable the Triple_Data Encryption Standard encryption algorithm.</p> <p><i>AES128</i> - This parameter will enable or disable the Advanced Encryption Standard AES128 encryption algorithm.</p> <p><i>AES192</i> - This parameter will enable or disable the Advanced Encryption Standard AES192 encryption algorithm.</p> <p><i>AES256</i> - This parameter will enable or disable the Advanced Encryption Standard AES256 encryption algorithm.</p> <p><i>arcfour</i> - This parameter will enable or disable the Arcfour encryption algorithm.</p> <p><i>blowfish</i> - This parameter will enable or disable the Blowfish encryption algorithm.</p> <p><i>cast128</i> - This parameter will enable or disable the Cast128 encryption algorithm.</p> <p><i>twofish128</i> - This parameter will enable or disable the twofish128 encryption algorithm.</p> <p><i>twofish192</i> - This parameter will enable or disable the twofish192 encryption algorithm.</p> <p><i>twofish256</i> - This parameter will enable or disable the twofish256 encryption algorithm.</p> <p><i>MD5</i> - This parameter will enable or disable the MD5 Message Digest encryption algorithm.</p> <p><i>SHA1</i> - This parameter will enable or disable the Secure Hash Algorithm encryption.</p> <p><i>RSA</i> - This parameter will enable or disable the RSA encryption algorithm.</p> <p><i>DSA</i> - This parameter will enable or disable the Digital Signature Algorithm encryption.</p> <p><i>[enable disable]</i> – This allows users to enable or disable algorithms entered in this command, on the Switch.</p>
Restrictions	Only administrator-level and operator-level users can issue this command.

Usage example:

To configure SSH algorithm:

```
DGS-3627:5# config ssh algorithm Blowfish enable
Command: config ssh algorithm Blowfish enable

Success.

DGS-3627:5#
```

show ssh algorithm

Purpose	Used to display the SSH algorithm setting.
Syntax	show ssh algorithm
Description	This command will display the current SSH algorithm setting status.

show ssh algorithm

Parameters	None.
Restrictions	None.

Usage Example:

To display SSH algorithms currently set on the Switch:

```
DGS-3627:5#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

DGS-3627:5#
```


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 ciphersuite 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}}
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}}
config ssl cachetimeout timeout	<value 60-86400>
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}}
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	<p><i>ciphersuite</i> - 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:</p> <ul style="list-style-type: none"> • <i>RSA_with_RC4_128_MD5</i> – This ciphersuite combines the RSA key exchange, stream cipher RC4 encryption with 128-bit keys and the MD5 Hash Algorithm. • <i>RSA_with_3DES_EDE_CBC_SHA</i> - This ciphersuite combines the RSA key exchange, CBC Block Cipher 3DES_EDE encryption and the SHA Hash Algorithm. • <i>DHE_DSS_with_3DES_EDE_CBC_SHA</i> - This ciphersuite combines the DSA Diffie Hellman key exchange, CBC Block Cipher 3DES_EDE encryption and SHA Hash Algorithm. • <i>RSA_EXPORT_with_RC4_40_MD5</i> - This ciphersuite combines the RSA Export key exchange, stream cipher RC4 encryption with 40-bit keys. <p>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.</p>
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To enable SSL on the Switch for all ciphersuites:

```
DGS-3627:5#enable ssl
```

```
Command:enable ssl
```

Note: Web will be disabled if SSL is enabled.

Success.

```
DGS-3627:5#
```



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 your 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}}
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	<p><i>ciphersuite</i> - 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:</p> <ul style="list-style-type: none"> • <i>RSA_with_RC4_128_MD5</i> – This ciphersuite combines the RSA key exchange, stream cipher RC4 encryption with 128-bit keys and the MD5 Hash Algorithm. • <i>RSA_with_3DES_EDE_CBC_SHA</i> - This ciphersuite combines the RSA key exchange, CBC Block Cipher 3DES_EDE encryption and the SHA Hash Algorithm. • <i>DHE_DSS_with_3DES_EDE_CBC_SHA</i> - This ciphersuite combines the DSA Diffie Hellman key exchange, CBC Block Cipher 3DES_EDE encryption and SHA Hash Algorithm. • <i>RSA_EXPORT_with_RC4_40_MD5</i> - This ciphersuite combines the RSA Export key exchange, stream cipher RC4 encryption with 40-bit keys.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To disable the SSL status on the Switch:

```
DGS-3627:5#disable ssl
Command: disable ssl

Success.

DGS-3627:5#
```

To disable ciphersuite RSA_EXPORT_with_RC4_40_MD5 only:

```
DGS-3627:5#disable ssl ciphersuite RSA_EXPORT_with_RC4_40_MD5
Command: disable ssl ciphersuite RSA_EXPORT_with_RC4_40_MD5

Success.

DGS-3627:5#
```

config ssl cachetimeout timeout

Purpose	Used to configure the SSL cache timeout.
Syntax	config ssl cachetimeout <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

config ssl cachetimeout timeout

	process.
Parameters	<i>timeout <value 60-86400></i> - 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 and operator-level users can issue this command.

Example usage:

To set the SSL cachetimeout for 7200 seconds:

```
DGS-3627:5#config ssl cachetimeout 7200
Command: config ssl cachetimeout 7200

Success.

DGS-3627:5#
```

show ssl cachetimeout

Purpose	Used to show the SSL cache timeout.
Syntax	show ssl cachetimeout
Description	Entering this command will allow the user 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-3627:5#show ssl cachetimeout
Command: show ssl cachetimeout

Cache timeout is 600 second(s).

DGS-3627:5#
```

show ssl

Purpose	Used to view the SSL status and the certificate file status on the Switch.
Syntax	show ssl {certificate}
Description	This command is used to view the SSL status on the Switch.
Parameters	<i>{certificate}</i> – Use this parameter to display the SSL certificate file information currently implemented on the Switch.
Restrictions	None.

Example usage:

To view the SSL status on the Switch:

```
DGS-3627:5#show ssl
Command: show ssl

SSL Status                               Disabled
RSA_WITH_RC4_128_MD5                     0x0004 Enabled
RSA_WITH_3DES_EDE_CBC_SHA                0x000A Enabled
DHE_DSS_WITH_3DES_EDE_CBC_SHA           0x0013 Enabled
RSA_EXPORT_WITH_RC4_40_MD5               0x0003 Enabled

DGS-3627:5#
```

Example usage:

To view certificate file information on the Switch:

```
DGS-3627:5# show ssl certificate
Command: show ssl certificate

Loaded with RSA Certificate!

DGS-3627:5#
```

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	<i><ipaddr></i> - Enter the IP address of the TFTP server. <i>certfilename <path_filename 64></i> - Enter the path and the filename of the certificate file you wish to download. <i>keyfilename <path_filename 64></i> - Enter the path and the filename of the key exchange file you wish to download.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To download a certificate file and key file to the Switch:

```
DGS-3627:5#download ssl certificate 10.53.13.94 certfilename c:/cert.der
keyfilename c:/pkey.der
Command: download ssl certificate 10.53.13.94 certfilename c:/cert.der
keyfilename c:/pkey.der

Certificate Loaded Successfully!

DGS-3627:5#
```

JUMBO FRAME COMMANDS

Certain switches can support jumbo frames (frames larger than the Ethernet frame size of 1536 bytes). To transmit frames of up to 9K (and 9216 bytes tagged), the user can increase the maximum transmission unit (MTU) size from the default of 1536 by enabling the Jumbo Frame command.

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

Command	Parameters
enable jumbo_frame	
disable jumbo_frame	
show jumbo_frame	

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

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 9216 bytes tagged.
Parameters	None.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To enable the jumbo frame function on the Switch:

```
DGS-3627:5#enable jumbo_frame
Command: enable jumbo_frame

Success.

DGS-3627:5#
```

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-level and operator-level users can issue this command.

Example usage:

To disable the jumbo frame function on the Switch:

```
DGS-3627:5#disable jumbo_frame
Command: disable jumbo_frame

Success.

DGS-3627:5#
```

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.

Usage Example:

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

```
DGS-3627:5#show jumbo_frame
Command: show jumbo_frame

Jumbo frame state: disabled
Maximum frame size: 1536 bytes

DGS-3627:5#
```

LLDP COMMANDS

Command	Parameters
enable lldp	
disable lldp	
config lldp	message_tx_interval <sec 5-32768>
config lldp	message_tx_hold_multiplier <int 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}] [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 <vid_list>] [enable disable]
config lldp ports	[<portlist> all] dot1_tlv_vlan_name [vlan [all <vlan_name 32>] vlanid <vid_list>] [enable disable]
config lldp ports	[<portlist> all] dot1_tlv_protocol_identity[all { eapol lacp gvrp stp}] [enable disable]
config lldp ports	[<portlist> all] dot3_tlvs [all {mac_phy_configuration_status link aggregation maximum_frame_size}] [enable disable]
config lldp	forward_message [enable disable]
show lldp	
show lldp mgt_addr	{[ipv4 <ipaddr> ipv6 <ipv6addr>]}
show lldp ports	{<portlist>}
show lldp local_ports	{<portlist>} {mode [brief normal detailed]}
show lldp remote_ports	{<portlist>} {mode [brief normal detailed]}
show lldp statistics	
show lldp statistics ports	{<portlist>}

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

enable lldp

Purpose	Used to enable LLDP operation on the Switch.
Syntax	enable lldp

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 setting. For the advertisement of LLDP packets, the switch announces the information to its neighbor through ports. For the receiving of LLDP packets, the switch will learn the information from the LLDP packets advertised from the neighbor in the Neighbor's table. The default state for LLDP is disabled.
Parameters	None.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To enable LLDP:

```
DGS-3627:5#enable lldp
Command: enable lldp
```

```
Success.
```

```
DGS-3627:5#
```

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-level and operator-level users can issue this command.

Example usage:

To disable LLDP:

```
DGS-3627:5#disable lldp
Command: disable lldp
```

```
Success.
```

```
DGS-3627:5#
```

config lldp message_tx_interval

Purpose	Used to change the packet transmission interval.
Syntax	config lldp message_tx_interval <sec 5 – 32768>
Description	This interval controls how often active ports retransmit advertisements to their neighbors.
Parameters	<i>message_tx_interval</i> – 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-level and operator-level users can issue this command.

Usage Example:

To show the packet transmission interval:

```
DGS-3627:5#config lldp message_tx_interval 30
Command: config lldp message_tx_interval 30

Success.

DGS-3627:5#
```

config lldp message_tx_hold_multiplier

Purpose	Used to configure the message hold multiplier.
Syntax	config lldp message_tx_hold_multiplier <int 2-10 >
Description	This parameter is a multiplier on the msgTxInterval that is used to compute the TTL value of txTTL in an LLDPDU. The TTL will be carried in the LLDPDU packet. The lifetime will be the minimum of 65535 and (message_tx_interval * message_tx_hold_multiplier). At the partner switch, when the time-to-live for a given advertisement expires, the advertised data is deleted from the neighbor switch's MIB.
Parameters	<i>message_hold_multiplier</i> – The range is from 2 to 10. The default setting is 4.
Restrictions	Only administrator-level and operator-level users can issue this command.

Usage Example:

To change the multiplier value:

```
DGS-3627:5#config lldp message_tx_hold_multiplier 3
Command: config lldp message_tx_hold_multiplier 3

Success.

DGS-3627:5#
```

config lldp tx_delay

Purpose	Used to change the minimum time (delay-interval) LLDP ports will delay in 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	<i>tx_delay</i> - 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-level and operator-level users can issue this command.

Example usage:

To configure the delay interval:

```
DGS-3627:5#config lldp tx_delay 8
Command: config lldp tx_delay 8

Success.

DGS-3627:5#
```

config lldp reinit_delay

Purpose	Change the minimum time of the reinitialization delay interval.
Syntax	config lldp reinit_delay <sec 1 - 10>
Description	A re-enabled LLDP port will wait for reinit_delay after last disable command before reinitializing.
Parameters	<i>reinit_delay</i> – The range is from 1 second to 10 seconds. The default setting is 2 seconds.
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To changes the re-initialization delay interval to five seconds:

```
DGS-3627:5#config lldp reinit_delay 5
Command: config lldp reinit_delay 5

Success.

DGS-3627:5#
```

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	Globally change the interval between successive LLDP change notifications generated by the switch.
Parameters	<i>notification_interval</i> – The range is from 5 seconds to 3600 seconds. The default setting is 5 seconds.
Restrictions	Only administrator-level and operator-level users can issue this command.

Usage Example:

To change the notification interval to 10 seconds:

```
DGS-3627:5#config lldp notification_interval 10
Command: config lldp notification_interval 10

Success.

DGS-3627:5#
```

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	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	<i><portlist></i> - Use this parameter to define ports to be configured. <i>all</i> – Use this parameter to set all ports in the system. <i>notification</i> – 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-level and operator-level users can issue this command.

Example usage:

To change the SNMP notification state of ports 1 to 5 to enable:

```
DGS-3627:5#config lldp ports 1:1-1:5 notification enable
Command: config lldp ports 1:1-1:5 notification enable

Success.

DGS-3627:5#
```

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	These options 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	<p><portlist>- Use this parameter to define ports to be configured.</p> <p>all – Use this parameter to set all ports in the system.</p> <p>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.</p>
Restrictions	Only administrator-level and operator-level users can issue this command.

Example usage:

To configure ports 1 to 5 to transmit and receive:

```
DGS-3627:5#config lldp ports 1:1-1:5 admin_status tx_and_rx
Command: config lldp ports 1:1-1:5 admin_status tx_and_rx

Success.

DGS-3627:5#
```

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	<p><portlist>- Use this parameter to define ports to be configured.</p> <p>all – Use this parameter to set all ports in the system.</p> <p>ipv4 – The IP address of IPv4.</p> <p>ipv6 – The IP address of IPv6.</p>
Restrictions	Only administrator-level and operator-level users can issue this command.

Usage Example:

To enable ports 1 to 2 to manage address entry:

```
DGS-3627:5#config lldp ports 1:1-1:2 mgt_addr ipv4 192.168.254.10
enable
Command: config lldp ports 1:1-1:2 mgt_addr ipv4 192.168.254.10
enable

Success.

DGS-3627:5#
```

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 f 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 <i>port_description</i> , <i>system_name</i> , <i>system_description</i> , and <i>system_capability</i> .
Parameters	<p><portlist>- Use this parameter to define ports to be configured.</p> <p>all – Use this parameter to set all ports in the system.</p> <p><i>port_description</i> – This TLV optional data type indicates that LLDP agent should transmit 'Port Description TLV on the port. The default state is disabled.</p> <p><i>system_name</i> – This TLV optional data type includes indicates that LLDP agent should transmit 'System Name TLV'. The default state is disabled.</p> <p><i>system_description</i> – This TLV optional data type includes indicates that LLDP agent should transmit 'System Description TLV'. The default state is disabled.</p> <p><i>system_capabilities</i> – This TLV optional data type includes indicates that LLDP agent should transmit 'System Capabilities TLV'. The system capability will indicate whether the device provides repeater, bridge, or router function, and whether the provided functions are currently enabled. The default state is disabled.</p>
Restrictions	Only administrator-level 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-3627:5#config lldp ports all basic_tlvs system_name enable
Command: config lldp ports all basic_tlvs system_name enable

Success.

DGS-3627:5#
```

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 organization port VLAN ID TLV data types from outbound LLDP advertisements.
Syntax	config lldp ports [<portlist> all] dot1_tlv_pvid [enable disable]
Description	This TLV optional data type determines whether the IEEE 802.1 organization defined port VLAN TLV transmission is allowed on a given LLDP transmission capable port.
Parameters	<p><portlist>- Use this parameter to define ports to be configured.</p> <p>all – Use this parameter to set all ports in the system.</p> <p>dot1_tlv_pvid – This TLV optional data type determines whether the IEEE 802.1 organization defined port VLAN ID TLV transmission is allowed on a given LLDP transmission capable port. The default state is disabled.</p>
Restrictions	Only administrator-level 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-3627:5#config lldp ports all dot1_tlv_pvid enable
```

```
Command: config lldp ports all dot1_tlv_pvid enable
```

```
Success.
```

```
DGS-3627:5#
```

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 organization 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 <vidlist>] [enable disable]
Description	This TLV optional data type indicates 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	<p><portlist>- Use this parameter to define ports to be configured.</p> <p>all – Use this parameter to set all ports in the system.</p> <p>dot1_tlv_protocol_vid – This TLV optional data type determines whether the IEEE 802.1 organization defined port and protocol VLAN ID TLV transmission is allowed on a given LLDP transmission capable port. The default state is disabled.</p>
Restrictions	Only administrator-level 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-3627:5#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-3627:5#
```

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 organization 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 <vidlist>] [enable disable]
Description	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.
Parameters	<p><portlist>- Use this parameter to define ports to be configured.</p> <p>all – Use this parameter to set all ports in the system.</p> <p>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.</p>
Restrictions	Only administrator-level 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-3627:5#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-3627:5#
```


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 organization protocol identity TLV data types from outbound LLDP advertisements.
Syntax	config lldp ports [<portlist> all] dot1_tlv_protocol_identity [all {eapol lacp gvrp stp } [enable disable]
Description	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 identity will be advertised.
Parameters	<p><portlist>- Use this parameter to define ports to be configured.</p> <p>all – Use this parameter to set all ports in the system.</p> <p>dot1_tlv_protocol_identity – This TLV optional data type indicates whether the corresponding Local System's Protocol Identity instance will be transmitted on the port. The Protocol Identity TLV provides a way for stations to advertise protocols that are important to the operation of the network, such as Spanning Tree Protocol, the Link Aggregation Control Protocol, and numerous vendor proprietary variations which are responsible for maintaining the topology and connectivity of the network. If EAPOL, GVRP, STP (including MSTP), and LACP protocol identity is enabled on this port and it is enabled to be advertised, then this protocol identity will be advertised. The default state is disabled.</p>
Restrictions	Only administrator-level 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-3627:5#config lldp ports all dot1_tlv_protocol_identity all
enable
Command: config lldp ports all dot1_tlv_protocol_identity all
enable

Success.

DGS-3627:5#
```

config lldp dot3_tlvs

Purpose	Used to configure an individual port or group of ports to exclude one or more of IEEE 802.3 organization 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	Each Specific TLV in this extension can be enabled individually.
Parameters	<p><portlist>- Use this parameter to define ports to be configured.</p> <p>all – Use this parameter to set all ports in the system.</p> <p>mac_phy_configuration_status - This TLV optional data type indicates</p>

config lldp dot3_tlvs

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-level 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-3627:5#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-3627:5#
```

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-level and operator-level users can issue this command.

Usage Example:

To configure LLDP forward_message:

```
DGS-3627:5#config lldp forward_message enable
Command: config lldp forward_message enable

Success.

DGS-3627:5#
```

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-3627:5#show lldp
Command: show lldp

LLDP System Information
  Chassis ID Subtype      : MAC Address
  Chassis ID              : 00-19-5B-F1-CA-80
  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-3627:5#
```

show lldp mgt_addr

Purpose	Used to display the LLDP management address information.
Syntax	show lldp mgt_addr {[ipv4 <ipaddr> ipv6 <ipv6addr>]}
Description	Displays the LLDP management address information.
Parameters	<i>ipv4</i> – The IP address of IPv4. <i>ipv6</i> – The IP address of IPv6.
Restrictions	None.

Example usage:

To display management address information for port 1:

```
DGS-3627:5# 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     : 1:1-1:5, 1:7, 2:10-2:20

DGS-3627:5#
```

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-3627:5#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_Protcol_VLAN_ID
  (None)
  Enabled VLAN Name    (None)
  Enabled Protocol_Identity
  (None)
  MAC/PHY Configuration/Status Disabled
  Link Aggregation     Disabled
  Maximum Frame Size   Disabled

DGS-3627:5#
```

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	<p><portlist>- Use this parameter to define ports to be configured.</p> <p><i>brief</i> – Display the information in brief mode.</p> <p><i>normal</i> – Display the information in normal mode. This is the default display mode.</p> <p><i>detailed</i> – Display the information in detailed mode.</p>
Restrictions	None.

Usage Example:

To display outbound LLDP advertisements for port 1:

```
DGS-3627:5#show lldp local_ports 1
Command: show lldp local_ports 1

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                   : 1/1
Port Description          : RMON Port 1 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 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-3627:5#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	The global LLDP statistics displays an overview of neighbor detection activity on the switch.
Parameters	None.
Restrictions	None.

Example usage:

To display global statistics information:

```
DGS-3627:5#show lldp statistics
```

```
Command: show lldp statistics
```

```
Last Change Time      : 1705
Number of Table Insert : 0
Number of Table Delete : 0
Number of Table Drop   : 0
Number of Table Ageout : 0
```

```
DGS-3627:5#
```

show lldp statistics ports

Purpose	Used to display the ports LLDP statistics information.
Syntax	show lldp statistics ports{<portlist>}
Description	The per-port LLDP statistics command displays 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-3627:5#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-3627:5#
```

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 as 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 up to 33 switches (numbered 0-32), including the Commander Switch (numbered 0).
- 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 management 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-3600 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-3600, 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 Candidate 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 xStack DGS-3600 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 xStack DGS-3600 Series switches have 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 MS firmware downloads from a TFTP server.
- Configuration Files – This switch now supports 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 MS log files to a TFTP server.



NOTE: For more details regarding improvements made in SIMv1.6, please refer to the Single IP Management 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-3627:5#enable sim
Command: enable sim

Success.

DGS-3627:5#
```

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-3627:5#disable sim
Command: disable sim

Success.

DGS-3627:5#
```

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.

show sim

	<p>MAC Address - Displays the MAC Address of the Switch.</p> <p>Capabilities – Displays the type of switch, be it Layer 2 (L2) or Layer 3 (L3).</p> <p>Platform – Switch Description including name and model number.</p> <p>SIM State –Displays the current Single IP Management State of the Switch, whether it be enabled or disabled.</p> <p>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.</p> <p>Discovery Interval - Time in seconds the Switch will send discovery packets out over the network.</p> <p>Hold time – Displays the time in seconds the Switch will hold discovery results before dropping it or utilizing it.</p>
Parameters	<p><i>candidates <candidate_id 1-100></i> - 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.</p> <p><i>members <member_id 1-32></i> - 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.</p> <p><i>group {commander_mac <macaddr>}</i> - Entering this parameter will display information concerning the SIM group. To view a specific group, include the commander's MAC address of the group.</p> <p><i>neighbor</i> – 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:</p> <ul style="list-style-type: none"> • 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	Only administrator-level and operator-level users can issue this command.

Example usage:

To show the SIM information in detail:

```
DGS-3627:5#show sim
Command: show sim

Group Name       : default
SIM Version      : VER-1.61
Firmware Version : 2.40.B19
Device Name      :
MAC Address      : 00-10-20-33-45-00
Capabilities     : L3
Platform        : DGS-3627 L3 Switch
SIM State       : Disabled
Role State      : Candidate
Discovery Interval : 30 sec
Holdtime        : 100 sec

DGS-3627:5#
```

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

```

DGS-3627:5#show sim candidates
Command: show sim candidates

ID  MAC Address          Platform /
---  -----          -----
2   00-55-55-00-55-00    DGS-3627 L3 Switch   140   2.40.B19   default master

Total Entries: 2

DGS-3627:5#
    
```

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

```

DGS-3627:5#show sim member 1
Command: show sim member 1

ID  MAC Address          Platform /
---  -----          -----
1   00-01-02-03-04-00    DGS-3627 L3 Switch   40    2.40.B19   The Man

Total Entries: 2

DGS-3627:5#
    
```

To show other groups information in summary:

```

DGS-3627:5#show sim group
Command: show sim group

SIM Group Name : default

ID  MAC Address          Platform /
---  -----          -----
*1  00-01-02-03-04-00    DGS-3627 L3 Switch   40    2.40.B19   Tiberius

SIM Group Name : SIM2

ID  MAC Address          Platform /
---  -----          -----
*1  00-01-02-03-04-00    DGS-3627 L3 Switch   40    2.40.B19   Neo

'*' means commander switch.

DGS-3627:5#
    
```

Example usage:

To view SIM neighbors:

```

DGS-3627:5#show sim neighbor
Command: show sim neighbor

Neighbor Info Table

Port  MAC Address          Role
-----
23    00-35-26-00-11-99    Commander
23    00-35-26-00-11-91    Member
24    00-35-26-00-11-90    Candidate
    
```

Total Entries: 3

DGS-3627:5#

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	<i>member_id <value 1-32></i> - Select the ID number of the member switch the user desires to configure. <i>exit</i> – 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-3627:5#reconfig member_id 2
Command: reconfig member_id 2

DGS-3627:5#
Login:
```

config sim_group

Purpose	Used to add candidates and delete members from the SIM group.
Syntax	config sim [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	<i>add <candidate_id 1-100> <password></i> - 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). <i>delete <member_id 1-32></i> - 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-3627:5#config sim_group add 2
Command: config sim_group add 2

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

Success.

DGS-3627:5#
```

To delete a member:

```
DGS-3627:5#config sim_group delete 1
```

```
Command: config sim_group delete 1
```

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

```
Success.
```

```
DGS-3627:5#
```

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	<p><i>commander</i> – Use this parameter to configure the commander switch(CS) for the following parameters:</p> <ul style="list-style-type: none"> ▪ <i>group_name</i> <groupname 64> - Used to update the name of the group. Enter an alphanumeric string of up to 64 characters to rename the SIM group. ▪ <i>dp_interval</i> <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 <i>dp_interval</i> from 30 to 90 seconds. ▪ <i>hold time</i> <sec 100-255> – 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 255 seconds. <p><i>candidate</i> – Used to change the role of a CS (commander) to a CaS (candidate).</p> <ul style="list-style-type: none"> ▪ <i>dp_interval</i> <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 <i>dp_interval</i> from 30 to 90 seconds. ▪ <i>hold time</i> <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.

To change the time interval of the discovery protocol:

```
DGS-3627:5# config sim commander dp_interval 40
```

```
Command: config sim commander dp_interval 40
```

```
Success.
```

```
DGS-3627:5#
```

To change the hold time of the discovery protocol:

```
DGS-3627:5# config sim hold_time 120
Command: config sim hold_time 120

Success.

DGS-3627:5#
```

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

```
DGS-3627:5# config sim candidate
Command: config sim candidate

Success.

DGS-3627:5#
```

To transfer the Switch to be a CS:

```
DGS-3627:5# config sim commander
Command: config sim commander

Success.

DGS-3627:5#
```

To update the name of a group:

```
DGS-3627:5# config sim commander group_name Demetrius
Command: config sim commander group_name Demetrius

Success.

DGS-3627:5#
```

download sim_ms

Purpose	Used to download firmware or configuration file to an indicated device.
Syntax	download sim [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	<p><i>firmware_from_tftp</i> – Specify this parameter to download firmware to members of a SIM group.</p> <p><i>configuration_from_tftp</i> - Specify this parameter to download a switch configuration to members of a SIM group.</p> <p><i><ipaddr></i> – Enter the IP address of the TFTP server.</p> <p><i><path_filename></i> – Enter the path and the filename of the firmware or switch on the TFTP server.</p> <p><i>members</i> – Enter this parameter to specify the members the user prefers to download firmware or switch configuration files to. The user may specify a member or members by adding one of the following:</p> <ul style="list-style-type: none"> ▪ <i><mslist 1-32></i> - Enter a value, or values to specify which members of the SIM group will receive the firmware or switch configuration. ▪ <i>all</i> – Add this parameter to specify all members of the SIM group will receive the firmware or switch configuration.

download sim_ms

Restrictions Only administrator-level users can issue this command.

Example usage:

To download firmware:

```
DGS-3627:5# download sim_ms firmware_from_tftp 10.53.13.94 c:/dgs3627.had all
Command: download sim_ms firmware_from_tftp 10.53.13.94 c:/dgs3627.had all

This device is updating firmware. Please wait...

Download Status :
```

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

```
DGS-3627:5#
```

To download configuration files:

```
DGS-3627:5# download sim configuration_from_tftp 10.53.13.94 c:/dgs3627.txt all
Command: download sim configuration_from_tftp 10.53.13.94 c:/dgs3627.txt all

This device is updating configuration. Please wait...

Download Status :
```

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

```
DGS-3627:5#
```

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	<p><i>configuration_to_tftp</i> - Specify this parameter if the user wishes to upload a switch configuration to members of a SIM group.</p> <p><i>log_to_tftp</i> - Specify this parameter to download a switch log to members of a SIM group.</p> <p><i><ipaddr></i> - Enter the IP address of the TFTP server to upload a configuration file to.</p> <p><i><path_filename></i> - Enter a user-defined path and file name on the TFTP server to which to upload configuration files.</p> <p><i>members</i> - Enter this parameter to specify the members the user prefers to upload switch configuration or log files to. The user may specify a member or members by adding one of the following:</p>

upload sim_ms

- *<mslist>* - Enter a value, or values to specify which members of the SIM group will receive the switch configuration or log files.
- *all* – Add this parameter to specify all members of the SIM group will receive the switch configuration or log files.

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

Example usage:

To upload configuration files to a TFTP server:

```
DGS-3627:5# upload sim_ms configuration 10.55.47.1 D:\configuration.txt 1
Command: upload sim_ms configuration 10.55.47.1 D:\configuration.txt 1
```

```
Success.
```

```
DGS-3627:5#
```

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
?	{<command>}
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-3627:5#?
..
?
clear
clear arptable
clear counters
clear dhcp_binding
clear fdb
clear log
clear port_security_entry port
config 802.1p default_priority
config 802.1p user_priority
config 802.1x auth_mode
config 802.1x auth_parameter ports
config 802.1x capability ports
config 802.1x guest_vlan
config 802.1x guest_vlan ports
config 802.1x init
config 802.1x reauth
config access_profile profile_id
config account
CTRL+C ESC q Quit SPACE n Next Page Enter Next Entry a All
```

To display the parameters for a specific command:

```
DGS-3627:5#? config stp
Command:? config stp

Command: config stp
Usage: {maxage <value 6-40> | maxhops <value1-20> | hellotime <value 1-10> | forwarddelay <value 4-30> | txholdcount <value 1-10> | fbpdudisable | lbd [enable | disable] | lbd_recover_timer [0 | <value 60-1000000>]}
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-3627:5#
```

config command_history	
Purpose	Used to configure the command history.
Syntax	config command_history <value 1-40>
Description	This command is used to configure the command history.
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-3627:5#config command_history 20
Command: config command_history 20

Success.

DGS-3627:5#
```

show command_history	
Purpose	Used to display the command history.
Syntax	show command_history
Description	This command will display the command history.
Parameters	None.
Restrictions	None.

Example usage

To display the command history:

```
DGS-3627:5#show command_history
Command: show command_history

?
? show
show vlan
show command history

DGS-3627:5#
```

TECHNICAL SPECIFICATIONS

General		
Protocols	IEEE 802.3 10BASE-T Ethernet IEEE 802.3u 100BASE-TX Fast Ethernet IEEE 802.3ab 1000BASE-T Gigabit Ethernet IEEE 802.3z 1000BASE-T (SFP “Mini GBIC”) IEEE 802.1D Spanning Tree IEEE 802.1s Multiple Spanning Tree IEEE 802.1w Rapid Spanning Tree IEEE 802.1Q VLAN IEEE 802.1V Protocol VLAN IEEE 802.1p Priority Queues IEEE 802.1X Port Based Network Access Control IEEE 802.3ad Link Aggregation Control IEEE 802.3x Full-duplex Flow Control IEEE 802.3 Nway auto-negotiation	
Fiber-Optic	SFP (Mini GBIC) Support IEEE 802.3z 1000BASE-LX (DEM-310GT transceiver) IEEE 802.3z 1000BASE-SX (DEM-311GT transceiver) IEEE 802.3z 1000BASE-SX (DEM-312GT2 transceiver) IEEE 802.3z 1000BASE-LH (DEM-314GT transceiver) IEEE 802.3z 1000BASE-ZX (DEM-315GT transceiver) IEEE 802.3z WDM Transceiver (DEM-330T transceiver) IEEE 802.3z WDM Transceiver (DEM-330R transceiver) IEEE 802.3z WDM Transceiver (DEM-331T transceiver) IEEE 802.3z WDM Transceiver (DEM-331R transceiver)	
XFP Support		
CX4 Support	IEEE 802.3ae 10G Fiber-Optic	
Standards	IEEE 802.3ak 10G Copper	
Standards	CSMA/CD	
Data Transfer Rates:	Half-duplex	Full-duplex
Ethernet	10 Mbps	20Mbps
Fast Ethernet	100Mbps	200Mbps
Gigabit Ethernet	n/a	2000Mbps
Topology	Star	
Network Cables	Cat.5 Enhanced for 1000BASE-T UTP Cat.5, Cat. 5 Enhanced for 100BASE-TX UTP Cat.3, 4, 5 for 10BASE-T EIA/TIA-568 100-ohm screened twisted-pair (STP)(100m)	
Number of Ports	DGS-3627: 24 x 10/100/1000Mbps ports 4 x 1000Mbps Combo SFP ports 3 available slots for optional 10GE modules DGS-3627G: 24 x 1000Mbps SFP ports	

	4 x 10/100/1000Mbps Combo Ports 3 available slots for optional 10GE modules
DGS-3650:	48 x 10/100/1000 Mbps ports 4 x 1000Mbps Combo SFP Ports 2 available slots for optional 10GE modules
DGS-3612G:	12 x 100/1000Mbps SFP ports 4 x Combo 10/100/1000Mbps ports
DGS-3612:	12 x 10/100/1000Mbps copper ports 4 x Combo 100/1000Mbps SFP ports

Physical and Environmental	
Internal Power Supply	Input: 100~240V, AC/1.3A, 50~60Hz Output: 12V, 10A (MAX)
Power Consumption	DGS-3627 – 72.3W DGS-3627G – 77W DGS-3650 – 131.3W DGS-3612G – 60W DGS-3612 – 38W
DC Fans	DGS-3627 – Four 40mm x 40mm x 20mm; one 50mm x 50mm x 20mm; one 44mm x 44mm x 11mm DGS-3627G – Four 40mm x 40mm x 20mm; one 50mm x 50mm x 20mm fans DGS-3650 – Two 40mm x 40mm x 20mm; three 40mm x 40mm x 10mm; one 75.7mm x 75.7mm x 30mm fans; one 44mm x 44mm x 11mm DGS-3612G – Three 40mm x 40mm x 20mm; one 50mm x 50mm x 20mm fans DGS-3612 - Two 40mm x 40mm x 20mm fans
Operating Temperature	0 - 40°C
Storage Temperature	-40 - 70°C
Humidity	5 - 95% non-condensing
Dimensions	DGS-3627, DGS-3627G, DGS-3650, DGS-3612G – 441mm x 389mm x 44mm DGS-3612 - 441mm x 310mm x 44mm
Weight	DGS-3627, DGS-3627G – 5.5kg (12.13 lbs) DGS-3650 – 6kg (13.23 lbs) DGS-3612G – 5kg (11.02 lbs) DGS-3612 - 3.8kg (8.38 lbs)
EMI	CE Class A, FCC Class A, C-Tick, VCCI
Safety	CB report, CUL

Performance

Transmission Method	Store-and-forward
Packet Buffer	2 MB per device
Packet Filtering/Forwarding Rate	14,881 pps (10M port) 148.810 pps (100M port) 1,488,100 pps (1Gbps port)
MAC Address Learning	Automatic update. Supports 16K MAC address.
Priority Queues	8 Priority Queues per port.
Forwarding Table Age Time	Max age: 10-1000000 seconds. Default = 300.