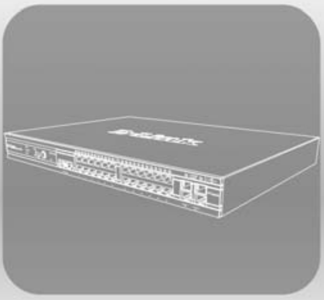


CLI Manual

Product Model : xStack® DGS-3400 Series

Layer 2+ Gigabit Ethernet Managed Switch

Release 2.6

D-Link®

July 2009

651GS3400095G

RECYCLABLE

Table of Contents

1

INTRODUCTION

The xStack® DGS–3400 Series is a member of the D–Link xStack® switch family. xStack® is a complete family of stackable switches that range from edge 10/100Mbps switches to core Gigabit switches. xStack® provides unsurpassed performance, fault tolerance, scalable flexibility, robust security, standard–based interoperability and an impressive support for 10–Gigabit technology to future–proof departmental and enterprise network deployments with an easy migration path.

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. For detailed information on installing hardware please refer also to the Manual.

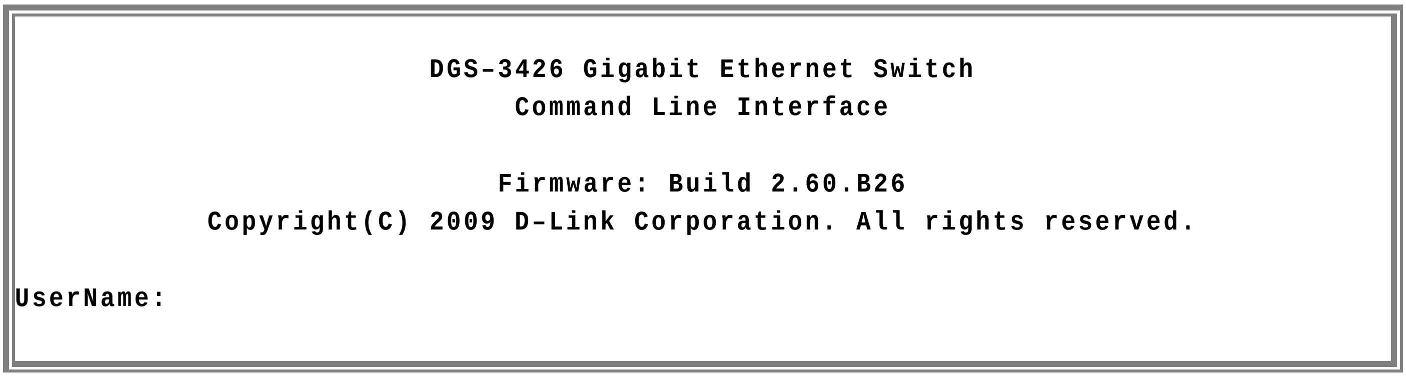
Accessing the Switch via the Serial Port

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 o refresh the console screen.



```
                    DGS–3426 Gigabit Ethernet Switch
                         Command Line Interface

                        Firmware: Build 2.60.B26
          Copyright(C) 2009 D–Link Corporation. All rights reserved.

UserName:
```

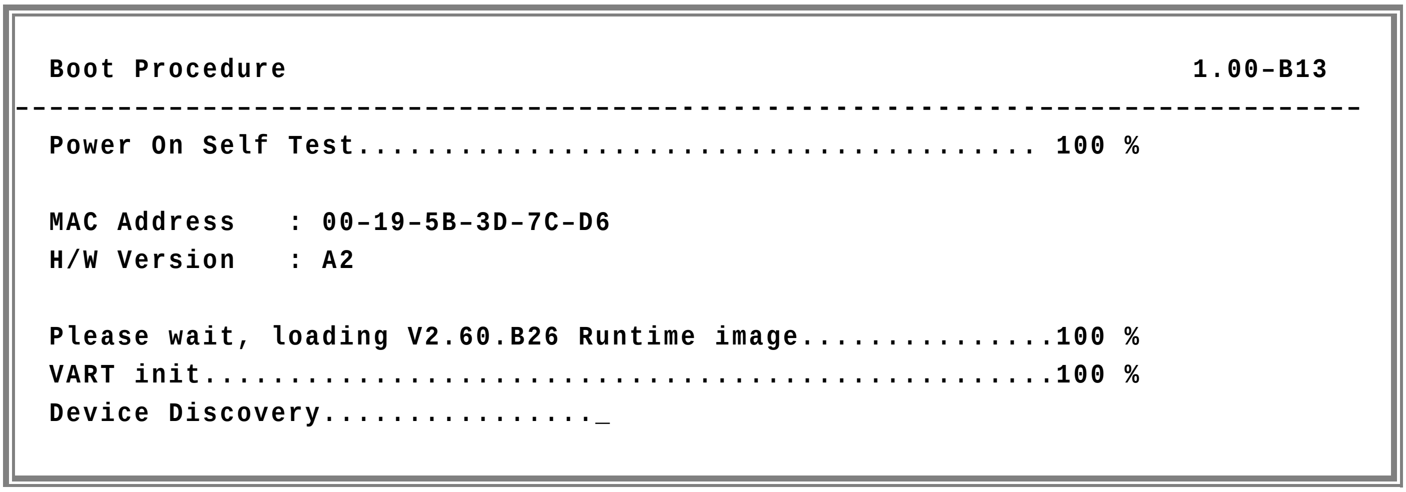
Figure 1–1. Initial CLI screen

There is no initial username or password. Just press the **Enter** key twice to display the CLI input cursor – **DGS–3426:5#**. 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                                                     1.00-B13
-------------------------------------------------------------------------------
  Power On Self Test....................................... 100 %

  MAC Address   : 00-19-5B-3D-7C-D6
  H/W Version   : A2

  Please wait, loading V2.60.B26 Runtime image...............100 %
  VART init..................................................100 %
  Device Discovery................_
```

Figure 1–2. Boot Screen

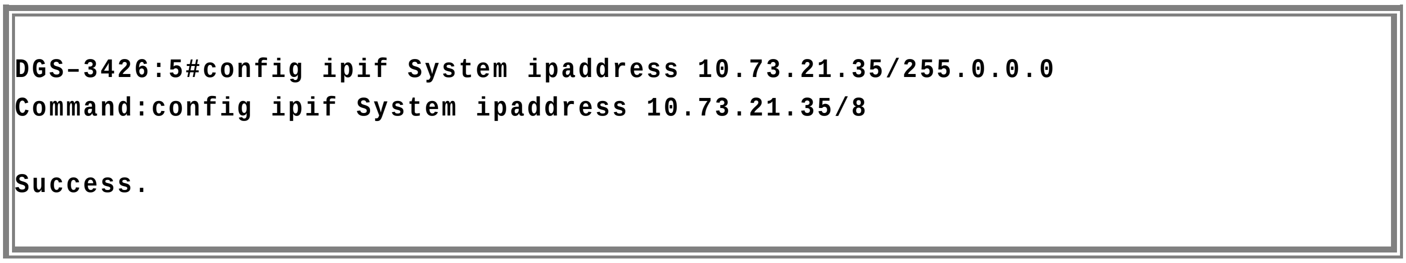
The Switch’s MAC address can also be found in the Web management program on the Switch Information (Basic Settings) window on the Configuration menu.

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-3426:5#config ipif System ipaddress 10.73.21.35/255.0.0.0
Command:config ipif System ipaddress 10.73.21.35/8

Success.
```

Figure 1–3. Assigning an IP Address

In the above example, the Switch was assigned an IP address of 10.73.21.35 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.

Note: The DGS–3400 series of switches have the capability to be configured for an IP address of 0.0.0.0, or, in essence, have no IP address. This function maybe used to disable Layer 3 functions of the Switch. When the IP address is set to 0.0.0.0 (invalid IP address), the Switch can only be managed through the console port or SIM. Other management applications such as Telnet, Web–based and SNMP cannot be used to manage the Switch when its IP address is 0.0.0.0.

2

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 an SNMP–based network management software over the network.

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

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

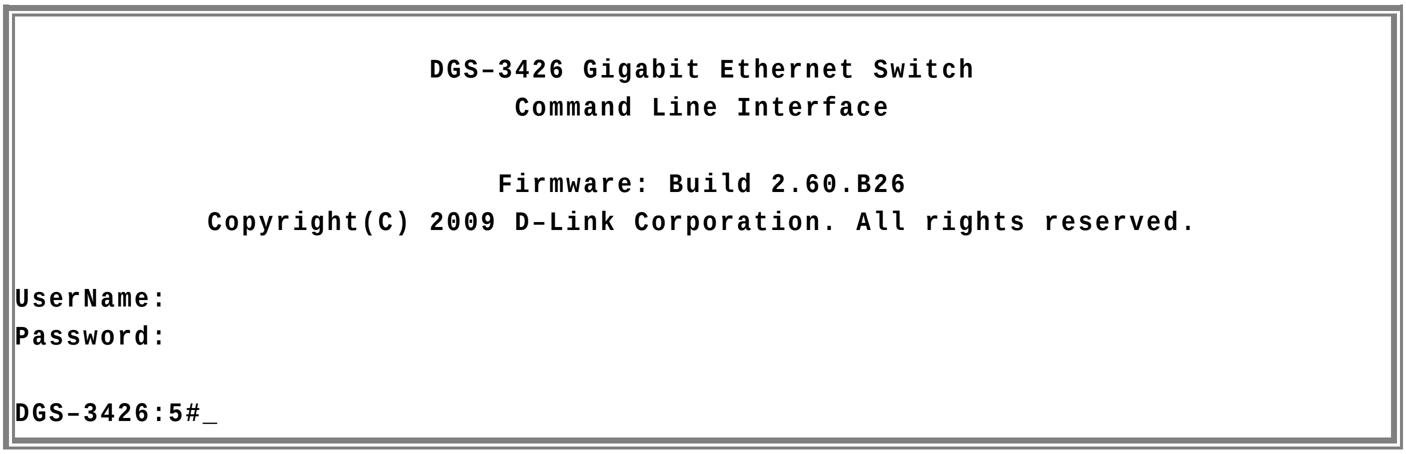
Connecting to the Switch

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

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

Users may also access the same functions over a Telnet interface. Once you have set an IP address for your Switch, you 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:

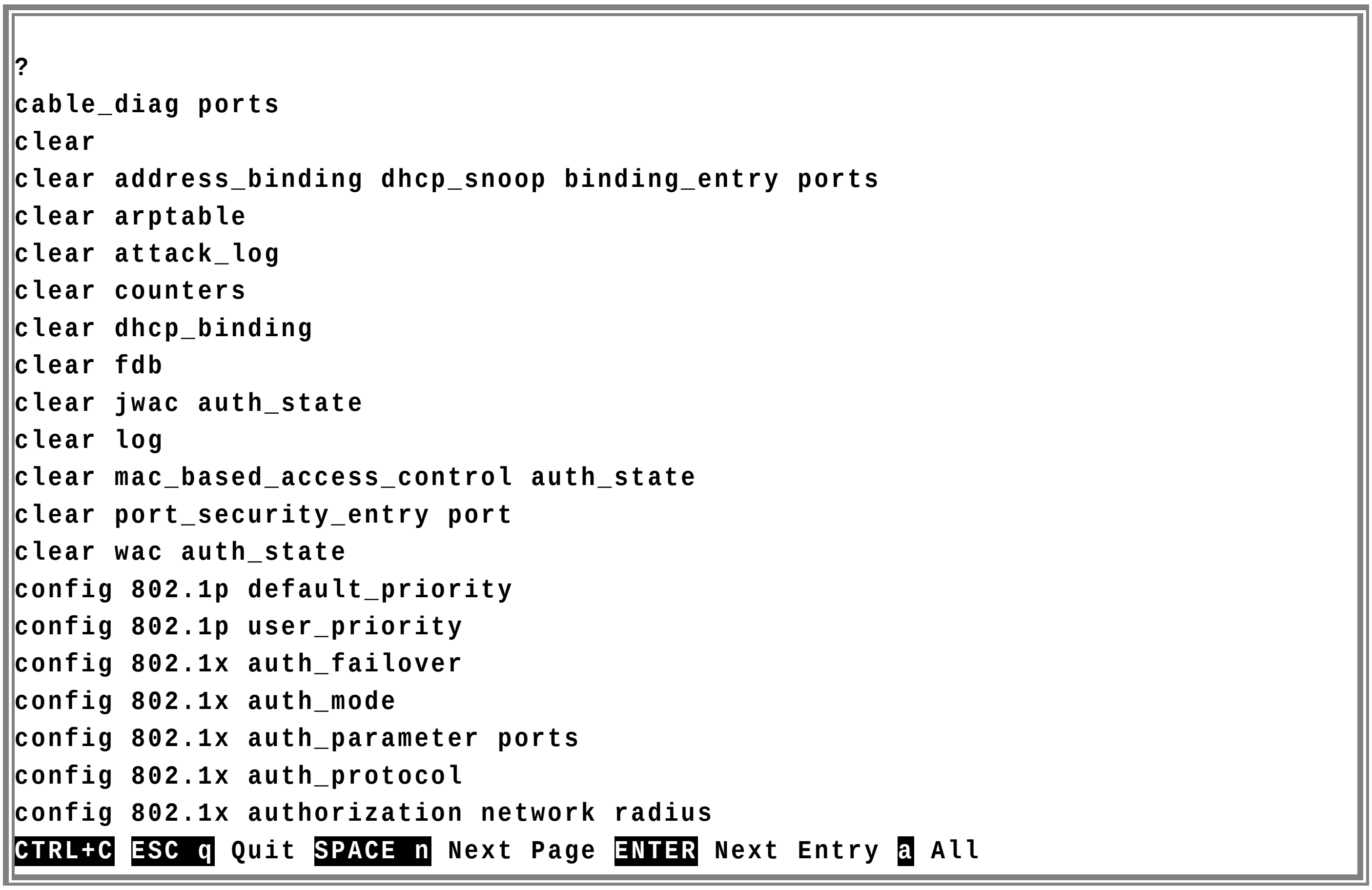


```
                         DGS-3426 Gigabit Ethernet Switch
                             Command Line Interface

                           Firmware: Build 2.60.B26
             Copyright(C) 2009 D-Link Corporation. All rights reserved.

UserName:
Password:

DGS-3426:5#_
```

Figure 2– 1. Initial Console Screen after logging in

Commands are entered at the command prompt, **DGS–3426:5#**.

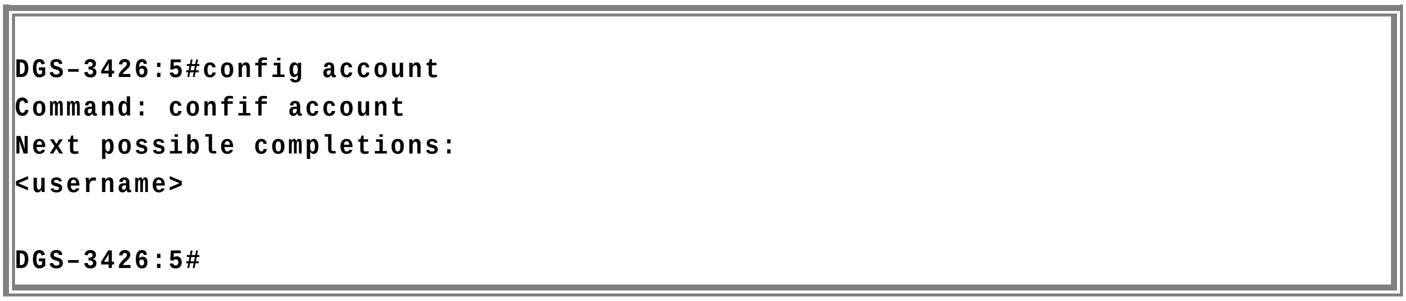
There are a number of helpful features included in the CLI. Entering the **?** command will display a list of all of the top–level commands.



```
?
cable_diag ports
clear
clear address_binding dhcp_snoop binding_entry ports
clear arptable
clear attack_log
clear counters
clear dhcp_binding
clear fdb
clear jwac auth_state
clear log
clear mac_based_access_control auth_state
clear port_security_entry port
clear wac auth_state
config 802.1p default_priority
config 802.1p user_priority
config 802.1x auth_failover
config 802.1x auth_mode
config 802.1x auth_parameter ports
config 802.1x auth_protocol
config 802.1x authorization network radius
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

Figure 2– 2. The ? Command

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



```
DGS-3426:5#config account
Command: confif account
Next possible completions:
<username>

DGS-3426:5#
```

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, users can see all of the next possible sub–commands, in sequential order, by repeatedly pressing the **Tab** key.

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

```
DGS-3426:5#config account
Command: confif account
Next possible completions:
<username>

DGS-3426:5#config account
Command: confif account
Next possible completions:
<username>

DGS-3426:5#
```

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

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

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

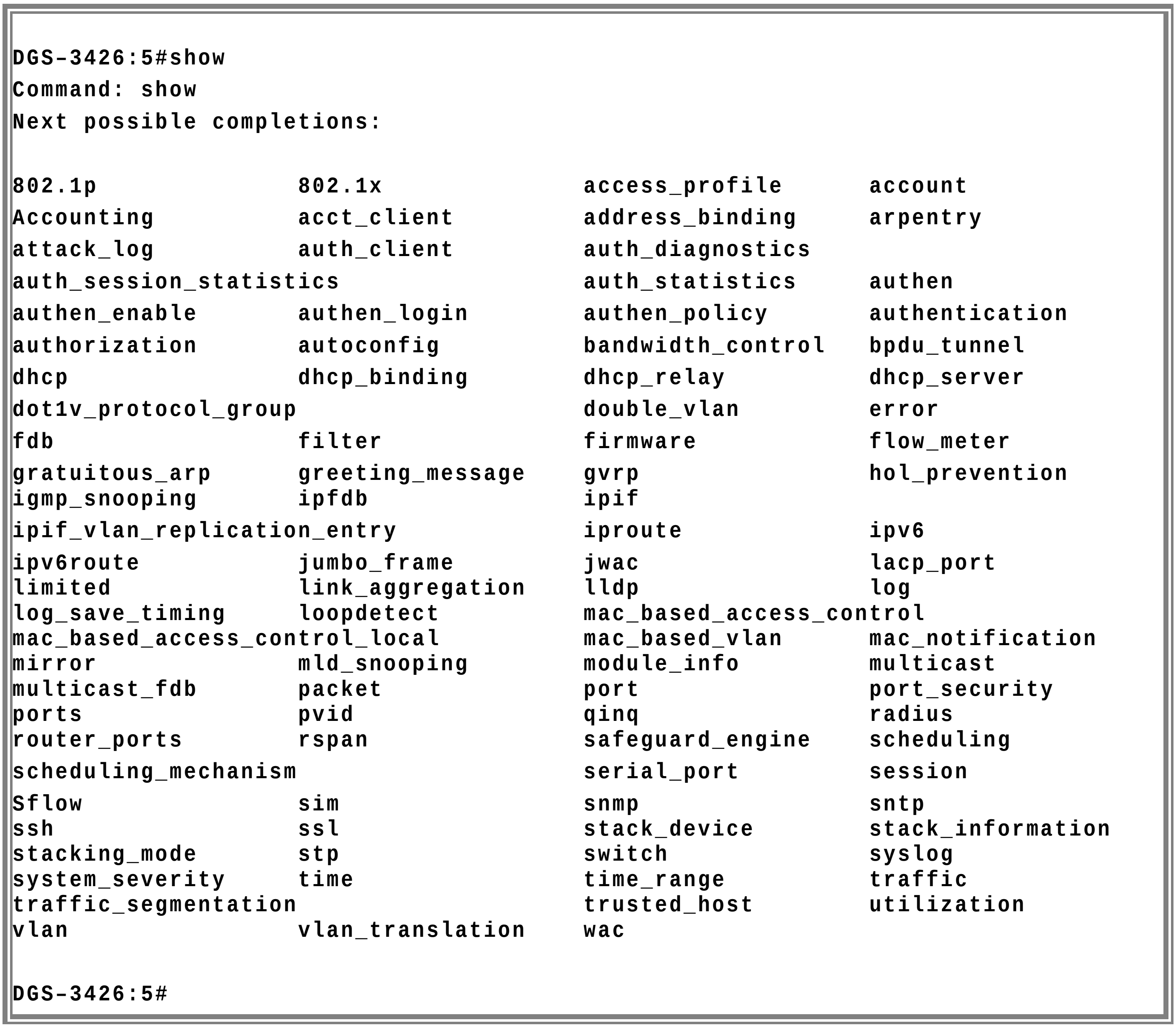
If a command is entered that is unrecognized by the CLI, the top–level commands will be displayed under the **Available commands:** prompt.

```
DGS-3426:5#the
Available commands:
..                  ?                   cable_diag        clear
config              create              debug             delete
disable             download            enable            login
logout              no                  ping              ping6
reboot              reconfig            reset             save
show                telnet              upload

DGS-3426:5#
```

Figure 2– 5. Available Commands

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

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



```
DGS-3426:5#show
Command: show
Next possible completions:

802.1p              802.1x              access_profile      account
Accounting          acct_client         address_binding     arpentry
attack_log          auth_client         auth_diagnostics
auth_session_statistics                 auth_statistics     authen
authen_enable       authen_login        authen_policy       authentication
authorization       autoconfig          bandwidth_control   bpdu_tunnel
dhcp                dhcp_binding        dhcp_relay          dhcp_server
dot1v_protocol_group                    double_vlan         error
fdb                 filter              firmware            flow_meter
gratuitous_arp      greeting_message    gvrp                hol_prevention
igmp_snooping       ipfdb               ipif
ipif_vlan_replication_entry             iproute             ipv6
ipv6route           jumbo_frame         jwac                lacp_port
limited             link_aggregation    lldp                log
log_save_timing     loopdetect          mac_based_access_control
mac_based_access_control_local          mac_based_vlan      mac_notification
mirror              mld_snooping        module_info         multicast
multicast_fdb       packet              port                port_security
ports               pvid                qinq                radius
router_ports        rspan               safeguard_engine    scheduling
scheduling_mechanism                    serial_port         session
Sflow               sim                 snmp                sntp
ssh                 ssl                 stack_device        stack_information
stacking_mode       stp                 switch              syslog
system_severity     time                time_range          traffic
traffic_segmentation                    trusted_host        utilization
vlan                vlan_translation    wac

DGS-3426:5#
```

Figure 2– 6. Next possible completions: Show Command

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

3

COMMAND SYNTAX

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

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

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

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

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

{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. Do not type the braces.
Example command	**reset config**

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

Line Editing Key Usage	
Delete	Deletes the character under the cursor and then shifts the remaining characters in the line to the left.
Backspace	Deletes the character to the left of the cursor and then shifts the remaining characters in the line to the left.
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.

4

BASIC SWITCH COMMANDS

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

Command	Parameters
create account	[admin | operator | user] <username 15>
config account	<username> {encrypt [plain_text| sha_1] <password>}
show account	
delete account	<username> {<string>}
enable password encryption	
disable password encryption	
show module_info	
show device_status	
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]} (1)
enable clipaging	
disable clipaging	
telnet	<ipaddr> {tcp_port <value 0-65535>}
enable telnet	<tcp_port_number 1-65535>
disable telnet	
enable web	<tcp_port_number 1-65535>
disable web	
save	{[config <config_id 1-2> | log | all]}
reboot	{<string>}
reset	{[config | system]} {<string>}
login	
logout	
create trusted_host	[<ipaddr> | network <network_address>]
delete trusted_host	[ipaddr <ipaddr> | network <network_address> | all]
show trusted_host	{<network_address>}

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

create account

Purpose	Used to create user accounts.
Syntax	**create account [admin | operator | user] <username 15>**
Description	This command is used to create user accounts that consist of a case sensitive username of 1 to 15 characters and a case sensitive password of 0 to 15 characters. Up to 8 user accounts can be created.
Parameters	[admin | operator | user] <username 15>
Restrictions	Only Administrator-level users can issue this command. Usernames can be between 1 and 15 characters. Passwords can be between 0 and 15 characters.

Example usage:

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

```
DGS-3426:5#create account admin dlink
Command: create account admin dlink

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

DGS-3426:5#
```

NOTICE: In case of lost passwords or password corruption, please refer to the Appendix B at the end of this manual, which will guide you through the steps necessary to resolve this issue.

config account

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

Example usage:

To configure the user password of “dlink” account:

```
DGS-3426:5#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-3426:5#
```

show account

Purpose	Used to display user accounts.
Syntax	**show account**
Description	This command 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-3426:5#show account
Command: show account

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

Total Entries: 1

DGS-3426:5#
```

delete account

Purpose	Used to delete an existing user account.
Syntax	**delete account <username> {<string>}**
Description	This command deletes an existing entry.
Parameters	*<username>* – Name of the user who will be deleted. *<string>* - yes | no
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete the user account “dgallinari”:

```
DES-3528:5#delete account dgallinari
Command: delete account dgallinari

Success.

DES-3528:5#
```

enable password encryption

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

Example usage:

To enable password encryption:

```
DGS-3426:5#enable password encryption
Command: enable password encryption

Success.


DGS-3426:5#
```

disable password encryption

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

Example usage:

To disable password encryption:

```
DGS-3426:5#disable password encryption
Command: disable password encryption

Success.


DGS-3426:5#
```

show module_info

Purpose	Used to display information about installed modules.
Syntax	**show module_info**
Description	Displays information about optional modules that may be installed on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display information about installed modules:

```
DGS-3426:5# show module_info
Command: show module_info

BOX  ID    Module Name   Rev.    Serial       Description
ID                                            No.
---  --  -------------  ----    ----------   -------------------------
1     1    DEM-410X          A0      PA5A5A5A5     1 Port XFP Module
1     2    DEM-410X          A0      PA5A5A5A5     1 Port XFP Module

DGS-3426:5#
```

show device_status

Purpose	Used to display current status of fans and power or power supplies on the system.
Syntax	**show device_status**
Description	This command displays the current status of power(s) and fan(s) on the system. There is a status display for all the fans on the Switch. If all fans are working normally, there will a corresponding "OK" in the Fan display field. If any fan fails there will be a corresponding fail message in the Fan display field, such as "1,3 Fail".
Parameters	None.
Restrictions	None.

Example usage:

To display status of fans and power supply:

```
DGS-3426P:5#show device_status
Command: show device_status

Unit  1:
    Internal Power: Active
    External Power: Fail
    Left Fan      : OK
    Right Fan     : OK
    Back Fan      : OK
    CPU Fan       : ---

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

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

Example usage:

To display the way that the users logged in:

```
DGS-3427:4#show session
Command: show session

 ID   Live Time     From        Level    Name
 ---  -----------  ---------    -----    ----------
 8  0:8:48.860    Serial Port    4       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-3426:5#show switch
Command: show switch

Device Type       : DGS-3426 Gigabit Ethernet Switch
MAC Address       : 00-01-02-03-04-05
IP Address        : 172.18.211.246 (Manual)
VLAN Name         : default
Subnet Mask       : 255.255.255.0
Default Gateway   : 0.0.0.0
Boot PROM Version : Build 1.00-B13
Firmware Version  : Build 2.60.B26
Hardware Version  : A2
System Name       :
System Location   :
System Contact    :
Spanning Tree     : Disabled
GVRP              : Disabled
IGMP Snooping     : Disabled
MLD Snooping      : Disabled
TELNET            : Enabled (TCP 23)
WEB               : Enabled (TCP 80)
SNMP              : Disabled
RMON              : Disabled
SSL status        : Disabled
SSH status        : Disabled
802.1x            : Disabled
Jumbo Frame       : Off
Clipaging         : Enabled
MAC Notification  : Disabled
Port Mirror       : Disabled
SNTP              : Disabled
HOL Prevention State : Enabled
Syslog Global State  : Disabled
Single IP Management : Disabled
Dual Image           : Supported
Password Encryption Status : Disabled

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

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-3427:4#show serial_port
Command: show serial_port

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

DGS-3427:4#
```

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

Example usage:

To configure baud rate:

```
DGS-3426:5#config serial_port baud_rate 115200
Command: config serial_port baud_rate 115200

Success.

DGS-3426:5#
```

enable clipaging

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

Example usage:

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

```
DGS-3426:5#enable clipaging
Command: enable clipaging

Success.

DGS-3426:5#
```

disable clipaging

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

Example usage:

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

```
DGS-3426:5#disable clipaging
Command: disable clipaging

Success.

DGS-3426:5#
```

telnet

Purpose	Specifies to instruct the Telnet client to connect to the specific Telnet server.
Syntax	**<ipaddr> {tcp_port <value 0-65535>}**
Description	This command will instruct the Telnet client to connect to the specific Telnet server. The parameters specified by the command will only be used for the establishment of this specific session. They will not affect other sessions.
Parameters	*ipaddr* – The IP address of the Telnet server. *tcp_port* – Specifies the Telnet server port number to be connected. If not specified, the default port is 23.
Restrictions	None.

Example usage:

To enable Telnet:

```
DGS-3426:5#telnet 172.18.211.252 23 linemode
Command: telnet 172.18.211.252 23 linemode

Success

DGS-3426:5#
```

enable telnet

Purpose	Used to enable communication with and management of the Switch using the Telnet protocol.
Syntax	**enable telnet <tcp_port_number 1–65535>**
Description	This command is used to enable the Telnet protocol on the Switch. The user can specify the TCP or UDP port number the Switch will use to listen for Telnet requests.
Parameters	*<tcp_port_number 1–65535>* – The TCP port number. TCP ports are numbered between 1 and 65535. The “well–known” TCP port for the Telnet protocol is 23.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable Telnet and configure the port number:

```
DGS-3426:5#enable telnet 23
Command: enable telnet 23

Success.

DGS-3426:5#
```

disable telnet

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

Example usage:

To disable the Telnet protocol on the Switch:

```
DGS-3426:5#disable telnet
Command: disable telnet

Success.

DGS-3426:5#
```

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.
Parameters	*<tcp_port_number 1–65535>* – The TCP port number. TCP ports are numbered between 1 and 65535. The “well–known” port for the Web–based management software is 80.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable HTTP and configure port number:

```
DGS-3426:5#enable web 80
Command: enable web 80

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

DGS-3426:5#
```

disable web

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

Example usage:

To disable HTTP:

```
DGS-3426:5#disable web
Command: disable web

Success.

DGS-3426:5#
```

save

Purpose	Used to save changes in the Switch’s configuration to non–volatile RAM.
Syntax	**save {[config <config_id 1–2> | log | all]}**
Description	This command is used to enter the current switch configuration into non–volatile RAM. The saved switch configuration will be loaded into the Switch’s memory each time the Switch is restarted.
Parameters	*config <config_id 1–2>* – Specify to save current settings to configuration file 1 or 2. *log* – Specify to save current Switch log to NV–RAM. *all* – Specify to save all configuration settings. If nothing is specified after “save”, the Switch will save all.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To save the Switch’s current configuration to non–volatile RAM:

```
DGS-3426:5#save
Command: save

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

DGS-3426:5#
```

reboot

Purpose	Used to restart the Switch.
Syntax	**reboot {<string>}**
Description	This command is used to restart the Switch.
Parameters	<*string*> – This parameter is used to perform the command without prompt if a user enters /*y* for yes or /*n* for no.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To restart the Switch:

```
DGS-3426:5#reboot
Command: reboot
Are you sure want to proceed with the system reboot? (y|n)
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	*config* – If the keyword 'config' is specified, all of the factory default settings are restored on the Switch including the IP address, user accounts, the switch history log and banner. The Switch will not save or reboot. *system* – If the keyword 'system' is specified all of the factory default settings are restored on the Switch. The Switch will save and reboot after the settings are changed to default. Rebooting will clear all entries in the Forwarding Data Base. If no parameter is specified, the Switch's current IP address, user accounts, the switch history log and banner are not changed. All other parameters are restored to the factory default settings. The Switch will not save or reboot. <*string*> - This parameter is used to perform the command without prompt if a user enters /*y* for yes or /*n* for no.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

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

```
DGS-3426:5#reset config
Command: reset config

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

Success.

DGS-3426:5#
```

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–3426:5#login
Command: login

UserName:
```

create trusted_host

Purpose	Used to create the trusted host.
Syntax	**create trusted_host [<ipaddr> | network <network_address>]**
Description	This 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	*<ipaddr>* – The IP address of the trusted host to be created. *<network_address>* – The network address of the trusted network. The form of network address is xxx.xxx.xxx.xxx/y.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create a trusted host:

```
DGS-3426:5#create trusted_host network 10.23.23.23/8
Command: create trusted_host network 10.23.23.23/8

Success.

DGS-3426:5#
```

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>* – The network address of the trusted host to be viewed.
Restrictions	None.

Example usage:

To display the list of trusted hosts:

```
DGS-3426:5#show trusted_host
Command: show trusted_host

Management Stations

IP Address
---------------
10.0.0.0/8

Total Entries: 1

DGS-3426:5#
```

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 <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	*<ipaddr>* – The IP address of the trusted host. *<network_address>* – The network address of the trusted network. <all> – Delete all trusted hosts.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete a trusted host with an IP address 10.48.74.121:

```
DGS-3426:5#delete trusted_host ipaddr 10.48.74.121
Command: delete trusted_host 10.48.74.121

Success.

DGS-3426:5#
```

logout

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

Example usage:

To terminate the current user’s console session:

```
DGS-3426:5#logout
```

5

SWITCH PORT COMMANDS

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

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

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 {capability_advertised {10_half | 10_full | 100_half | 100_full | 1000_full} (1) } | 10_half | 10_full | 100_half | 100_full | 1000_full { [master | slave] }] | auto_negotiation restart_an | flow_control [enable | disable] | learning [enable | disable] | state [enable | disable] | [description <desc 1-32> | clear_description]} (1)**
Description	This command allows for the configuration of the Switch's Ethernet ports. Only the ports listed in the *<portlist>* will be affected.
Parameters	*all* – Configure all ports on the Switch. *<portlist>* – Specifies a port or range of ports to be configured. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3–2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. Non–contiguous portlist entries are separated by a comma. (ex: 1:1–1:3,1:7–1:9) *medium_type [fiber | copper]* – This applies only to the Combo ports. If configuring the Combo ports this defines the type of transport medium used. *speed* – Allows the user to adjust the speed for a port or range of ports. The user has a choice of the following: • *auto* – Enables auto–negotiation for the specified range of ports. • *capability advertised* – Configures the capability that advertises to the link partner to determine the fastest available auto setting. • *[10 | 100 | 1000]* – Configures the speed in Mbps for the specified range of ports. Gigabit ports are statically set to 1000 and cannot be set to slower speeds. • *[half | full]* – Configures the specified range of ports as either full–duplex or half–duplex. • *[master | slave]* – 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 form 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.

config ports

	auto_negotiation restart_an - Restart the auto-negotiation process. *flow_control [enable* | *disable]* – Enable or disable flow control for the specified ports. *learning [enable* | *disable]* – Enables or disables the MAC address learning on the specified range of ports. *state [enable* | *disable]* – Enables or disables the specified range of ports. *description <desc 32>* – Enter an alphanumeric string of no more than 32 characters to describe a selected port interface. *clear_description* – Enter this command to clear the port description of the selected port(s).
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

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

```
DGS-3426P:5#config  ports  1:1-1:3  speed  10_full  learning  enable  flow_control
enable
Command: config ports 1:1-1:3 speed 10_full learning enable flow_control enable

Success.

DGS-3426P:5#
```

show ports

Purpose	Used to display the current configuration of a range of ports.
Syntax	**show ports {<portlist>} { [description | err_disabled |auto_negotiation |details | media_type] }**
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 port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3–2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. Non–contiguous portlist entries are separated by a comma. (ex: 1:1–1:3,1:7–1:9) *description* – Adding this parameter to the **show ports** command indicates that a previously entered port description will be included in the display. *err_disabled* – Use this to list disabled ports including connection status and reason for being disabled. *auto_negotiation* – Indicate if port auto negotiation information will be included in the display. *details* – Indicates if port detail information will be included in the display. *media_type* – Specifies to display the port transceiver type.
Restrictions	None.

Example usage:

To display the configuration of all ports on the switch:

```
DGS-3426:5#show ports
Command: show ports

Port      Port            Settings             Connection           Address
           State     Speed/Duplex/FlowCtrl  Speed/Duplex/FlowCtrl   Learning
 -------  --------  ---------------------  ----------------------  ---------
 1:1      Enabled   Auto/Disabled           Link Down               Enabled
 1:2      Enabled   Auto/Disabled           Link Down               Enabled
 1:3      Enabled   Auto/Disabled           Link Down               Enabled
 1:4      Enabled   Auto/Disabled           Link Down               Enabled
 1:5      Enabled   Auto/Disabled           Link Down               Enabled
 1:6      Enabled   Auto/Disabled           Link Down               Enabled
 1:7      Enabled   Auto/Disabled           1000M/Full/None         Enabled
 1:8      Enabled   Auto/Disabled           Link Down               Enabled
 1:9      Enabled   Auto/Disabled           Link Down               Enabled
 1:10     Enabled   Auto/Disabled           Link Down               Enabled
 1:11     Enabled   Auto/Disabled           Link Down               Enabled
 1:12     Enabled   Auto/Disabled           Link Down               Enabled
 1:13     Enabled   Auto/Disabled           Link Down               Enabled
 1:14     Enabled   Auto/Disabled           Link Down               Enabled
 1:15     Enabled   Auto/Disabled           100M/Full/None          Enabled
 1:16     Enabled   Auto/Disabled           Link Down               Enabled
 1:17     Enabled   Auto/Disabled           Link Down               Enabled
 1:18     Enabled   Auto/Disabled           Link Down               Enabled
 1:19     Enabled   Auto/Disabled           Link Down               Enabled

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

Example usage:

To display the description of all ports on switch one:

```
DGS-3426:5#show ports description
Command: show ports description

Port      Port            Settings             Connection          Address
           State     Speed/Duplex/FlowCtrl  Speed/Duplex/FlowCtrl   Learning
 -------  --------  ---------------------  ----------------------  ---------
 1:1      Enabled   Auto/Disabled           Link Down               Enabled
           Description:
 1:2      Enabled   Auto/Disabled           Link Down               Enabled
           Description:
 1:3      Enabled   Auto/Disabled           Link Down               Enabled
           Description:
 1:4      Enabled   Auto/Disabled           Link Down               Enabled
           Description:
 1:5      Enabled   Auto/Disabled           Link Down               Enabled
           Description:
 1:6      Enabled   Auto/Disabled           Link Down               Enabled
           Description:
 1:7      Enabled   Auto/Disabled           1000M/Full/None         Enabled
           Description:
 1:8      Enabled   Auto/Disabled           Link Down               Enabled
           Description:
 1:9      Enabled   Auto/Disabled           Link Down               Enabled
           Description:


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

6

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]} (1)
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]} (1)**
Description	This command allows for the configuration of the port security feature. Only the ports listed in the *<portlist>* are affected.
Parameters	*portlist* – Specifies a port or range of ports to be configured. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3–2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. Non–contiguous portlist entries are separated by a comma. (ex: 1:1–1:3,1:7–1:9) *all* – Configure port security for all ports on the Switch. *admin_state [enable* | *disable]* – Enable or disable port security for the listed ports. *max_learning_addr <max_lock_no 0–16>* – Use this to limit the number of MAC addresses dynamically learned in the FDB for the ports. *lock_address_mode [Permanent* | *DeleteOnTimeout* | *DeleteOnReset]* – Indicates the method of locking addresses. The user has three choices: ▪ *Permanent* – The locked addresses will not age out after the aging timer expires or the switch restarts. ▪ *DeleteOnTimeout* – The locked addresses will age out after the aging timer expires. ▪ *DeleteOnReset* – The locked addresses will not age out until the Switch has been reset or restarted.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure port security:

```
DGS-3426:5#config port_security ports 1:1-1:5 admin_state enable
max_learning_addr 5 lock_address_mode DeleteOnReset
Command: config port_security ports 1:1-1:5 admin_state enable max_learning_addr
5 lock_address_mode DeleteOnReset

Success.

DGS-3426:5#
```

delete port_security_entry

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. This command will only take effect if the lock address mode set using the **config port_security ports** command is set as permanent or delete on reset.
Parameters	*vlan name <vlan_name 32>* – Enter the corresponding VLAN name of the port to delete. *port <port>* – Enter the port number which has learned the previously entered MAC address. The port is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. *mac_address <macaddr>* – Enter the corresponding MAC address, previously learned by the port, to delete.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete a port security entry:

```
DGS-3426:5#delete port_security_entry vlan_name default port 1:6 mac_address
00-01-30-10-2C-C7
Command: delete port_security_entry vlan_name default port 1:6 mac_address 00-
01-30-10-2C-C7

Success.

DGS-3426:5#
```

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. This command will only take effect if the lock address mode set using the **config port_security ports** command is set as permanent or delete on reset.
Parameters	*<portlist>* – Specifies a port or port range to clear. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3–2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. Non–contiguous portlist entries are separated by a comma. (ex: 1:1–1:3,1:7–1:9)
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To clear a port security entry by port:

```
DGS-3426:5# clear port_security_entry port 1:6
Command: clear port_security_entry port 1:6

Success.

DGS-3426:5#
```

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 port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3–2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. Non–contiguous portlist entries are separated by a comma. (ex: 1:1–1:3,1:7–1:9)
Restrictions	None.

Example usage:

To display the port security configuration:

```
DGS-3426:5#show port_security ports 1:1-1:5
Command: show port_security ports 1:1-1:5

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

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

7

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	
show stack_device	

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	*current_box_id <value 1–12>* – Identifies the Switch being configured. Range is 1–12. *priority <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 and Operator-level users can issue this command.

Usage example:

To configure box priority:

```
DGS-3426:5#config box_priority current_box_id 1 priority 1
Command: config box_priority current_box_id 1 priority 1

Success.

DGS-3426:5#
```

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	*current_box_id* – Identifies the Switch being configured. Range is 1–12. *new_box_id* – The new ID being assigned to the Switch (box). Range is 1–12. • *auto* – Allows the box ID to be assigned automatically.
Restrictions	Only Administrator and Operator-level users can issue this command.

Usage example:

To change a box ID:

```
DGS-3426:5#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-3426:5#
```

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-3426:5#show stack_information
Command: show stack_information

Topology      :Duplex_Chain
My Box ID     :1
Master ID     :1
BK Master ID  :1
Box Count     :1


 Box User                    Prio-                    Prom     Runtime   H/W
 ID  Set  Type         Exist rity        MAC         Version  Version  Version
 --- ---- ------------ ----- ---- ------------------ -------- -------- --------
   1 AUTO DGS-3426     Exist 32   00-19-5B-3D-7C-D6  1.00-B13 2.60-B26 A2
   2    - Not_Exist    No
   3    - Not_Exist    No
   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
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

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	*enable* | *disable* – 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. *<string>* – This parameter is used to perform the command without prompt if a user enters */y* for yes or */n* for no.
Restrictions	Only Administrator-level and Operator-level users can issue this command.

NOTE: Only ports 26 and 27 of the DGS–3427 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-3426:5#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	None.

Usage example:

To view the current stacking mode:

```
DGS-3426:5#show stacking mode
Command: show stacking mode

Stacking mode : Enabled

DGS-3426:5#
```

show stack_device

Purpose	Used to display the information for stacking devices.
Syntax	**show stack_device**
Description	This command will display stack device information.
Parameters	None.
Restrictions	None.

Usage example:

To display the stacking devices:

```
DGS–3426:5#show stack_device
Command: show stack_device

Box ID  Box Type      H/W Version  Serial Number
------  ------------  -----------  --------------------
2       DGS-3426      2A1G         avc

DGS–3426:5#
```

8

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 xStack® DGS–3400 Series supports the Simple Network Management Protocol (SNMP) versions 1, 2c, and 3. Users may 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

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	<username 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	<username 32>
show snmp user	
create snmp view	<view_name 32> <oid> view_type [included | excluded]
delete snmp view	<view_name 32> [all | oid]
show snmp view	<view_name 32>
create snmp community	<community_string 32> view <view_name 32> [read_only | read_write]
delete snmp community	<community_string 32>
show snmp community	<community_string 32>
config snmp engineID	<snmp_engineID 10–64>
show snmp engineID	
create snmp group	<groupname 32> {v1 | v2c | v3 [noauth_nopriv | auth_nopriv | auth_priv]} {read_view <view_name 32> | write_view <view_name 32> | notify_view <view_name 32>} (1)

Command	Parameters
delete snmp group	<groupname 32>
show snmp groups	
create snmp	[host <ipaddr> | v6host <ipv6addr>] [v1 | v2c | v3 [noauth_nopriv | auth_nopriv | auth_priv]] <auth_string 32>
delete snmp	[host <ipaddr> | v6host <ipv6addr>]
show snmp host	{<ipaddr>}
show snmp v6host	{<ipv6addr>}
enable snmp traps	
enable snmp authenticate traps	
show snmp traps	{ linkchange_traps { ports <portlist>}}
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 the SNMP function on the Switch.
Syntax	**enable snmp**
Description	This command is used to enable Simple Network Management Protocol (SNMP) on the Switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable SNMP:

```
DGS-3426:5#enable snmp
Command: enable snmp

Success.


DGS-3426:5#
```

disable snmp

Purpose	Used to disable SNMP on the Switch.
Syntax	**disable snmp**
Description	This command is used to disable the Simple Network Management Protocol (SNMP) on the Switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable SNMP:

```
DGS-3426:5#disable snmp
Command: disable snmp

Success.


DGS-3426:5#
```

enable snmp linkchange_traps

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

Example usage:

To enable SNMP linkchange traps:

```
DGS-3426:5#enable snmp linkchange_traps
Command: enable snmp linkchange_traps

Success.

DGS-3426:5#
```

disable snmp linkchange_traps

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

Example usage:

To disable SNMP linkchange traps:

```
DGS-3426:5#disable snmp linkchange_traps
Command: disable snmp linkchange_traps

Success.

DGS-3426:5#
```

config snmp linkchange_traps	
Purpose	Used to configure SNMP linkchange 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	*all* – Configure all ports on the Switch. *<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). *enable* | *disable* – Used to enable or disable SMMP linkchange traps for the switch.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure SNMP linkchange traps on every port:

```
DGS-3426:5#config snmp linkchange_traps ports all enable
Command: config snmp linkchange_traps ports all enable

Success.

DGS-3426:5#
```

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

Example usage:

To create an SNMP user on the Switch:

```
DGS-3426:5#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-3426:5#
```

delete snmp user

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

Example usage:

To delete a previously entered SNMP user on the Switch:

```
DGS-3426:5#delete snmp user dlink
Command: delete snmp user dlink

Success.

DGS-3426:5#
```

show snmp user

Purpose	Used to display information about each SNMP username in the SNMP username table.
Syntax	**show snmp user**
Description	This command is used to display information about each SNMP username in the SNMP username table.
Parameters	None.
Restrictions	None.

Example usage:

To display the SNMP users currently configured on the Switch:

```
DGS-3426:5#show snmp user
Command: show snmp user

Username                  Group Name                 VerAuthPriv
------------------------- -------------------------- -----------
u3                           g3                        V3 NoneNone
initial                      initial                   V3 NoneNone

Total Entries: 2

DGS-3426:5#
```

create snmp view

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

Example usage:

To create an SNMP view:

```
DGS-3426:5#create snmp view dlinkview 1.3.6 view_type included
Command: create snmp view dlinkview 1.3.6 view_type included

Success.

DGS-3426:5#
```

delete snmp view

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

Example usage:

To delete a previously configured SNMP view from the Switch:

```
DGS-3426:5#delete snmp view dlinkview all
Command: delete snmp view dlinkview all

Success.

DGS-3426:5#
```

show snmp view

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

Example usage:

To display SNMP view configuration:

```
UserName:
PassWord:

DGS-3426P:4#show snmp view
Command: show snmp view

Vacm View Table Settings
View Name                  Subtree                     View Type

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

v3v                        1                             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: 9

DGS-3426P:4#
```

create snmp community

Purpose	Used to create an SNMP community string to define the relationship between the SNMP manager and an agent. The community string acts like a password to permit access to the agent on the Switch. One or more of the following characteristics can be associated with the community string: An Access List of IP addresses of SNMP managers that are permitted to use the community string to gain access to the Switch's SNMP agent. An MIB view that defines the subset of all MIB objects that will be accessible to the SNMP community. *read_write* or *read_only* level permission for the MIB objects accessible to the SNMP community.
Syntax	**create snmp community <community_string 32> view <view_name 32> [read_only | read_write]**
Description	This command is used to create an SNMP community string and to assign access–limiting characteristics to this community string.
Parameters	*<community_string 32>* – An alphanumeric string of up to 32 characters that is used to identify members of an SNMP community. This string is used like a password to give remote SNMP managers access to MIB objects in the Switch's SNMP agent. <*view_name 32*> – An alphanumeric string of up to 32 characters that is used to identify the group of MIB objects that a remote SNMP manager is allowed to access on the Switch. *read_only* – Specifies that SNMP community members using the community string created with this command can only read the contents of the MIBs on the Switch. *read_write* – Specifies that SNMP community members using the community string created with this command can read from and write to the contents of the MIBs on the Switch.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create the SNMP community string "dlink:"

```
DGS-3426:5#create snmp community dlink view ReadView read_write
Command: create snmp community dlink view ReadView read_write

Success.


DGS-3426:5#
```

delete snmp community

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

Example usage:

To delete the SNMP community string "dlink:"

```
DGS-3426:5#delete snmp community dlink
Command: delete snmp community dlink

Success.

DGS-3426:5#
```

show snmp community

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

Example usage:

To display the currently entered SNMP community strings:

```
DGS-3426P:4#show snmp community
Command: show snmp community

SNMP Community Table
Community Name       View Name         Access Right

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

private              CommunityView      read_write
public               CommunityView      read_only

Total Entries: 2

DGS-3426P:4#
```

config snmp engineID

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

Example usage:

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

```
DGS-3426:5#config snmp engineID 0035636666
Command: config snmp engineID 0035636666

Success.

DGS-3426:5#
```

show snmp engineID

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

Example usage:

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

```
DGS-3426:5#show snmp engineID
Command: show snmp engineID

SNMP Engine ID : 0035636666

DGS-3426:5#
```

create snmp group

Purpose	Used to create a new SNMP group, or a table that maps SNMP users to SNMP views.
Syntax	**create snmp group <groupname 32> [v1 | v2c | v3 [noauth_nopriv | auth_nopriv | auth_priv]] {read_view <view_name 32> | write_view <view_name 32> | notify_view <view_name 32>} (1)**
Description	This command 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 the SNMP group the new SNMP user will be associated with. *v1* – Specifies that SNMP version 1 will be used. The Simple Network Management Protocol (SNMP), version 1, is a network management protocol that provides a means to monitor and control network devices. *v2c* – Specifies that SNMP version 2c will be used. The SNMP v2c supports both centralized and distributed network management strategies. It includes improvements in the Structure of Management Information (SMI) and adds some security features. *v3* – Specifies that the SNMP version 3 will be used. SNMP v3 provides secure access to devices through a combination of authentication and encrypting packets over the network. SNMP v3 adds: • Message integrity – Ensures that packets have not been tampered with during transit. • Authentication – Determines if an SNMP message is from a valid source. • Encryption – Scrambles the contents of messages to prevent it being viewed by an unauthorized source. *noauth_nopriv* – Specifies that there will be no authorization and no encryption of packets sent between the Switch and a remote SNMP manager. *auth_nopriv* – Specifies that authorization will be required, but there will be no encryption of packets sent between the Switch and a remote SNMP manager. *auth_priv* – Specifies that authorization will be required, and that packets sent between the Switch and a remote SNMP manger will be encrypted. *read_view* – Specifies that the SNMP group being created can request SNMP messages. *write_view* – Specifies that the SNMP group being created has write privileges. *notify_view* – Specifies that the SNMP group being created can receive SNMP trap messages generated by the Switch's SNMP agent. *<view_name 32>* – An alphanumeric string of up to 32 characters that is used to identify the group of MIB objects that a remote SNMP manager is allowed to access on the Switch.

create snmp group

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

Example usage:

To create an SNMP group named “sg1:”

```
DGS-3426:5#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-3426:5#
```

delete snmp group

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

Example usage:

To delete the SNMP group named “sg1”.

```
DGS-3426:5#delete snmp group sg1
Command: delete snmp group sg1

Success.

DGS-3426:5#
```

show snmp groups

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

Example usage:

To display the currently configured SNMP groups on the Switch:

```
DGS-3426:5#show snmp groups
Command: show snmp groups
Vacm Access       Table Settings

Group    Name          : initial
ReadView Name          : restricted
WriteView Name         :
```

```
Notify View Name       : restricted
Security Model         : SNMPv3
Security Level         : NoAuthNoPriv

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

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

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

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

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

Group    Name           : ReadGroup
ReadView Name           : CommunityView
WriteView Name          :
Notify View Name        : CommunityView
Security Model          : 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: 9

DGS-3426:5#
```

create snmp host

Purpose	Used to create a recipient of SNMP traps generated by the Switch’s SNMP agent.
Syntax	**create snmp [host <ipaddr> | v6host <ipv6addr>] [v1 | v2c | v3 [noauth_nopriv | auth_nopriv | auth_priv] <auth_string 32>]**
Description	This command creates a recipient of SNMP traps generated by the Switch’s SNMP agent.
Parameters	*host <ipaddr>* – The IPv4 address of the remote management station that will serve as the SNMP host for the Switch. *v6host <ipv6addr>* – The IPv6 address of the remote management station that will serve as the SNMP host for the Switch. *v1* – Specifies that SNMP version 1 will be used. The Simple Network Management Protocol (SNMP), version 1, is a network management protocol that provides a means to monitor and control network devices. *v2c* – Specifies that SNMP version 2c will be used. The SNMP v2c supports both centralized and distributed network management strategies. It includes improvements in the Structure of Management Information (SMI) and adds some security features. *v3* – Specifies that the SNMP version 3 will be used. SNMP v3 provides secure access to devices through a combination of authentication and encrypting packets over the network. SNMP v3 adds: • Message integrity – ensures that packets have not been tampered with during transit. • Authentication – determines if an SNMP message is from a valid source. • Encryption – scrambles the contents of messages to prevent it being viewed by an unauthorized source. *noauth_nopriv* – Specifies that there will be no authorization and no encryption of packets sent between the Switch and a remote SNMP manager. *auth_nopriv* – Specifies that authorization will be required, but there will be no encryption of packets sent between the Switch and a remote SNMP manager. *auth_priv* – Specifies that authorization will be required, and that packets sent between the Switch and a remote SNMP manger will be encrypted. *<auth_sting 32>* – An alphanumeric string used to authorize a remote SNMP manager to access the Switch’s SNMP agent.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create an SNMP IPv4 host to receive SNMP messages:

```
DGS-3426:5#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-3426:5#
```

To create an SNMP IPv6 host to receive SNMP messages:

```
DGS-3426:5#create snmp v6host FF::FF v3 noauth_nopriv initial
Command: create snmp v6host FF::FF v3 noauth_nopriv initial

Success.

DGS-3426:5#
```

delete snmp host

Purpose	Used to remove a recipient of SNMP traps generated by the Switch's SNMP agent.
Syntax	**delete snmp [host <ipaddr> | v6host <ipv6addr>]**
Description	This command is used to delete a recipient of SNMP traps generated by the Switch's SNMP agent.
Parameters	*host <ipaddr>* – The IPv4 address of the remote management station that will serve as the SNMP host for the Switch. *v6host <ipv6addr>* – The IPv6 address of the remote management station that will serve as the SNMP host for the Switch.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete an IPv4 SNMP host entry:

```
DGS-3426:5#delete snmp host 10.48.74.100
Command: delete snmp host 10.48.74.100

Success.

DGS-3426:5#
```

To delete an IPv6 SNMP host entry:

```
DGS-3426:5#delete snmp v6host FF::FF
Command: delete snmp v6host FF::FF

Success.

DGS-3426:5#
```

show snmp host

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

Example usage:

To display the currently configured SNMP hosts on the Switch:

```
DGS-3426:5#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-3426:5#
```

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	This 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	*v6host <ipv6addr>* – The IPv6 address of a remote SNMP manager that will receive SNMP traps generated by the Switch's SNMP agent.
Restrictions	None.

Example usage:

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

```
DGS-3426:5#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-3426:5#
```

enable snmp traps

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

Example usage:

To enable SNMP trap support on the Switch:

```
DGS-3426:5#enable snmp traps
Command: enable snmp traps

Success.

DGS-3426:5#
```

enable snmp authenticate traps

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

Example usage:

To turn on SNMP authentication trap support:

```
DGS-3426:5#enable snmp authenticate traps
Command: enable snmp authenticate traps

Success.

DGS-3426:5#
```

show snmp traps

Purpose	Used to show SNMP trap support on the Switch .
Syntax	**show snmp traps { linkchange_traps { ports <portlist>} }**
Description	This command is used to view the SNMP trap support status currently configured on the Switch.
Parameters	*portlist* – Enter a list of ports to be displayed.
Restrictions	None.

Example usage:

To view the current SNMP trap support:

```
DGS-3426:5#show snmp traps linkchange_traps ports 1
Command: show snmp traps linkchange_traps ports 1:1

Linkchange Trap  :   Enabled
       Port 1:1  :   Enabled

DGS-3426:5#
```

disable snmp traps

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

Example usage:

To prevent SNMP traps from being sent from the Switch:

```
DGS-3426:5#disable snmp traps
Command: disable snmp traps

Success.

DGS-3426:5#
```

disable snmp authenticate traps

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

Example usage:

To disable the SNMP authentication trap support:

```
DGS-3426:5#disable snmp authenticate traps
Command: disable snmp authenticate traps

Success.

DGS-3426:5#
```

config snmp system_contact

Purpose	Used to enter the name of a contact person who is responsible for the Switch.
Syntax	**config snmp system_contact <sw_contact>**
Description	This command is used to enter the name and/or other information to identify a contact person who is responsible for the Switch. A maximum of 255 character can be used.
Parameters	*<sw_contact>* – A maximum of 255 characters is allowed.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

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

```
DGS-3426:5#config snmp system_contact MIS Department II
Command: config snmp system_contact MIS Department II

Success.

DGS-3426:5#
```

config snmp system_location

Purpose	Used to enter a description of the location of the Switch.
Syntax	**config snmp system_location <sw_location>**
Description	This command is used to enter a description of the location of the Switch. A maximum of 255 characters can be used.
Parameters	*<sw_location>* – A maximum of 255 characters is allowed.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

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

```
DGS-3426:5#config snmp system_location HQ 5F
Command: config snmp system_location HQ 5F

Success.

DGS-3426:5#
```

config snmp system_name

Purpose	Used to configure the name for the Switch.
Syntax	**config snmp system_name <sw_name>**
Description	This command is used to configure the name of the Switch.
Parameters	*<sw_name>* – A maximum of 255 characters is allowed.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the Switch name for "DGS-3400 Switch":

```
DGS-3426:5#config snmp system_name DGS-3400 Switch
Command: config snmp system_name DGS-3400 Switch

Success.

DGS-3426:5#
```

enable rmon

Purpose	Used to enable RMON on the Switch.
Syntax	**enable rmon**
Description	This command is used to enable remote monitoring (RMON) on the Switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable RMON:

```
DGS-3426:5#enable rmon
Command: enable rmon

Success.

DGS-3426:5#
```

disable rmon	
Purpose	Used to disable RMON on the Switch.
Syntax	**disable rmon**
Description	This command is used to disable remote monitoring (RMON) on the Switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable RMON:

```
DGS-3426:5#disable rmon
Command: disable rmon

Success.

DGS-3426:5#
```

9

SWITCH UTILITY COMMANDS

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

Command	Parameters
download	[firmware_fromTFTP [<ipaddr> |<ipv6addr>] <path_filename 64> {image_id<int 1-2>} {unit [all|<unitid 1-12>]} | cfg_fromTFTP [<ipaddr> |<ipv6addr>] <path_filename 64> {[<config_id 1-2> | increment]}]
config firmware	{unit [<unitid_list 1-12>|all]} image_id <int 1-2> [delete|boot_up]
show firmware information	
config configuration	<config_id 1–2> [boot_up | delete | active]
show config	[current_config | config_in_nvram <config_id 1–2> | information]
upload	[cfg_toTFTP [<ipaddr> | <ipv6addr>] <path_filename 64> {<config_id 1–2>} | log_toTFTP [<ipaddr> | <ipv6addr>] <path_filename 64>] | attack_log_toTFTP [<ipaddr> | <ipv6addr>] <path_filename 64>] {unit <unit_id 1–12>}]
clear attack_log	{[unit <unit_id 1–12> | all]}
show attack_log	{unit <unit_id 1–12>} {index <value_list>}
enable autoconfig	
disable autoconfig	
show autoconfig	
ping	<ipaddr> {times <value 0–255>} {timeout <sec 1–99>}
ping6	<ipv6addr> {times <value 0–255> | size <value 1–6000> | timeout <value 1–10>}

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

download

Purpose	Used to download and install new firmware or a new configuration on the switch from a TFTP server.
Syntax	**download [firmware_fromTFTP [<ipaddr> |<ipv6addr>] <path_filename 64> {image_id<int 1-2>} {unit [all|<unitid 1-12>]} | cfg_fromTFTP [<ipaddr> |<ipv6addr>] <path_filename 64> {[<config_id 1-2> | increment]}]**
Description	This command is used to download a new firmware or a switch configuration file from a TFTP server. The firmware can be loaded to different images and units according to the image ID and unit ID,and you can choose to download through IPv6 if your switch supports IPv6. If the image id or the unit id does not exist in the system, the download will fail and give an error message.
Parameters	*firmware_fromTFTP* – Download and install new firmware on the Switch from a TFTP server. *cfg_fromTFTP* – Download and install a new configuration file on the Switch from a TFTP server. • *image_id* – Specifies the image index ID number of the firmware in the Switch’s memory. The Switch can store two firmware images for use. Image ID 1 will be the default boot up firmware for the Switch unless otherwise configured by the user. • *unit [all* | *<unitid 1–12>] – all* specifies all units (switches), *<unitid>* is the unit ID of the switch in the switch stack that will receive the download. This parameter is for downloading firmware only.

download	
	• *config* – Download a new configuration on the switch from a TFTP server. • *<ipaddr>* – The IPv4 address of the TFTP server. • *<ipv6addr>* – The IPv6 address of the TFTP server. • *<path_filename 64>* – The DOS path and filename of the firmware or switch configuration file on the TFTP server. For example, C:\dgs3427.had. • *config_id <int 1–2>* – The Switch can hold two configuration files specified by section ID. If no configuration ID is specified, the configuration being downloaded is applied to the system. If a configuration ID is specified, the configuration being downloaded is saved only to flash memory in the chosen section (1 or 2) and will not be applied to the system. Keep in mind that configuration ID 1 is the boot-up configuration unless this is changed using the config command. • *increment* – Allows the download of a partial switch configuration file. This allows a file to be downloaded that will change only the switch parameters explicitly stated in the configuration file. All other switch parameters will remain unchanged.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To download a configuration file:

```
DGS-3426:5#download cfg_fromTFTP 10.48.74.121 unit all c:\cfg\setting.txt
Command: download cfg_fromTFTP  10.48.74.121 unit all c:\cfg\setting.txt

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

DGS-3426:5#
DGS-3426:5##--------------------------------------------------------------
DGS-3426:5##            DGS-3426 Gigabit Ethernet Switch
DGS-3426:5##                        Configuration
DGS-3426:5##
DGS-3426:5##                     Firmware: Build 2.60.B26
DGS-3426:5##    Copyright(C) 2009 D-Link Corporation. All rights reserved.
DGS-3426:5##--------------------------------------------------------------
DGS-3426:5#
DGS-3426:5## STACK
DGS-3426:5#
DGS-3426:5#
DGS-3426:5## BASIC
DGS-3426:5#
DGS-3426:5#config serial_port auto_logout never
Command: config serial_port auto_logout never
```

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–3400” appears followed by the command prompt.

```
DGS-3426:5# # ROUTE
DGS-3426:5#
DGS-3426:5# create iproute default 172.18.212.253 1
Command: create iproute default 172.18.212.253 1

Success.

DGS-3426:5#
DGS-3426:5# #-------------------------------------------------------------
DGS-3426:5# #             End of configuration file for DGS-3426
DGS-3426:5# #-------------------------------------------------------------
DGS-3426:5# #
```

config configuration

Purpose	Used to designate a stored configuration file section ID as a boot up configuration, active configuration or to delete the configuration file.
Syntax	**config configuration <config_id 1–2> [boot_up | delete | active]**
Description	This command is used to configure the section ID index of a stored configuration as the boot up or active configuration, or to delete the contents of the specified configuration section.
Parameters	*config_id* – Specifies the section being configured or deleted. *delete* – Entering this parameter will delete the contents of the specified section. *boot_up* – Entering specifies the configuration section as a boot up section. *active* – Entering specifies the configuration section as an active section.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure configuration section 1 as a boot up section:

```
DGS-3426:5#config configuration 1 boot_up
Command: config configuration 1 boot_up

Success.

DGS-3426:5#
```

config firmware

Purpose	Used to configure the firmware section as a boot up section, or to delete the firmware section
Syntax	**config firmware {unit [<unitid_list 1-12>|all]} image_id <int 1-2> [delete|boot_up]**
Description	This command is used to configure the firmware section. The user may choose to remove the firmware section or use it as a boot up section.
Parameters	*unit <unit_id 1–12>* – Select the switch in the switch stack for which to configure the firmware image. *unitid_list*: Specifies the list of stacked units to apply the command to. This command is supported by projects which can set firmware on multiple units at a time. *all* : Specifies to select all units. *image_id* – Specifies the working section. The Switch can hold two firmware versions for the user to select from, which are specified by image ID. • *<int 1–2>* – Select the ID number of the firmware in the Switch’s memory to be configured. *delete* – Entering this parameter will delete the specified firmware section. *boot_up* – Entering this parameter will specify the firmware image ID as a boot up section.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure firmware section 1 as a boot up section:

```
DGS-3426:5#config firmware image_id 1 boot_up
Command: config firmware image_id 1 boot_up

Success.

DGS-3426:5#
```

show firmware information

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

Example usage:

To display the current firmware information on the Switch:

```
DGS-3426P:5#show firmware information
Command: show firmware information

 Box ID  Version   Size(B) Update Time         From                User
 --- --  --------- ------- ------------------- ------------------- -------------
 1   *1  2.60.B26  3763691 2009/03/05 10:23:40 10.73.21.1(R)

 1    2  (empty)

'*' means boot up firmware
(R) means firmware update through Serial Port(RS232)
(T) means firmware update through TELNET
(S) means firmware update through SNMP
(W) means firmware update through WEB
(SIM) means firmware update through Single IP Management

DGS-3426P:5#
```

show config	
Purpose	Used to display the current or saved version of the configuration settings of the switch.
Syntax	**show config [current_config | config_in_nvram <config_id 1–2> | information]**
Description	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). The configuration settings are listed by category in the following order: 1. Stack 2. Double VLAN 3. Basic (serial port, Telnet and web management status) 4. Account List 5. storm control 6. IP group management 7. syslog 8. QoS 9. port mirroring 10. traffic segmentation 11. SSL 12. port 13. PoE 14. Port lock 15. SNMPv3 16. MANAGEMENT 17. VLAN 18. 802.1X 19. Guest VLAN 20. TR 21. ACL 22. FDB (forwarding data base) 23. Address Binding 24. MAC Address Table Notification 25. STP 26. SAFEGUARD ENGINE 27. BANNER PROMPT 28. SSH 29. SNTP 30. LACP 31. IP and auto config 32. IGMP Snooping 33. MLD Snooping 34. ACCESS AUTHENTICATION CONTROL 35. DHCP Relay 36. IPv6 Neighbor Detection 37. ARP 38. Route
Parameters	*current_config* – Entering this parameter will display configurations entered without being saved to NVRAM. *config_in_nvram <config_id 1–2>* – Entering this parameter will display configurations to be specified *<config_id 1 –2>* which were saved in NV – RAM.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To view the current configuration settings:

```
DGS-3426:5#show config current_config
Command: show config current_config

#---------------------------------------------------------------------------
#                    DGS-3426 Gigabit Ethernet Switch
#                             Configuration
#
#                          Firmware: Build 2.60.B26
#        Copyright(C) 2009 D-Link Corporation. All rights reserved.
#-----------------------------------------------------------------------------


# STACK
##Box                                  Prio
##ID         Type           Exist      rity
##------     -------       ---------   -------
#  1           DGS-3426P     exist      16
#  2           DGS-3426      exist      32
#  3           DGS-3450      exist      32
#  4           Not_Exist       no
#  5           Not_Exist       no
#  6           Not_Exist       no
```

upload	
Purpose	Used to upload switch settings or the switch history log to a TFTP server.
Syntax	**upload [cfg_toTFTP [<ipaddr> | <ipv6addr>] <path_filename 64> {<config_id 1–2>} | log_toTFTP [<ipaddr> | <ipv6addr>] <path_filename 64>] | attack_log_toTFTP [<ipaddr> | <ipv6addr>] <path_filename 64>] {unit <unit_id 1–12>}]**
Description	This command is used to upload either the Switch's current settings or the Switch's history log to a TFTP server.
Parameters	*cfg_toTFTP* – Specifies that the Switch's current settings will be uploaded to the TFTP server. • *<ipaddr>* – The IPv4 address of the TFTP server. The TFTP server must be on the same IP subnet as the Switch. • *<ipv6addr>* – The IPv6 address of the TFTP server. The TFTP server must be on the same IP subnet as the Switch. • *<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. • *<config_id 1－2>* － Entering this parameter will upload configurations to be specified, which were saved in NV－RAM to TFTP server. *log_toTFTP* – Specifies that the switch history log will be uploaded to the TFTP server. • *<ipaddr>* – The IP address of the TFTP server. The TFTP server must be on the same IP subnet as the Switch. • *<ipv6addr>* – The IPv6 address of the TFTP server. The TFTP server must be on the same IP subnet as the Switch. • *<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. *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 and Operator-level users can issue this command.

Example usage:

To upload a configuration file:

```
DGS-3426:5#upload cfg_fromTFTP 10.48.74.121 c:\cfg\log.txt
Command: upload cfg_fromTFTP  10.48.74.121 c:\cfg\log.txt

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

DGS-3426:5#
```

Example usage:

To upload an attack log file:

```
DGS-3426:5#upload attack_log_toTFTP 10.53.13.23 c:\attacklog1 unit 1
Command: upload attack_log_toTFTP 10.53.13.23 c:\attacklog1 unit 1

Connecting to server................Done.
Upload attack log...................Done.

DGS-3426:5#
```

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	*unit <unit_id 1–12>* – Select the switch in the switch stack for which to view attack log files. *index <value list>* – This command will display the history log, beginning at 1 and ending at the value specified by the user in the *<value_list>* field. If no parameter is specified, all history log entries will be displayed.
Restrictions	None.

Example usage:

To display the attack log**:**

```
DGS-3426:5#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
1:23
1      2006-04-25  12:37:42  Possible spoofing attack from 000d010023001 port
1:23

DGS-3426:5#
```

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	*unit <unit_id 1–12>* – Select the switch in the switch stack for which to clear attack log files. *all* – Entering this parameter will clear all attack log files in the switch stack.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To clear the attack log for all switches in the switch stack**:**

```
DGS-3426:5#clear attack_log all
Command: clear attack_log all

Success.
```

```
DGS-3426:5#
```

enable autoconfig

Purpose	Used to activate the auto-configuration function for the Switch. This will load a configuration from the TFTP server specified in the reply.
Syntax	**enable autoconfig**
Description	When autoconfiguration 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	Only Administrator and Operator-level users can issue this command.

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

Example usage:

To enable auto-configuration on the Switch:

```
DGS-3426:5#enable autoconfig
Command: enable autoconfig

Success.

DGS-3426:5#
```

When auto-configuration 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 config** command. After the entire Switch configuration is loaded, the Switch will automatically "logout" the server.

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-3426 Gigabit Ethernet Switch
                             Command Line Interface

                            Firmware: Build 2.60.B26
              Copyright(C) 2009 D-Link Corporation. All rights reserved.

DGS-3426:5#
DGS-3426:5#
DGS-3426:5#download config 10.41.44.44 c:\cfg\setting.txt
Command: download config 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-3426:5# create iproute default 172.18.212.253 1
Command: create iproute default 172.18.212.253 1

Success.

DGS-3426:5#
DGS-3426:5##----------------------------------------------------
DGS-3426:5##        End of configuration file for DGS-3426
DGS-3426:5#

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

NOTE: With auto-configuration 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 auto-configuration from DHCP.
Syntax	**disable autoconfig**
Description	This instructs the Switch not to accept auto-configuration instruction from the DHCP server. This does not change the IP settings of the Switch. The IPIFsettings will continue as DHCP client until changed with the **config ipif** command.
Parameters	Only Administrator and Operator-level users can issue this command.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To stop the auto-configuration function:

```
DGS-3426:5#disable autoconfig
Command: disable autoconfig

Success.

DGS-3426:5#
```

show autoconfig

Purpose	Used to display the current auto-configuration status of the Switch.
Syntax	**show autoconfig**
Description	This will list the current status of the auto-configuration function.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To view the auto-configuration status:

```
DGS-3426:5#show autoconfig
Command: show autoconfig

Autoconfig State: Disabled.

DGS-3426:5#
```

ping

Purpose	Used to test the connectivity between network devices.
Syntax	**ping <ipaddr> {times <value 1–255>} {timeout <sec 1–99>}**
Description	This command 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	*<ipaddr>* – Specifies the IP address of the host. *times <value 1–255>* – The number of individual ICMP echo messages to be sent. The maximum value is 255. *timeout <sec 1–99>* – Defines the time–out period while waiting for a response from the remote device. A value of 1 to 99 seconds can be specified. The default is 1 second.
Restrictions	None.

Example usage:

To ping the IP address 10.48.74.121 four times:

```
DGS-3426:5#ping 10.48.74.121 times 4
Command: ping 10.48.74.121

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

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

DGS-3426:5#
```

ping6

Purpose	Used to test the connectivity between IPv6 ready network devices.
Syntax	**ping6 <ipv6addr> {times <value 0–255> | size <value 1–6000>} {timeout <value 1–10>}**
Description	This 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	*<ipv6addr>* – Specifies the IP address of the host. *times <value 0–255>* – The number of individual ICMP echo messages to be sent. The maximum value is 255. *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-3426:5#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-3426:5#
```

10

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>}
enable syslog	
disable 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	<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	[severity [informational | warning | all] | facility [local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7] | udp_port <udp_port_number> | state [enable | disable]]
delete syslog host	[<index 1–4> | all]
show syslog host	{<index 1–4>}
show syslog	
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 port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3–2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. Non–contiguous portlist entries are separated by a comma. (ex: 1:1–1:3,1:7–1:9)
Restrictions	None.

Example usage:

To display the packets analysis for port 7 of switch 1:

```
DGS-3426:5#show packet ports 1:7
Command: show packet ports 1:7

Port number : 1:7
 ===============================================================
 Frame Size/Type       Frame Counts                  Frames/sec
 ---------------       ----------------------        -----------
 64                    213448                        19
 65-127                64318                         5
 128-255               42651                         0
 256-511               17647                         2
 512-1023              10225                         3
 1024-1518             30804                         7
 Unicast RX            62807                         0
 Multicast RX          70925                         15
 Broadcast RX          238728                        21

 Frame Type            Total                         Total/sec
 ---------------       ----------------------        -----------
 RX Bytes              83947600                      13780
 RX Frames             372460                        36
 TX Bytes              863819                        0
 TX Frames             6633                          0

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 port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3–2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. Non–contiguous portlist entries are separated by a comma. (ex: 1:1–1:3,1:7–1:9)
Restrictions	None.

Example usage:

To display the errors of the port 3 of switch 1:

```
DGS-3426:5#show error ports 1:3
Command: show error ports 1:3

Port number : 1:3
                    RX Frames                               TX Frames
                    ---------                               ---------
 CRC Error          0                    Excessive Deferral    0
 Undersize          0                    CRC Error             0
 Oversize           0                    Late Collision        0
 Fragment           0                    Excessive Collision   0
 Jabber             0                    Single Collision      0
 Drop Pkts          0                    Collision             0
 Symbol Error       0
 Buffer Full Drop   0
 ACL Drop           0
 Multicast Drop     0
 VLAN Ingress Drop  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	*ports* – Entering this parameter will display the current port utilization of the Switch. *cpu* – Entering this parameter will display the current CPU utilization of the Switch.
Restrictions	None.

Example usage:

To display the port utilization statistics:

```
DGS-3426:5#show utilization ports
Command: show utilization ports

Port     TX/sec     RX/sec    Util      Port     TX/sec     RX/sec    Util
 -----   ---------- ---------- ----      -----   ---------- ---------- ----
 1:1     0          0          0         1:22    0          0          0
 1:2     0          0          0         1:23    0          0          0
 1:3     0          0          0         1:24    0          0          0
 1:4     0          0          0
 1:5     0          0          0
 1:6     0          0          0
 1:7     31         9          1
 1:8     0          0          0
 1:9     0          0          0
 1:10    0          0          0
 1:11    0          0          0
 1:12    0          0          0
 1:13    0          0          0
 1:14    0          0          0
 1:15    10         31         1
 1:16    0          0          0
 1:17    0          0          0
 1:18    0          0          0
 1:19    0          0          0
 1:20    0          0          0
 1:21    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-3426:5#show utilization cpu
Command: show utilization cpu

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

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

clear counters

Purpose	Used to clear the Switch’s statistics counters.
Syntax	**clear counters {ports<portlist>}**
Description	This command will clear the counters used by the Switch to compile statistics.
Parameters	*ports <portlist>* – Specifies a port or range of ports to be displayed. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3–2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. Non–contiguous portlist entries are separated by a comma. (ex: 1:1–1:3,1:7–1:9)
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To clear the counters:

```
DGS-3426:5#clear counters ports 1:2-1:9
Command: clear counters ports 1:2-1:9

Success.

DGS-3426:5#
```

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 and Operator-level users can issue this command.

Example usage:

To clear the log information:

```
DGS-3426:5#clear log
Command: clear log

Success.

DGS-3426:5#
```

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	*index <value list>* – This command will display the history log, beginning at 1 and ending at the value specified by the user in 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-3426:5#show log index 1-5
Command: show log index 1-5

Index  Date       Time       Log Text
-----  ---------  ---------  ------------------------------------------
5         2006-04-2    09:38:18    Successful  login  through  Console  (Username:
Anonymous)
4      2006-04-26 09:36:20  System started up
3      2006-04-25 12:38:18  Port 1 link up, 100Mbps FULL duplex
2      2006-04-25 12:38:00  Spanning Tree Protocol is disabled
1      2006-04-25 12:37:42  Configuration saved to flash (Username: Anonymous)

DGS-3426:5#
```

enable syslog

Purpose	Used to enable the system log to be sent to a remote syslog server.
Syntax	**enable syslog**
Description	This command enables the system log to be sent to a remote syslog server.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable the syslog function on the Switch:

```
DGS-3426:5#enable syslog
Command: enable syslog

Success.

DGS-3426:5#
```

disable syslog

Purpose	Used to disable the system log to be sent to a remote system log.
Syntax	**disable syslog**
Description	This command disables the system log to be sent to a remote syslog server.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable the syslog function on the Switch:

```
DGS-3426:5#disable syslog
Command: disable syslog


Success.


DGS-3426:5#
```

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	This command is used to create a new syslog host.
Parameters	*<index 1–4>* – Specifies that the command will be applied to an index of hosts. There are four available indexes, numbered 1 through 4. *severity* – Severity level indicator, as shown below: **Bold** font indicates that the corresponding severity level is currently supported on the Switch. Numerical Severity Code 0 Emergency: system is unusable 1 Alert: action must be taken immediately 2 Critical: critical conditions 3 Error: error conditions **4 Warning: warning conditions** 5 Notice: normal but significant condition **6 Informational: informational messages** 7 Debug: debug–level messages *informational* – Specifies that informational messages will be sent to the remote host. This corresponds to number 6 from the list above. *warning* – Specifies that warning messages will be sent to the remote host. This corresponds to number 4 from the list above. *all* – Specifies that all of the currently supported syslog messages that are generated by the Switch will be sent to the remote host. *facility* – Some of the operating system daemons and processes have been assigned Facility values. Processes and daemons that have not been explicitly assigned a Facility may use any of the "local use" facilities or they may use the "user–level" Facility. Those Facilities that have been designated are shown in the following: **Bold** font indicates the facility values 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)**

create syslog host

	18 local use 2 (local2) **19 local use 3 (local3)** **20 local use 4 (local4)** **21 local use 5 (local5)** **22 local use 6 (local6)** **23 local use 7 (local7)** *local0* – Specifies that local use 0 messages will be sent to the remote host. This corresponds to number 16 from the list above. *local1* – Specifies that local use 1 messages will be sent to the remote host. This corresponds to number 17 from the list above. *local2* – Specifies that local use 2 messages will be sent to the remote host. This corresponds to number 18 from the list above. *local3* – Specifies that local use 3 messages will be sent to the remote host. This corresponds to number 19 from the list above. *local4* – Specifies that local use 4 messages will be sent to the remote host. This corresponds to number 20 from the list above. *local5* – Specifies that local use 5 messages will be sent to the remote host. This corresponds to number 21 from the list above. *local6* – Specifies that local use 6 messages will be sent to the remote host. This corresponds to number 22 from the list above. *local7* – Specifies that local use 7 messages will be sent to the remote host. This corresponds to number 23 from the list above. *udp_port <udp_port_number>* – Specifies the UDP port number that the syslog protocol will use to send messages to the remote host. *ipaddress <ipaddr>* – Specifies the IP address of the remote host where syslog messages will be sent. Only IPv4 addresses are supported for this feature. *state [enable | disable]* – Allows the sending of syslog messages to the remote host, specified above, to be enabled and disabled.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create a syslog host:

```
DGS-3426:5#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-3426:5#
```

config syslog host

Purpose	Used to configure the syslog protocol to send system log data to a remote host.
Syntax	**config 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	This command is used to configure the syslog protocol to send system log information to a remote host.
Parameters	*<index 1–4>* – Specifies that the command will be applied to an index of hosts. There are four available indexes, numbered 1 through 4. *severity* – Severity level indicator. These are described in the following: **Bold** font indicates that the corresponding severity level is currently supported on the

config syslog host

Switch.

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

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

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

all – Specifies that all of the currently supported syslog messages that are generated by the Switch will be sent to the remote host.

facility – Some of the operating system daemons and processes have been assigned Facility values. Processes and daemons that have not been explicitly assigned a Facility may use any of the "local use" facilities or they may use the "user–level" Facility. Those Facilities that have been designated are shown in the following: **Bold** font indicates the facility values the Switch currently supports.

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

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

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

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

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

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

config syslog host

	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. *ipaddress <ipaddr>* – Specifies the IP address of the remote host where syslog messages will be sent. Only IPv4 addresses are supported for this feature. *state [enable | disable]* – Allows the sending of syslog messages to the remote host, specified above, to be enabled and disabled.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure a syslog host:

```
DGS-3426:5#config syslog host 1 severity all
Command: config syslog host 1 severity all

Success.

DGS-3426:5#config syslog host 1 facility local0
Command: config syslog host 1 facility local0

Success.

DGS-3426:5#config syslog host 1  udp_port  6000
Command: config syslog host 1  udp_port  6000

Success.

DGS-3426:5#config syslog host 1 ipaddress 10.44.67.8
Command: config syslog host 1 ipaddress 10.44.67.8

Success.

DGS-3426:5#config syslog host 1 state enabled
Command: config syslog host 1 state enabled

Success.

DGS-3426:5#
```

config syslog host all

Purpose	Used to configure the syslog protocol to send system log data to a remote host.
Syntax	**config syslog host all [severity [informational | warning | all] | facility [local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7] | udp_port <udp_port_number> | state [enable | disable]]**
Description	This command is used to configure the syslog protocol to send system log information to a remote host.
Parameters	*all* – Specifies that the command will be applied to all hosts. *severity* – Severity level indicator, as described below: **Bold** font indicates that the corresponding severity level is currently supported on the Switch. Numerical Severity

config syslog host all

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

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

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

all – Specifies that all of the currently supported syslog messages that are generated by the Switch will be sent to the remote host.

facility – Some of the operating system daemons and processes have been assigned Facility values. Processes and daemons that have not been explicitly assigned a Facility may use any of the "local use" facilities or they may use the "user–level" Facility. Those Facilities that have been designated are shown in the following: **Bold** font indicates that 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)**

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.

config syslog host all

	local6 – Specifies that local use 6 messages will be sent to the remote host. This corresponds to number 22 from the list above. *local7* – Specifies that local use 7 messages will be sent to the remote host. This corresponds to number 23 from the list above. *udp_port <udp_port_number>* – Specifies the UDP port number that the syslog protocol will use to send messages to the remote host. *state [enable* | *disable]* – Allows the sending of syslog messages to the remote host, specified above, to be enabled and disabled.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure all syslog hosts:

```
DGS-3426:5#config syslog host all severity all
Command: config syslog host all severity all

Success.

DGS-3426:5#config syslog host all facility local0
Command: config syslog host all facility local0

Success.

DGS-3426:5#config syslog host all  udp_port  6000
Command: config syslog host all  udp_port  6000

Success.

DGS-3426:5#config syslog host all ipaddress 10.44.67.8
Command: config syslog host all ipaddress 10.44.67.8

Success.

DGS-3426:5#config syslog host all state enabled
Command: config syslog host all state enabled

Success.

DGS-3426:5#
```

delete syslog host

Purpose	Used to remove a syslog host, that has been previously configured, from the Switch.
Syntax	**delete syslog host [<index 1–4> | all]**
Description	This command is used to remove a syslog host that has been previously configured from the Switch.
Parameters	*<index 1–4>* – Specifies that the command will be applied to an index of hosts. There are four available indexes, numbered 1 through 4. *all* – Specifies that the command will be applied to all hosts.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete a previously configured Syslog host:

```
DGS-3426:5#delete syslog host 4
Command: delete syslog host 4

Success.

DGS-3426:5#
```

show syslog host

Purpose	Used to display the syslog hosts currently configured on the Switch.
Syntax	**show syslog host {<index 1–4>}**
Description	This command is used to display the syslog hosts that are currently configured on the Switch.
Parameters	*<index 1–4>* – Specifies that the command will be applied to an index of hosts. There are four available indexes, numbered 1 through 4.
Restrictions	None.

Example usage:

To show syslog host information:

```
DGS-3426:5#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-3426:5#
```

show syslog

Purpose	Used to display the global current running status of the syslog function.
Syntax	**show syslog**
Description	This command will display the current running status of the syslog function on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To show the global state of the syslog function:

```
DGS-3426:5#show syslog
Command: show syslog

Syslog Global State: Disabled

DGS-3426:5#
```

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	This command is used to configure the system severity levels on the Switch. When an event occurs on the Switch, a message will be sent to the SNMP agent (trap), the Switch's log or both. Events occurring on the Switch are separated into three main categories, these categories are NOT precisely the same as the parameters of the same name (see below). • Information – Events classified as information are basic events occurring on the Switch that are not deemed as problematic, such as enabling or disabling various functions on the Switch. • Warning – Events classified as warning are problematic events that are not critical to the overall function of the Switch but do require attention, such as unsuccessful downloads or uploads and failed logins. • Critical – Events classified as critical are fatal exceptions occurring on the Switch, such as hardware failures or spoofing attacks.
Parameters	Choose one of the following to identify where severity messages are to be sent. • *trap* – Entering this parameter will define which events occurring on the Switch will be sent to a SNMP agent for analysis. • *log* – Entering this parameter will define which events occurring on the Switch will be sent to the Switch's log for analysis. • *all* – Entering this parameter will define which events occurring on the Switch will be sent to a SNMP agent and the Switch's log for analysis. Choose one of the following to identify what level of severity warnings are to be sent to the destination entered above. *critical* – Entering this parameter along with the proper destination, stated above, will instruct the Switch to send only critical events to the Switch's log or SNMP agent. *warning* – Entering this parameter along with the proper destination, stated above, will instruct the Switch to send critical and warning events to the Switch's log or SNMP agent. *information* – Entering this parameter along with the proper destination, stated above, will instruct the switch to send informational, warning and critical events to the Switch's log or SNMP agent.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the system severity settings for critical traps only:

```
DGS-3426:5#config system_severity trap critical
Command: config system_severity trap critical

Success.

DGS-3426:5#
```

Example usage:

To upload an attack log file:

```
DGS-3426:5#upload attack_log_toTFTP 10.53.13.23 c:\attacklog1 unit 1
Command: upload attack_log_toTFTP 10.53.13.23 c:\attacklog1 unit 1

Connecting to server................... Done.
Upload attack log...................Done.

DGS-3426:5#
```

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	This command allows the user to configure the time method used in saving log files to the switch’s flash memory.
Parameters	*time_interval <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. *on_demand* – 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. *log_trigger* – Users who choose this method will have log files saved to the Switch every time a log event occurs on the Switch.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

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

```
DGS-3426:5#config log_save_timing time_interval 30
Command: config log_save_timing time_interval 30

Success.

DGS-3426:5#
```

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	This 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-3426:5#show log_save_timing
Command: show log_save_timing

Saving log method: every 30 minute(s)

DGS-3426:5#
```

11

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 BDPU packets so receiving devices can distinguish spanning tree instances, spanning tree regions and the VLANs associated with them. These instances will be classified by an *instance_id*. MSTP will connect multiple spanning trees with a Common and Internal Spanning Tree (CIST). The CIST will automatically determine each MSTP region, its maximum possible extent and will appear as one virtual bridge that runs a single spanning tree. Consequentially, frames assigned to different VLANs will follow different data routes within administratively established regions on the network, continuing to allow simple and full processing of frames, regardless of administrative errors in defining VLANs and their respective spanning trees. Each switch utilizing the MSTP on a network will have a single MSTP configuration that will have the following three attributes:

a) A configuration name defined by an alphanumeric string of up to 32 characters (defined in the **config stp mst_config_id** command as *name <string>*).

b) A configuration revision number (named here as a *revision_level*) and;

c) A 4096 element table (defined here as a *vid_range*) which will associate each of the possible 4096 VLANs supported by the Switch for a given instance.

To utilize the MSTP function on the Switch, three steps need to be taken:

a) The Switch must be set to the MSTP setting (**config stp version**)

b) The correct spanning tree priority for the MSTP instance must be entered (**config stp priority**).

c) VLANs that will be shared must be added to the MSTP Instance ID (**config stp instance_id**).

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

Command	Parameters
enable stp	
disable stp	
config stp version	[mstp | rstp | stp]
config stp	{maxage <value 6-40>|maxhops <value 1-40> |hellotime <value 1-10>| forwarddelay <value 4-30>|txholdcount <value 1-10>|fbpdu [enable|disable]|lbd [enable|disable] |lbd_recover_timer [<value 0> | <value 60-1000000>]|nni_bpdu_addr [dot1d | dot1ad]} (1)
config stp ports	<portlist> {externalCost [auto | <value 1-200000000>] |hellotime <value 1-10> | migrate [yes|no] |edge [true|false|auto]| p2p [true|false|auto] |state [enable|disable]| restricted_role [true|false] |restricted_tcn [true|false] | lbd [enable|disable]|fbpdu [enable|disable]} (1)
create stp instance_id	<value 1–15>
config stp instance _id	<value 1–15> [add_vlan | remove_vlan] <vidlist>
delete stp instance_id	<value 1–15>
config stp priority	<value 0–61440> instance_id <value 0–15>
config stp mst_config_id	{revision_level <int 0–65535> | name <string>} (1)
config stp mst_ports	<portlist> instance_id <value 0–15> {internalCost [auto | value 1–200000000] | priority <value 0–240>} (1)
show stp	
show stp ports	{<portlist>}
show stp instance	{<value 0–15>}

Command	Parameters
show stp mst_config_id	

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

enable stp

Purpose	Used to globally enable STP on the Switch.
Syntax	**enable stp**
Description	This command allows the Spanning Tree Protocol to be globally enabled on the Switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable STP, globally, on the Switch:

```
DGS-3426:5#enable stp
Command: enable stp

Success.

DGS-3426:5#
```

disable stp

Purpose	Used to globally disable STP on the Switch.
Syntax	**disable stp**
Description	This command allows the Spanning Tree Protocol to be globally disabled on the Switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable STP on the Switch:

```
DGS-3426:5#disable stp
Command: disable stp

Success.

DGS-3426:5#
```

config stp version

Purpose	Used to globally set the version of STP on the Switch.
Syntax	**config stp version [mstp | rstp | stp]**
Description	This command allows the user to choose the version of the spanning tree to be implemented on the Switch.
Parameters	*mstp* – Selecting this parameter will set the Multiple Spanning Tree Protocol (MSTP) globally on the Switch. *rstp* – Selecting this parameter will set the Rapid Spanning Tree Protocol (RSTP) globally on the Switch. *stp* – Selecting this parameter will set the Spanning Tree Protocol (STP) globally on the Switch.

config stp version

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

Example usage:

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

```
DGS–3426:5#config stp version mstp
Command: config stp version mstp

Success.

DGS–3426:5#
```

config stp

Purpose	Used to setup STP, RSTP, and MSTP on the Switch.
Syntax	**config stp {maxage <value 6-40>|maxhops <value 1-40> |hellotime <value 1-10>| forwarddelay <value 4-30>|txholdcount <value 1-10>|fbpdu [enable|disable]|lbd [enable|disable] |lbd_recover_timer [<value 0> | <value 60-1000000>]|nni_bpdu_addr [dot1d | dot1ad]} (1)**
Description	This command is used to setup the Spanning Tree Protocol (STP) for the entire switch. All commands here will be implemented for the STP version that is currently set on the Switch.
Parameters	*maxage <value 6–40>* – This value may be set to ensure that old information does not endlessly circulate through redundant paths in the network, preventing the effective propagation of the new information. Set by the Root Bridge, this value will aid in determining that the Switch has spanning tree configuration values consistent with other devices on the bridged LAN. If the value ages out and a BPDU has still not been received from the Root Bridge, the Switch will start sending its own BPDU to all other switches for permission to become the Root Bridge. If it turns out that your switch has the lowest Bridge Identifier, it will become the Root Bridge. The user may choose a time between 6 and 40 seconds. The default value is 20. *maxhops <value 1–40>* – The number of hops between devices in a spanning tree region before the BPDU (bridge protocol data unit) packet sent by the Switch will be discarded. Each switch on the hop count will reduce the hop count by one until the value reaches zero. The Switch will then discard the BDPU packet and the information held for the port will age out. The user may set a hop count from 1 to 40. The default is 20. If the entered value is less than 6, the maxhops will be 6. *hellotime <value 1–10>* – The user may set the time interval between transmission of configuration messages by the root device in STP, or by the designated router in RSTP, thus stating that the Switch is still functioning. A time between 1 and 10 seconds may be chosen, with a default setting of 2 seconds. If the value is more than 2, the hellotime will be 2. 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 BDPU Hello packets transmitted per interval. Default value = 6. *fbpdu [enable* | *disable]* – Allows the forwarding of STP BPDU packets from other network devices when STP is disabled on the Switch. The default is *disable*. *lbd [enable* | *disable]* – When this is enabled, the Switch will temporarily block STP switch–wide when a BDPU packet has been looped back. If the Switch detects its own BDPU 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 default is *enable*. *lbd_recover_timer [0 | < second 60 –1000000 >]* – Time allowed for recovery after an STP

config stp	
	loopback has been detected. After the timer has expired the Switch checks for an STP loopback, if no loopback detected, STP will be resumed. Entering 0 will disable LBD recovery. *nni_bpdu_addr [dot1d | dot1ad]* – Used to determine the BPDU protocol address for STP in a service provided site. It can use 802.1d STP address, 802.1ad service provider STP address or a user defined mutilcast address. The range of the user defined address is 0180C2000000 - 0180C2FFFFFF.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure STP with maxage 18 and maxhops of 15:

```
DGS-3426:5#config stp maxage 18 maxhops 15
Command: config stp maxage 18 maxhops 15

Success.

DGS-3426:5#
```

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|auto]| p2p [true|false|auto] |state [enable|disable]| restricted_role [true|false] |restricted_tcn [true|false]|lbd [enable|disable]|fbpdu [enable|disable]} (1)**
Description	This command is used to create and configure STP for a group of ports.
Parameters	*<portlist>* – Specifies a range of ports to be configured. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3–2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. Non–contiguous portlist entries are separated by a comma. (ex: 1:1–1:3,1:7–1:9) *externalCost* – This defines a metric that indicates the relative cost of forwarding packets to the specified port list. Port cost can be set automatically or as a metric value. The default value is *auto*. • *auto* – Setting this parameter for the external cost will automatically set the speed for forwarding packets to the specified port(s) in the list for optimal efficiency. Default port cost: 100Mbps port = 200000. Gigabit port = 20000. • *<value 1–200000000>* – Define a value between 1 and 200000000 to determine the external cost. The lower the number, the greater the probability the port will be chosen to forward packets. *hellotime <value 1–10>* – 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. If the value is more than 2, the hellotime will be 2. *migrate [yes | no]* – Setting this parameter as "*yes*" will set the ports to send out BDPU packets to other bridges, requesting information on their STP setting If the Switch is configured for RSTP, the port will be capable to migrate from 802.1d STP 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 | auto]* – *true* designates the port as an edge port. Edge ports cannot create

config stp ports

	loops, however an edge port can lose edge port status if a topology change creates a potential for a loop. An edge port normally should not receive BPDU packets. If a BPDU packet is received it automatically loses edge port status. *false* indicates that the port does not have edge port status. *auto* allows the port to have edge status whenever possible and operate as if the edge status were true. In auto mode, the bridge will delay for a period of time to become edge port if no bridge BPDU is received. *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*. *restricted_role [true* | *false]* –To decide if this port will be selected as the Root Port. The default value is false. *restricted_tcn [true* | *false]* –To decide if this port not to propagate topology change. The default value is false. *lbd [enable* | *disable]* – When this is enabled, the Switch will temporarily block STP on the port when a BDPU packet has been looped back. If the Switch detects its own BDPU 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 default is *disable*. *fbpdu [enable* | *disable]* – Enabling this parameter will allow the forwarding of STP BPDU from other network devices when STP is disabled on the port. The default is *disable*.
Restrictions	Only Administrator 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 of module 1.

```
DGS-3426:5#config stp ports 1:1-1:5 externalCost 19 hellotime 5 migrate yes
state enable
Command: config stp ports 1:1-1:5 externalCost 19 hellotime 5 migrate yes state
enable

Success.

DGS-3426:5#
```

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 is used to create an STP instance ID for the Multiple Spanning Tree Protocol. There are 16 STP instances on the Switch (one internal CIST, unchangeable) and the user may create up to 15 instance IDs for the Switch.
Parameters	*<value 1–15>* – Enter a value between 1 and 15 to identify the Spanning Tree instance on the Switch.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create a spanning tree instance 2:

```
DGS-3426:5#create stp instance_id 2
Command: create stp instance_id 2

Success.

DGS-3426:5#
```

config stp instance_id

Purpose	Used to add or delete vlans for instance ID.
Syntax	**config stp instance_id <value 1–15> [add_vlan | remove_vlan] <vidlist>**
Description	This command is used to map VIDs (VLAN IDs) to previously configured STP instances on the Switch by creating an *instance_id*. A STP instance may have multiple members with the same MSTP configuration. There is no limit to the number of STP regions in a network but each region only supports a maximum of 16 spanning tree instances (one unchangeable default entry). VIDs can belong to only one spanning tree instance at a time. Note that switches in the same spanning tree region having the same STP *instance_id* must be mapped identically, and have the same configuration *revision_level* number and the same *name*.
Parameters	<*value 1–15*> – Enter a number between 1 and 15 to define the instance_id. The Switch supports 16 STP regions with one unchangeable default instance ID set as 0. *add_vlan* – Along with the vid_range <vidlist> parameter, this command will add VIDs to the previously configured STP instance_id. *remove_vlan* – Along with the vid_range <vidlist> parameter, this command will remove VIDs to the previously configured STP instance_id. <*vidlist*> – Specify the VID range from configured VLANs set on the Switch. Supported VIDs on the Switch range from ID number 1 to 4094.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure instance ID 2 to add VID 10:

```
DGS-3426:5#config stp instance_id 2 add_vlan 10
Command : config stp instance_id 2 add_vlan 10

Success.

DGS-3426:5#
```

Example usage:

To remove VID 10 from instance ID 2:

```
DGS-3426:5#config stp instance_id 2 remove_vlan 10
Command : config stp instance_id 2 remove_vlan 10

Success.

DGS-3426:5#
```

delete stp instance_id

Purpose	Used to delete a STP instance ID from the Switch.
Syntax	**delete stp instance_id <value 1–15>**
Description	This command allows the user to delete a previously configured STP instance ID from the Switch.
Parameters	*<value 1–15>* – Enter a value between 1 and 15 to identify the Spanning Tree instance on the Switch.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete STP instance ID 2 from the Switch.

```
DGS-3426:5#delete stp instance_id 2
Command: delete stp instance_id 2

Success.

DGS-3426:5#
```

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 *instance_id* for forwarding packets. The lower the priority value set, the higher the priority.
Parameters	*priority <value 0–61440>* – Select a value between 0 and 61440 to specify the priority for a specified instance id for forwarding packets. The lower the value, the higher the priority. This entry must be divisible by 4096. *instance_id <value 0–15>* – Enter the value corresponding to the previously configured instance id of which the user wishes to set the priority value. An instance id of *0* denotes the default *instance_id* (CIST) internally set on the Switch.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

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

```
DGS-3426:5#config stp priority 4096 instance_id 2
Command : config stp priority 4096 instance_id 2

Success.

DGS-3426:5#
```

config stp mst_config_id

Purpose	Used to update the MSTP configuration identification.
Syntax	**config stp mst_config_id {revision_level <int 0–65535> | name <string>} (1)**
Description	This command will uniquely identify the MSTP configuration currently configured on the Switch. Information entered here will be attached to BPDU packets as an identifier for the MSTP region to which it belongs. Switches having the same *revision_level* and *name* will be considered as part of the same MSTP region.

config stp mst_config_id	
Parameters	*revision_level <int 0–65535>*– Enter a number between *0* and *65535* to identify the MSTP region. This value, along with the name will identify the MSTP region configured on the Switch. The default setting is *0*. *name <string>* – Enter an alphanumeric string of up to 32 characters to uniquely identify the MSTP region on the Switch. This *name*, along with the *revision_level* value will identify the MSTP region configured on the Switch. If no *name* is entered, the default name will be the MAC address of the device.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the MSTP region of the Switch with *revision_level* 10 and the *name* “Trinity”:

```
DGS-3426:5#config stp mst_config_id revision_level 10 name Trinity
Command : config stp mst_config_id revision_level 10 name Trinity

Success.

DGS-3426:5#
```

config stp mst_ports	
Purpose	Used to update the port configuration for a MSTP instance.
Syntax	**config stp mst_ports <portlist> instance_id <value 0–15> {internalCost [auto | <value 1–200000000>] priority <value 0–240>} (1)**
Description	This command will update the port configuration for a STP *instance_id*. If a loop occurs, the MSTP function will use the port priority to select an interface to put into the forwarding state. Set a higher priority value for interfaces to be selected for forwarding first. In instances where the priority value is identical, the MSTP function will implement the lowest port number into the forwarding state and other interfaces will be blocked. Remember that lower priority values mean higher priorities for forwarding packets.
Parameters	*<portlist>* – Specifies a range of ports to be configured. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3–2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. Non–contiguous portlist entries are separated by a comma. (ex: 1:1–1:3,1:7–1:9) *instance_id <value 0–15>* – Enter a numerical value between 0 and 15 to identify the *instance_id* previously configured on the Switch. An entry of 0 will denote the CIST (Common and Internal Spanning Tree). *internalCost* – This parameter is set to represent the relative cost of forwarding packets to specified ports when an interface is selected within a STP instance. The default setting is *auto*. There are two options: • *auto* – Selecting this parameter for the *internalCost* will set quickest route automatically and optimally for an interface. The default value is derived from the media speed of the interface. • *value 1–200000000* – Selecting this parameter with a value in the range of 1–200000000 will set the quickest route when a loop occurs. A lower *internalCost* represents a quicker transmission. *priority <value 0–240>* – Enter a value between 0 and 240 to set the priority for the port interface. A higher priority will designate the interface to forward packets first. A lower number denotes a higher priority.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

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

```
DGS-3426:5#config stp mst_ports 1:1-1:2 instance_id 0 internalCost auto priority
0
Command: config stp mst_ports 1:1-1:2 instance_id 0 internalCost auto priority 0

Success.

DGS-3426:5#
```

show stp	
Purpose	Used to display the Switch’s current STP configuration.
Syntax	**show stp**
Description	This command displays the Switch’s current STP configuration.
Parameters	None.
Restrictions	None.

Example usage:

To display the status of STP on the Switch:

Status 1: STP enabled with STP compatible version

```
DGS-3426:5#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 Age                 : 20
TX Hold Count           : 3
Forwarding BPDU         : Enabled
Loopback Detection      : Enabled
LBD Recover Time        : 60
NNI BPDU Address        : dot1ad

DGS-3426:5#
```

Status 2 : STP enabled for RSTP

```
DGS-3426:5#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 Age                  : 20
TX Hold Count            : 3
Forwarding BPDU          : Enabled
Loopback Detection       : Enabled
LBD Recover Time         : 60
NNI BPDU Address         : dot1ad

DGS-3426:5#
```

Status 3 : STP enabled for MSTP

```
DGS-3426:5#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
 NNI BPDU Address         : dot1ad

DGS-3426:5#
```

show stp ports

Purpose	Used to display the Switch’s current STP port configuration.
Syntax	**show stp ports <portlist>**
Description	This command is used to display the STP port settings and STP port Operational Status currently implemented on the Switch.
Parameters	<*portlist*> – Specifies a range of ports to be configured. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3–2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. Non–contiguous portlist entries are separated by a comma. (ex: 1:1–1:3,1:7–1:9)
Restrictions	None.

Example usage:

To show STP ports:

```
DGS-3426:5#show stp ports 1:1-1:9
Command: show stp ports 1:1-1:9

MSTP Port Information
 ----------------------
Port Index     : 1:1   , Hello Time: 2 /2 , Port STP : Enabled  , LBD : No
External PathCost : Auto/200000   , Edge Port : False/No , P2P : Auto /Yes
Port RestrictedRole : False,  Port RestrictedTCN : False
Port Forward BPDU : Disabled
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 r Refresh
```

show stp instance

Purpose	Used to display the Switch’s STP instance configuration
Syntax	**show stp instance <value 0–15>**
Description	This command is used to display the Switch’s current STP Instance Settings and the STP Instance Operational Status.
Parameters	<*value 0–15*> – Enter a value defining the previously configured *instance_id* on the Switch. An entry of *0* will display the STP configuration for the CIST internally set on the Switch.
Restrictions	None.

Example usage:

To display the STP instance configuration for instance 0 (the internal CIST) on the Switch:

```
DGS-3426:5#show stp instance 0
Command: show stp instance 0

STP Instance Settings
 ---------------------------
 Instance Type                : CIST
 Instance Status              : Enabled
 Instance Priority            : 32768(Bridge Priority : 32768, SYS ID Ext : 0 )

 STP Instance Operational Status
 --------------------------------
 Designated Root Bridge   : 32766/00-90-27-39-78-E2
 External Root Cost       : 200012
 Regional Root Bri        : 32768/00-53-13-1A-33-24
 Internal Root Cost       : 0
 Designated Bridge        : 32768/00-50-BA-71-20-D6
 Root Port                : 1:23
 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 is used to display 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-3426:5#show stp mst_config_id
Command: show stp mst_config_id

 Current MST Configuration Identification
 ----------------------------------------
 Configuration Name : 00:19:5B:3D:7C:D6        Revision Level :0
 MSTI ID     Vid list
 -------     ------------------------------------------------------
    CIST     1-4094

DGS-3426:5#
```

12

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}
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>}
show ipfdb	<ipaddr>

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 is used to make an entry in the Switch’s unicast MAC address forwarding database.
Parameters	*<vlan_name 32>* – The name of the VLAN on which the MAC address resides. *<macaddr>* – The MAC address that will be added to the forwarding table. *port <port>* – The port number corresponding to the MAC destination address. The Switch will always forward traffic to the specified device through this port. The port is specified by listing the switch number and the port number on that switch, separated by a colon. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create a unicast MAC FDB entry**:**

```
DGS-3426:5#create fdb default 00-00-00-00-01-02 port 1:5
Command: create fdb default 00-00-00-00-01-02 port 1:5

Success.

DGS-3426:5#
```

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 is used to make an entry in the Switch's multicast MAC address forwarding database.
Parameters	<*vlan_name 32*> – The name of the VLAN on which the MAC address resides. <*macaddr*> – The MAC address that will be added to the forwarding table.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create multicast MAC forwarding**:**

```
DGS-3426:5#create multicast_fdb default 01-00-00-00-00-01
Command: create multicast_fdb default 01-00-00-00-00-01

Success.

DGS-3426:5#
```

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 is used to configure 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 port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3–2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. Non–contiguous portlist entries are separated by a comma. (ex: 1:1–1:3,1:7–1:9)
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To add multicast MAC forwarding:

```
DGS-3426:5#config multicast_fdb default 01-00-00-00-00-01 add 1:1-1:5
Command: config multicast_fdb default 01-00-00-00-00-01 add 1:1-1:5

Success.

DGS-3426:5#
```

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 and Operator-level users can issue this command.

Example usage:

To set the FDB aging time:

```
DGS-3426:5#config fdb aging_time 300
Command: config fdb aging_time 300

Success.

DGS-3426:5#
```

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 deleted from the forwarding table.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete a permanent FDB entry:

```
DGS-3426:5#delete fdb default 00-00-00-00-01-02
Command: delete fdb default 00-00-00-00-01-02

Success.

DGS-3426:5#
```

Example usage:

To delete a multicast FDB entry:

```
DGS-3426:5#delete fdb default 01-00-00-00-01-02
Command: delete fdb default 01-00-00-00-01-02

Success.

DGS-3426:5#
```

clear fdb

Purpose	Used to clear the Switch’s forwarding database of all dynamically learned MAC addresses.
Syntax	**clear fdb [vlan <vlan_name 32> | port <port> | all]**
Description	This command is used to clear dynamically learned entries to the Switch’s forwarding database.
Parameters	*<vlan_name 32>* – The name of the VLAN on which the MAC address resides. *port <port>* – The port number corresponding to the MAC destination address. The Switch will always forward traffic to the specified device through this port. The port is specified by listing the switch number and the port number on that switch, separated by a colon. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. Non–contiguous portlist entries are separated by a comma. (ex: 1:1–1:3,1:7–1:9) *all* – Clears all dynamic entries to the Switch’s forwarding database.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To clear all FDB dynamic entries:

```
DGS-3426:5#clear fdb all
Command: clear fdb all

Success.

DGS-3426:5#
```

show multicast_fdb

Purpose	Used to display the contents of the Switch’s multicast forwarding database.
Syntax	**show mulitcast_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	*<vlan_name 32>* – The name of the VLAN on which the MAC address resides. The VID of the VLAN on which the MAC address resides. *<vidlist>* – Displays the entries for the VLANs indicated by the VID list. *<macaddr>* – The MAC address that is present in the forwarding database table.
Restrictions	None.

Example usage:

To display multicast MAC address table:

```
DGS-3426:5#show multicast_fdb vlan default
Command: show multicast_fdb vlan default

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

Total Entries  : 1

DGS-3426:5#
```

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 is used to display the current contents of the Switch’s forwarding database.
Parameters	*port <port>* – The port number corresponding to the MAC destination address. The Switch will always forward traffic to the specified device through this port. The port is specified by listing the switch number and the port number on that switch, separated by a colon. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. *<vlan_name 32>* – The name of the VLAN on which the MAC address resides. The VID of the VLAN on which the MAC address resides *<vidlist>* – Displays the entries for the VLANs indicated by the VID list. *<macaddr>* – The MAC address that is present in the forwarding database table. *static* – Displays the static MAC address entries. *aging_time* – Displays the aging time for the MAC address forwarding database.
Restrictions	None.

Example usage:

To display unicast MAC address table:

```
DGS-3426:5#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      1:10       Dynamic
1        default         00-00-51-43-70-00      1:10       Dynamic
1        default         00-00-5E-00-01-01      1:10       Dynamic
1        default         00-00-74-60-72-2D      1:10       Dynamic
1        default         00-00-81-05-00-80      1:10       Dynamic
1        default         00-00-81-05-02-00      1:10       Dynamic
1        default         00-00-81-48-70-01      1:10       Dynamic
1        default         00-00-E2-4F-57-03      1:10       Dynamic
1        default         00-00-E2-61-53-18      1:10       Dynamic
1        default         00-00-E2-6B-BC-F6      1:10       Dynamic
1        default         00-00-E2-7F-6B-53      1:10       Dynamic
1        default         00-00-E2-82-7D-90      1:10       Dynamic
1        default         00-00-F8-7C-1C-29      1:10       Dynamic
1        default         00-01-02-03-04-00      CPU        Self
1        default         00-01-02-03-04-05      1:10       Dynamic
1        default         00-01-30-10-2C-C7      1:10       Dynamic
1        default         00-01-30-FA-5F-00      1:10       Dynamic
1        default         00-02-3F-63-DD-68      1:10       Dynamic
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

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

Example usage:

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

```
DGS-3426:5#config multicast filtering_mode all filter_unregistered_groups
Command: config multicast filtering_mode all filter_unregistered_groups

Success.

DGS-3426:5#
```

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 is used to display the current multicast packet filtering mode for specified VLANs or all VLANs on the Switch.
Parameters	*vlan <vlan_name 32>* – Specifies a VLAN to display multicast filtering status.
Restrictions	None.

Example usage:

To view the multicast filtering mode for all VLANs:

```
DGS-3426:5#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-3426:5#
```

show ipfdb

Purpose	Used to display the current IP address forwarding database table.
Syntax	**show ipfdb <ipaddr>**
Description	This command is used to display the current contents of the Switch's IP forwarding database.
Parameters	*<ipaddr>* – The user may enter an IP address by which to view the table.
Restrictions	None.

Example usage:

To view the IP forwarding database table:

```
DGS-3426:5#show ipfdb
Command: show ipfdb

Interface      IP Address      Port    Learned
------------   --------------  ------  ------------
System        10.0.0.1          1:13    Dynamic
System        10.0.0.2          1:13    Dynamic
System        10.0.0.3          1:13    Dynamic
System        10.0.0.4          1:13    Dynamic
System        10.0.0.7          1:13    Dynamic
System        10.0.0.30         1:13    Dynamic
System        10.0.34.1         1:13    Dynamic
System        10.0.51.1         1:13    Dynamic
System        10.0.58.4         1:13    Dynamic
System        10.0.85.168       1:13    Dynamic
System        10.1.1.1          1:13    Dynamic
System        10.1.1.99         1:13    Dynamic
System        10.1.1.101        1:13    Dynamic
System        10.1.1.102        1:13    Dynamic
System        10.1.1.103        1:13    Dynamic
System        10.1.1.152        1:13    Dynamic
System        10.1.1.157        1:13    Dynamic
System        10.1.1.161        1:13    Dynamic
System        10.1.1.162        1:13    Dynamic
System        10.1.1.163        1:13    Dynamic
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

13

TRAFFIC CONTROL COMMANDS

On a computer network, packets such as Multicast packets and Broadcast packets continually flood the network as normal procedure. At times, this traffic may increase do to a malicious endstation on the network or a malfunctioning device, such as a faulty network card. Thus, switch throughput problems will arise and consequently affect the overall performance of the switch network. To help rectify this packet storm, the Switch will monitor and control the situation.

The packet storm is monitored to determine if too many packets are flooding the network, based on the threshold level provided by the user. Once a packet storm has been detected, the Switch will drop packets coming into the Switch until the storm has subsided. This method can be utilized by selecting the Drop option of the Action field in the window below. The Switch will also scan and monitor packets coming into the Switch by monitoring the Switch’s chip counter. This method is only viable for Broadcast and Multicast storms because the chip only has counters for these two types of packets. Once a storm has been detected (that is, once the packet threshold set below has been exceeded), the Switch will shutdown the port to all incoming traffic with the exception of STP BPDU packets, for a time period specified using the Countdown field. If this field times out and the packet storm continues, the port will be placed in a Shutdown Forever mode which will produce a warning message to be sent to the Trap Receiver. Once in Shutdown Forever mode, the only way to recover the shutdown forever port on the Switch is to use the **traffic control_recovery command**.

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>} (1)
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/dlf 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>} (1)

Description

This command is used to configure traffic control.

Parameters

<portlist> – Used to specify a range of ports to be configured for traffic control. This is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3–2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. Non–contiguous portlist entries are separated by a comma. (ex: 1:1–1:3,1:7–1:9)

all – Specifies all ports are to be configured for traffic control on the Switch.

broadcast [enable | disable] – Enables or disables broadcast storm control.

multicast [enable | disable] – Enables or disables multicast storm control.

dlf [enable | disable] – Enables or disables dlf traffic control.

action – Used to configure the action taken when a storm control has been detected on the Switch. The user has two options:

- *drop* – Utilizes the hardware Traffic Control mechanism, which means the Switch's hardware will determine the Packet Storm based on the Threshold value stated and drop packets until the issue is resolved.
- *shutdown* – Utilizes the Switch's software Traffic Control mechanism to determine the Packet Storm occurring. Once detected, the port will deny all incoming traffic to the port except STP BPDU packets, which are essential in keeping the Spanning Tree operational on the Switch. If the countdown timer has expired and yet the Packet Storm continues, the port will be placed in Shutdown Forever mode and is no longer operational until the user manually resets the port using the **config traffic control_recover** 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/dlf 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.

- *0* – 0 is the default setting for this field and 0 will denote that the port will never shutdown.
- *minutes 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 traffic control_recover** command mentioned previously in this manual.

Restrictions

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

Example usage:

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

```
DGS-3426:5#config traffic control all broadcast enable
Command: config traffic control all broadcast enable

Success.

DGS-3426:5#
```

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 shutdown 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. This is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3–2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. Non–contiguous portlist entries are separated by a comma. (ex: 1:1–1:3,1:7–1:9) *all* – All ports on switches in the switch stack.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure traffic control recover for ports 1–6 on unit 1:

```
DGS-3426:5#config traffic control_recover 1:1-1:6
Command: config traffic control_recover 1:1-1:6

Success.

DGS-3426:5#
```

config traffic trap

Purpose	Used to configure traps for traffic control.
Syntax	**config traffic trap [none | storm_occurred | storm_cleared | both]**
Description	This command is used to configure traffic storm trap messages.
Parameters	*none* – Will send no Storm trap warning messages regardless of action taken by the Traffic Control mechanism. *storm_occurred* – Will send Storm Trap warning messages upon the occurrence of a Traffic Storm only. *storm_cleared* – Will send Storm Trap messages when a Traffic Storm has been cleared by the Switch only. *both* – Will send Storm Trap messages when a Traffic Storm has been both detected and cleared by the Switch.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

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

```
DGS-3426:5#config traffic trap storm_occurred
Command: config traffic trap storm_occurred

Success.

DGS-3427:4#
```

show traffic control

Purpose	Used to display current traffic control settings.
Syntax	**show traffic control {<portlist>}**
Description	This command is used to display the current storm traffic control configuration on the Switch.
Parameters	<*portlist*> – Specify a range of ports to display. If unspecified, all ports will be displayed. This is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3–2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. Non–contiguous portlist entries are separated by a comma. (ex: 1:1–1:3,1:7–1:9)
Restrictions	None.

Example usage:

To display traffic control setting:

```
DGS-3426:5#show traffic control
Command: show traffic control

Traffic Storm Control Trap :[None]

Port Thres  Broadcast Multicast Unicast  Action   Count Time     Shutdown
     hold   Storm     Storm     Storm             down  Interval Forever
---- ------ --------- --------- -------- -------- ----- -------- --------
1:1  131072 Disabled  Disabled  Disabled drop     0     5
1:2  131072 Disabled  Disabled  Disabled drop     0     5
1:3  131072 Disabled  Disabled  Disabled drop     0     5
1:4  131072 Disabled  Disabled  Disabled drop     0     5
1:5  131072 Disabled  Disabled  Disabled drop     0     5
1:6  131072 Disabled  Disabled  Disabled drop     0     5
1:7  131072 Disabled  Disabled  Disabled drop     0     5
1:8  131072 Disabled  Disabled  Disabled drop     0     5
1:9  131072 Disabled  Disabled  Disabled drop     0     5
1:10 131072 Disabled  Disabled  Disabled drop     0     5
1:11 131072 Disabled  Disabled  Disabled drop     0     5
1:12 131072 Disabled  Disabled  Disabled drop     0     5
1:13 131072 Disabled  Disabled  Disabled drop     0     5
1:14 131072 Disabled  Disabled  Disabled drop     0     5
1:15 131072 Disabled  Disabled  Disabled drop     0     5
1:16 131072 Disabled  Disabled  Disabled drop     0     5
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

14

QOS COMMANDS

The xStack® DGS–3400 Series supports 802.1p priority queuing. The Switch has eight priority queues, one of which is internal and not configurable. 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 seven 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.

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

Command	Parameters
config bandwidth_control	[<portlist>| all]{rx_rate [no_limit | <value 64-10000000>] | tx_rate [no_limit | <value 64-10000000>]} (1)
show bandwidth_control	{<portlist>}
config scheduling	<class_id 0–6> {max_packet <value 0–15>} (1)
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	**config bandwidth_control [<portlist>| all]{rx_rate [no_limit | <value 64-10000000>] | tx_rate [no_limit | <value 64-10000000>]} (1)**
Description	This command is used to configure bandwidth on a port–by–port basis.
Parameters	*<portlist>* – Specifies a port or range of ports to be configured. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3–2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. Non–contiguous portlist entries are separated by a comma. (ex: 1:1–1:3,1:7–1:9) *rx_rate* – Specifies that one of the parameters below (*no_limit* or *<value 64-10000000>*) will be applied to the rate at which the above specified ports will be allowed to receive packets ▪ *no_limit* – Specifies that there will be no limit on the rate of packets received by the above specified ports. ▪ *<value 64–10000000>* – Specifies the receiving packet limit in Kbps, that the above ports will be allowed to receive. *tx_rate* – Specifies that one of the parameters below (*no_limit* or *<value 64-10000000>*) will be applied to the rate at which the above specified ports will be allowed to transmit packets. ▪ *no_limit* – Specifies that there will be no limit on the rate of packets transmitted by the above specified ports. ▪ *<value 64-10000000>* – Specifies the packet limit, in Kbps, that the above ports will be allowed to receive.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure bandwidth control:

```
DGS-3426:5#config bandwidth_control 1:1–1:8 rx_rate 64 tx_rate 64
Command: config bandwidth_control 1:1–1:8 rx_rate 64 tx_rate 64

Success.

DGS-3426:5#
```

show bandwidth_control

Purpose	Used to display the bandwidth control table.
Syntax	**show bandwidth_control {<portlist>}**
Description	This command is used to display the current bandwidth control configuration on the Switch, on a port–by–port basis.
Parameters	*<portlist>* – Specifies a port or range of ports to be viewed. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3–2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. Non–contiguous portlist entries are separated by a comma. (ex: 1:1–1:3,1:7–1:9)
Restrictions	None.

Example usage:

To display bandwidth control settings:

```
DGS-3426:5#show bandwidth_control 1:1-1:10
Command: show bandwidth_control 1:1-1:10

Bandwidth Control Table

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


DGS-3426P:4#
```

config scheduling

Purpose	Used to configure the traffic scheduling mechanism for each QoS queue.
Syntax	**config scheduling <class_id 0–6> {max_packet <value 0–15>} (1)**
Description	The Switch contains eight hardware priority queues, one of which is internal and not configurable. Incoming packets must be mapped to one of these seven queues. This command is used to specify the rotation by which these seven 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 max_packet 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. The *max_packets* parameter allows you 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 (number 6) will be allowed to transmit 3 packets – then the next lowest hardware priority queue (number 5) will be allowed to transmit 3 packets, and so on, until all of the queues have transmitted 3 packets. The process will then repeat.
Parameters	*<class_id 0–6>* – 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. *max_packet <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.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the traffic scheduling mechanism for each queue:

```
DGS-3426:5# config scheduling 0 max_packet 12
Command: config scheduling 0 max_packet 12

Success.

DGS-3426:5#
```

show scheduling

Purpose	Used to display the currently configured traffic scheduling on the Switch.
Syntax	**show scheduling**
Description	This 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-3426:5#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-3426:5#
```

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 is used to configure the way 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 seven hardware priority queues: 802.1p Hardware Queue Remark 0 2 Mid–low 1 0 Lowest 2 1 Lowest 3 3 Mid–low 4 4 Mid–high 5 5 Mid–high 6 6 Highest 7 6 Highest This mapping scheme is based upon recommendations contained in IEEE 802.1D. Users may change this mapping by specifying the 802.1p user priority you want to go to the *<class_id 0–6>* (the number of the hardware queue).
Parameters	*<priority 0–7>* – The 802.1p user priority you want to associate with the *<class_id 0–6>* (the number of the hardware queue) with. *<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 and Operator-level users can issue this command.

Example usage:

To configure 802.1 user priority on the Switch:

```
DGS-3426:5# config 802.1p user_priority 1 6
Command: config 802.1p user_priority 1 6

Success.

DGS-3426:5#
```

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	This command is used to display 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 display 802.1p user priority:

```
DGS-3426:5#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-3426:5#
```

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 is used to specify a default priority handling of untagged packets received by the Switch. The priority value entered with this command will be used to determine which of the seven hardware priority queues the packet is forwarded to.
Parameters	*<portlist>* – Specifies a port or range of ports to be configured. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3–2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. Non–contiguous portlist entries are separated by a comma. (ex: 1:1–1:3,1:7–1:9) *all* – Specifies that the command applies to all ports on the Switch. *<priority 0–7>* – The priority value to assign to untagged packets received by the Switch or a range of ports on the Switch.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure 802.1p default priority on the Switch:

```
DGS-3426:5#config 802.1p default_priority all 5
Command: config 802.1p default_priority all 5

Success.

DGS-3426:5#
```

show 802.1 default_priority

Purpose	Used to display the currently configured 802.1p priority value that will be assigned to an incoming, untagged packet before being forwarded to its destination.
Syntax	**show 802.1p default_priority {<portlist>}**
Description	This command is used to display the currently configured 802.1p priority value that will be assigned to an incoming, untagged packet before being forwarded to its destination.
Parameters	*<portlist>* – Specifies a port or range of ports to be configured. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3–2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. Non–contiguous portlist entries are separated by a comma. (ex: 1:1–1:3,1:7–1:9)
Restrictions	None.

Example usage:

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

```
DGS-3426:5#show 802.1p default_priority
Command: show 802.1p default_priority

Port       Priority      Effective Priority
----       -----------   ------------------
1              0                      0
2              0                      0
3              0                      0
4              0                      0
5              0                      0
6              0                      0
7              0                      0
8              0                      0
9              0                      0
10             0                      0
11             0                      0
12             0                      0
13             0                      0
14             0                      0
15             0                      0
16             0                      0
17             0                      0
18             0                      0
19             0                      0
20             0                      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	This command is used to to select between a **weight fair** 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. 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.
Parameters	*strict* – 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. *weight_fair* – Entering the weight fair parameter indicates that the priority classes of service will empty packets in a fair weighted order. That is to say that they will be emptied in an even distribution.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the traffic scheduling mechanism for each QoS queue:

```
DGS-3426:5#config scheduling_mechanism strict
Command: config scheduling_mechanism strict

Success.

DGS-3426:5#
```

show scheduling_mechanism

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

Example usage:

To show the scheduling mechanism:

```
DGS-3426:5#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-3426:5#
```

enable hol_prevention

Purpose	Used to enable HOL prevention.
Syntax	**enable hol_prevention**
Description	This command is used to enable Head of Line prevention.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable HOL prevention:

```
DGS-3426:5#enable hol_prevention
Command: enable hol_prevention

Success.

DGS-3426:5#
```

disable hol_prevention

Purpose	Used to disable HOL prevention.
Syntax	**disable hol_prevention**
Description	This command is used to disable Head of Line prevention.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable HOL prevention:

```
DGS-3426:5#disable hol_prevention
Command: disable hol_prevention

Success.

DGS-3426:5#
```

show hol_prevention

Purpose	Used to show HOL prevention.
Syntax	**show hol_prevention**
Description	This command is used to display the Head of Line prevention state.
Parameters	None.
Restrictions	None.

Example usage:

To view the HOL prevention status:

```
DGS-3426:5#show hol_prevention
Command: show hol_prevention

Device HOL Prevention State: Enabled

DGS-3426:5#
```

15

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 is used to allows a range of ports to have all of their traffic also sent to a designated port, where a network sniffer or other device can monitor the network traffic. In addition, users can specify that only traffic received by or sent by one or both is mirrored to the Target port.
Parameters	*<port>* – This specifies the Target port (the port where mirrored packets will be received). The target port must be configured in the same VLAN and must be operating at the same speed a s 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. The port is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. *[add* | *delete]* – Specifies to add or delete ports to be mirrored which are specified in the *source ports* parameter. *source ports* – The port or ports being mirrored. This cannot include the Target port. • *<portlist>* – This specifies a port or range of ports that will be mirrored. That is, the range of ports in which all traffic will be copied and sent to the Target port. That is, the range of ports in which all traffic will be copied and sent to the Target port. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. Non–contiguous portlist entries are separated by a comma. (ex: 1:1–1:3,1:7–1:9) *rx* – Allows the mirroring of only packets received by (flowing into) the port or ports in the port list. *tx* – Allows the mirroring of only packets sent to (flowing out of) the port or ports in the port list. *both* – Mirrors all the packets received or sent by the port or ports in the port list.
Restrictions	The Target port cannot be listed as a source port. Only Administrator and Operator-level users can issue this command.

Example usage:

To add the mirroring ports:

```
DGS-3426:5# config mirror port 1:1 add source ports 1:2-1:7 both
Command: config mirror port 1:1 add source ports 1:2-1:7 both

Success.

DGS-3426:5#
```

Example usage:

To delete the mirroring ports:

```
DGS-3426:5#config mirror port 1:1 delete source ports 1:2-1:4 both
Command: config mirror port 1:1 delete source ports 1:2-1:4 both

Success.

DGS-3426:5#
```

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 and Operator-level users can issue this command.

Example usage:

To enable mirroring configurations:

```
DGS-3426:5#enable mirror
Command: enable mirror

Success.

DGS-3426:5#
```

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 and Operator-level users can issue this command.

Example usage:

To disable mirroring configurations:

```
DGS-3426:5#disable mirror
Command: disable mirror

Success.

DGS-3426:5#
```

show mirror

Purpose	Used to show the current port mirroring configuration on the Switch.
Syntax	**show mirror**
Description	This command is used to display the current port mirroring configuration on the Switch.
Parameters	None
Restrictions	None.

Example usage:

To display mirroring configuration:

```
DGS-3426:5#show mirror
Command: show mirror

Current Settings
Mirror Status : Enabled
Target Port   : 1:1
Mirrored Port :
                  RX :
                  TX : 1:2-1:7

DGS-3426:5#
```

16

VLAN COMMANDS

Along with normal VLAN configurations, this Switch now incorporate Q-in-Q VLANs. Also known as Double VLANs, Q-in-Q 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] | delete] <portlist> | advertisement [enable | disable]} (1)
config gvrp	[<portlist> | all] {state [enable | disable] | ingress_checking [enable | disable] | acceptable_frame [tagged_only | admit_all] | pvid <vlanid 1–4094>} (1)
enable gvrp	
disable gvrp	
show vlan	{[<vlan_name 32> | vlanid <vidlist>] | ports <portlist>}
show 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>} (1)
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 is used to create VLANs on the Switch.
Parameters	*<vlan_name 32>* – The name of the VLAN to be created. *tag <vlanid 2–4094>* – The VLAN ID of the VLAN to be created. Allowed values = 2–4094 *type* – This parameter uses the *type* field of the packet header to determine the packet protocol and destination VLAN: ▪ *1q_vlan* – Allows the creation of a normal 802.1Q VLAN on the Switch. *advertisement* – Specifies that the VLAN is able to join GVRP.
Restrictions	Each VLAN name can be up to 32 characters. Only Administrator and Operator-level users can issue this command.

Example usage:

To create a VLAN v1, tag 2:

```
DGS-3426:5#create vlan v1 tag 2
Command: create vlan v1 tag 2

Success.

DGS-3426:5#
```

delete vlan

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

Example usage:

To remove the VLAN “v1”:

```
DGS-3426:5#delete vlan v1
Command: delete vlan v1

Success.

DGS-3426:5#
```

config vlan

Purpose	Used to add additional ports to a previously configured VLAN.
Syntax	**config vlan <vlan_name 32> {[add [tagged | untagged | forbidden] | delete] <portlist> | advertisement [enable | disable]} (1)**
Description	This command is used to add ports to the port list of a previously configured VLAN. The additional ports may be specified as tagging, untagging, or forbidden. The default is to assign the ports as untagging.
Parameters	*<vlan_name 32>* – The name of the VLAN to which to add ports. *add* – Entering the add parameter will add ports to the VLAN. There are three types of ports to add: • *tagged* – Specifies the additional ports as tagged. • *untagged* – Specifies the additional ports as untagged. • *forbidden* – Specifies the additional ports as forbidden *delete* – Deletes ports from the specified VLAN. *<portlist>* – A port or range of ports to add to, or delete from the specified VLAN. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, **1:3** specifies switch number 1, port 3. **2:4** specifies switch number 2, port 4. **1:3–2:4** specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. Non–contiguous portlist entries are separated by a comma. (ex: 1:1–1:3,1:7–1:9) *advertisement [enable | disable]* – Enables or disables GVRP on the specified VLAN.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

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

```
DGS-3426:5#config vlan v1 add tagged 1:4-1:8
Command: config vlan v1 add tagged 1:4-1:8

Success.

DGS-3426:5#
```

To delete ports from a VLAN:

```
DGS-3426:5#config vlan v1 delete 1:6-1:8
Command: config vlan v1 delete 1:6-1:8

Success.

DGS-3426:5#
```

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>} (1)**
Description	This command is used to configure the Group VLAN Registration Protocol on the Switch. Users may configure ingress checking, the sending and receiving of GVRP information, and the Port VLAN ID (PVID).
Parameters	*<portlist>* – A port or range of ports for which to enable GVRP. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3–2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. Non–contiguous portlist entries are separated by a comma. (ex: 1:1–1:3,1:7–1:9) *all* – Specifies all of the ports on the Switch. *state [enable* | *disable]* – Enables or disables GVRP for the ports specified in the port list. *ingress_checking [enable* | *disable]* – Enables or disables ingress checking for the specified port list. *acceptable_frame [tagged_only* | *admit_all]* – This parameter states the frame type that will be accepted by the Switch for this function. *tagged_only* implies that only VLAN tagged frames will be accepted, while *admit_all* implies tagged and untagged frames will be accepted by the Switch. *pvid <vlanid 1–4094>* – Specifies the default VLAN ID associated with the port.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

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

```
DGS-3426:5#config gvrp 1:1-1:4 state enable ingress_checking enable
acceptable_frame tagged_only pvid 2
Command: config gvrp 1:1-1:4 state enable ingress_checking enable
acceptable_frame tagged_only pvid 2

Success.

DGS-3426:5#
```

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 on the Switch, without changing the GVRP configuration on the Switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable the GARP VLAN Registration Protocol (GVRP):

```
DGS-3426:5#enable gvrp
Command: enable gvrp

Success.

DGS-3426:5#
```

disable gvrp

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

Example usage:

To disable the GARP VLAN Registration Protocol (GVRP):

```
DGS-3426:5#disable gvrp
Command: disable gvrp

Success.

DGS-3426:5#
```

show vlan

Purpose	Used to display the current VLAN configuration information including parameters settings and operational value on the Switch.
Syntax	**show vlan {[<vlan_name 32> | vlanid <vidlist>] | ports <portlist>}**
Description	This command is used to display summary information about each VLAN including the VLAN ID, VLAN name, the Tagging/Untagging status, and the Member/Non–member/Forbidden status of each port that is a member of the VLAN.
Parameters	*<vlan_name 32>* – The VLAN name of the VLAN for which to display a summary of settings. *vidlist* – Specifies a list of VLANs by VLAN ID. *ports* – Specifies a port or range of ports for which the VLAN status is to be displayed.
Restrictions	None.

Example usage:

To display the Switch's current VLAN settings:

```
DGS-3426:5#show vlan
Command: show vlan

VID             : 1          VLAN Name     : default
VLAN Type       : Static     Advertisement : Enabled
Member Ports    : 1:1-1:24
Static Ports    : 1:1-1:24
Current Tagged Ports  :
Current Untagged Ports: 1:1-1:24
Static Tagged Ports   :
Static Untagged Ports : 1:1-1:24
Forbidden Ports       :

Total Entries: 1

DGS-3426:5#
```

show gvrp

Purpose	Used to display the GVRP status for a port list on the Switch.
Syntax	**show gvrp {<portlist>}**
Description	This command is used to display the GVRP status for a port list on the Switch.
Parameters	*<portlist>* – Specifies a port or range of ports for which the GVRP status is to be displayed. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3–2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. Non–contiguous portlist entries are separated by a comma. (ex: 1:1–1:3,1:7–1:9)
Restrictions	None.

Example usage:

To display GVRP port status:

```
DGS-3426:5#show gvrp
Command: show gvrp

Global GVRP : Disabled

Port     PVID  GVRP     Ingress Checking  Acceptable Frame Type
-------  ----  -------- ----------------  ---------------------------
 1:1     1     Disabled  Enabled           All Frames
 1:2     1     Disabled  Enabled           All Frames
 1:3     1     Disabled  Enabled           All Frames
 1:4     1     Disabled  Enabled           All Frames
 1:5     1     Disabled  Enabled           All Frames
 1:6     1     Disabled  Enabled           All Frames
 1:7     1     Disabled  Enabled           All Frames
 1:8     1     Disabled  Enabled           All Frames
 1:9     1     Disabled  Enabled           All Frames
 1:10    1     Disabled  Enabled           All Frames
 1:11    1     Disabled  Enabled           All Frames
 1:12    1     Disabled  Enabled           All Frames
 1:13    1     Disabled  Enabled           All Frames
 1:14    1     Disabled  Enabled           All Frames
 1:15    1     Disabled  Enabled           All Frames
 1:16    1     Disabled  Enabled           All Frames
 1:17    1     Disabled  Enabled           All Frames
 1:18    1     Disabled  Enabled           All Frames
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

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

Example usage:

To enable the Q-in-Q VLAN feature on the Switch, thus disabling normal VLANs and GVRP:

```
DGS-3426:5#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-3426:5#
```

disable double_vlan

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

Example usage:

To disable the Q-in-Q VLAN feature on the Switch

```
DGS-3426:5#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-3426:5#
```

create double_vlan

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

Example usage:

To create a Q-in-Q VLAN on the Switch called “Tiberius”:

```
DGS-3426:5#create double_vlan Tiberius spvid 6 tpid 0x9100
Command: create double_vlan Tiverius spvid 6 tpid 0x9100

Success.

DGS-3426:5#
```

config double_vlan

Purpose	Used to config the parameters for a previously created Q-in-Q VLAN (Double VLAN) on the Switch.
Syntax	**config double_vlan <vlan_name> {[[add [access | uplink] | delete] <portlist> | tpid <hex 0x0–0xffff>]} (1)**
Description	This command is used to configure a Q-in-Q VLAN (service provider VLAN) on the Switch.
Parameters	*vlan <vlan_name 32>* – The name of the Q-in-Q VLAN to be configured. The user is to enter an alphanumeric string of up to 32 characters to identify this VLAN. *add* – Specify this parameter to add ports configured in the *<portlist>* as one of the two following types of ports. • *uplink* – 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. • *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 port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3–2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. Non–contiguous portlist entries are separated by a comma. (ex: 1:1–1:3,1:7–1:9) *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 port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3–2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. Non–contiguous portlist entries are separated by a comma. (ex: 1:1–1:3,1:7–1:9) *tpid <hex 0x0–0xffff>*– The tag protocol ID. This ID, identified here in hex form, will help identify packets to devices as Q-in-Q VLAN tagged packets. The default setting is 0x8100.
Restrictions	Only Administrator and Operator-level users can issue this command. Users must have the Switch enabled for Q-in-Q VLANs.

Example usage:

To add ports 4 through 8 as access ports to the Q-in-Q VLAN “Tiberius”:

```
DGS-3426:5#config double_vlan Tiberius add access 1:4-1:8
Command: config double_vlan Tiberius add access 1:4-1:8

Success.

DGS-3426:5#
```

Example usage:

To delete ports 4 through 8 on the Q-in-Q VLAN “Tiberius”:

```
DGS-3426:5#config double_vlan Tiberius delete 1:4-1:8
Command: config double_vlan Tiberius delete 1:4-1:8

Success.

DGS-3426:5#
```

show double_vlan

Purpose	Used to display the Q-in-Q VLAN settings on the Switch.
Syntax	**show double_vlan {<vlan_name>}**
Description	This command is used to display the current Q-in-Q VLAN parameters configured on the Switch.
Parameters	*vlan name* – Enter the name of a previously created VLAN for which to display the settings.
Restrictions	None.

Example usage:

To display parameters for the Q-in-Q VLAN "Tiberius":

```
DGS-3426:5#show double_vlan Tiberius
Command: show double_vlan Tiberius

Global Double VLAN : Enabled
====================================================
SPVID          : 6
VLAN Name      : Tiberius
TPID           : 0x9200
Uplink ports   :
Access ports   : 1:4-1:8
Unknow ports   :
----------------------------------------------------
Total Entries : 1

DGS-3426:5#
```

enable pvid auto_assign

Purpose	Used to enable auto–assign PVID.
Syntax	**enable pvid auto_assign**
Description	This command is used to enable auto–assign PVID. If "PVID auto_assign" is disabled, PVID can only be changed by PVID configuration (user changes explicitly). The VLAN configuration has no effect on PVID. If "PVID auto_assign" 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 VLAN list. When user removes a port from the untagged membership of the PVID's VLAN, the port's PVID will be assigned with "default VLAN". The default setting is enabled.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable the auto–assign PVID:

```
DGS-3426:5#enable pvid auto_assign
Command: enable pvid auto_assign

Success.

DGS-3426:5#
```

disable pvid auto_assign

Purpose	Used to disable auto–assign PVID
Syntax	**disable pvid auto_assign**
Description	The command is used to enable auto–assign PVID. If “PVID auto_assign” is disabled, PVID can only be changed by PVID configuration (user changes explicitly). The VLAN configuration has no effect on PVID. The default setting is enabled.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable the auto–assign PVID:

```
DGS-3426:5# disable pvid auto_assign
Command: disable pvid auto_assign

Success.

DGS-3426:5#
```

show pvid auto_assign

Purpose	Show PVID auto–assignment state.
Syntax	**show pvid auto_assign**
Description	This command is used to displays the PVID auto–assignment state.
Parameters	None.
Restrictions	None.

Example usage:

To display PVID auto–assignment state:

```
DGS-3426:5#show pvid auto_assign
Command: show pvid auto_assign

PVID Auto-assignment: Enabled

DGS-3426:5#
```

17

ISM VLAN COMMANDS

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

Command	Parameters
create igmp_snooping multicast_vlan	<vlan_name 32> <vlanid 2–4094>
delete igmp_snooping mutlticast_vlan	<vlan_name 32>
config igmp_snooping multicast_vlan	<vlan_name 32> {member_port <portlist> | source_port <portlist> tag_member_port <portlist>| state [enable|disable] |replace_source_ip <ipaddr>} (1)
config igmp_snooping multicast_vlan_group	<vlan_name 32> [[add | delete] <mcast_address_list> | delete_all]
show igmp_snooping multicast_vlan	{<vlan_name 32>}
show igmp_snooping multicast_vlan_group	{<vlan_name 32>}

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

create igmp_snooping multicast_vlan

Purpose	Used to create an ISM VLAN on the switch.
Syntax	**create igmp_snooping multicast_vlan <vlan_name 32> <vlanid 2–4094>**
Description	This command is used to create a multicast VLAN on the Switch.
Parameters	<*vlan_name 32*> – Specifies the ISM VLAN name, max length is 32 <*vlanid 2-4094*> – Specifies the ISM VLAN ID.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create an igmp_snooping multicast_vlan:

```
DGS-3426:5#create igmp_snooping multicast_vlan test 2
Command: create igmp_snooping multicast_vlan test 2

Success.

DGS-3426:5#
```

delete igmp_snooping multicast_vlan

Purpose	Used to delete a previously created ISM VLAN on the Switch.
Syntax	**delete igmp_snooping multicast_vlan <vlan_name 32>**
Description	This command is used to delete a previously created multicast VLAN on the Switch.
Parameters	<*vlan_name 32*> – Specifies the ISM VLAN name, max length is 32.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete an ISM VLAN

```
DGS-3426:5#delete igmp_snooping multicast_vlan test
Command: delete igmp_snooping multicast_vlan test

Success.

DGS-3426:5#
```

config igmp_snooping multicast_vlan	
Purpose	Used to configure an ISM VLAN on the Switch, add source port, member port to this VLAN, and set state
Syntax	**config igmp_snooping multicast_vlan <vlan_name 32> member_port <portlist> | source_port <portlist> | tag_member_port <portlist> |state [enable|disable] | replace_source_ip <ipaddr> (1)**
Description	This command is used to configure the settings for a previously created multicast VLAN on the Switch.
Parameters	*<vlan_name 32>* – Specifies the ISM VLAN name. The maximum length is 32 characters. *member_port <portlist>* – Add untagged member ports to ISM VLAN, which connect with PC users *tag_member_port <portlist>* – Add tagged member ports to ISM VLAN, which connect with PC users. *source_port <portlist>* – Add source ports to ISM VLAN, which connect with uplink server *state* [*enable* | *disable*] – Enable or disable the ISM VLAN. *replace_source_ip <ipaddr>* – Specifies the IP address used to replace a source IP address in the received IGMP control packet only if a unicast IP address is valid.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure a member port, source port, set of ISM VLANs:

```
DGS-3426:5#config vlan default delete 10-20
Command: config vlan default delete 10-20

Success.

DGS-3426:5#create vlan v10
Command: create vlan v10

Success.

DES-3426:4#create vlan v20
Command: create vlan v20

Success.

DGS-3426:5#config vlan v10 add untagged 10
Command: config vlan v10 add untagged 10

Success.

DGS-3426:5#config vlan v20 add untagged 20
Command: config vlan v20 add untagged 20

Success.

DGS-3426:5# config igmp_snooping multicast_vlan test member_port 10,20
source_port 1 state enable
Command: config igmp_snooping multicast_vlan test member_port 10,20 source_port
1 state enable

Success.

DGS-3426:5#
```

config igmp_snooping multicast_vlan_group	
Purpose	Used to configure multicast group in this ISM VLAN on the switch
Syntax	**config igmp_snooping multicast_vlan_group <vlan_name 32> [[add | delete] <mcast_address_list> | delete_all]**
Description	This command is used to configure the multicast group which will be learned with the specific multicast VLAN.
Parameters	*<vlan_name 32>* – Specifies the ISM VLAN name, max length is 32 *add|delete* – Specifies the action of configured multicast group of this ISM VLAN *add* – add multicast group to this ISM VLAN *delete* – delete multicast group from this ISM VLAN *mcast_address_list* – Specifies the multiast groups being configure in this command *delete_all* – Clear all the multicast groups in the ISM VLAN
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure multicast group to an ISM VLAN:

```
DGS-3426:5#config igmp_snooping multicast_vlan_group test add 225.1.1.1-
225.1.1.10,225.1.1.20
Command: config igmp_snooping multicast_vlan_group test add 225.1.1.1-
225.1.1.10,225.1.1.20

Success.

DGS-3426:5#
```

show igmp_snooping multicast_vlan

Purpose	Used to display an ISM VLAN on the Switch.
Syntax	**show igmp_snooping multicast_vlan {<vlan_name 32>}**
Description	This command is used to display the settings of a multicast VLAN on the Switch.
Parameters	<*vlan_name 32*> – Specifies the ISM VLAN name, max length is 32
Restrictions	None.

Example usage:

To display an ISM VLAN:

```
DGS-3426:5# show igmp_snooping multicast_vlan
Command: show igmp_snooping multicast_vlan

VLAN Name                : test
VID                      : 2
Member (Untagged) Ports :1-8
Tagged Member Ports     : 10
Source Ports            : 9
Status                  : Enabled
Replace Source IP       : 192.18.2.1
Total Entries: 1
```

show igmp_snooping multicast_vlan_group

Purpose	Used to display the ISM VLAN groups on the Switch.
Syntax	**show igmp_snooping multicast_vlan_group <vlan_name 32>**
Description	This command is used to display the settings of a multicast VLAN group on the Switch.
Parameters	<*vlan_name 32*> – Specifies the ISM VLAN name. The maximum length is 32.
Restrictions	None.

Example usage:

To display an ISM VLAN Group:

```
DGS-3426:5#show igmp_snooping multicast_vlan_group
Command: show igmp_snooping multicast_vlan_group

VLAN Name          VLAN ID     From            To
-----------------  -------    ------------   -----------
test                 2

DGS-3426:5#
```

18

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	<value1–32> {master_port <port> | ports <portlist> state [enable | disable]} (1)
config link_aggregation algorithm	[mac_source | mac_destination | mac_source_dest | ip_source | ip_destination | ip_source_dest]
show link_aggregation	{group_id <value 1–32> | 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 is used to create a link aggregation group with a unique identifier.
Parameters	*<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. *type* – Specify the type of link aggregation used for the group. If the type is not specified the default type is *static*. • *lacp* – This designates the port group as LACP compliant. LACP allows dynamic adjustment to the aggregated port group. LACP compliant ports may be further configured (see **config lacp_ports**). LACP compliant must be connected to LACP compliant devices. • *static* – This designates the aggregated port group as static. Static port groups cannot be changed as easily as LACP compliant port groups since both linked devices must be manually configured if the configuration of the trunked group is changed. If static link aggregation is used, be sure that both ends of the connection are properly configured and that all ports have the same speed/duplex settings.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create a link aggregation group:

```
DGS-3426:5#create link_aggregation group_id 1
Command: create link_aggregation group_id 1

Success.

DGS-3426:5#
```

NOTE: When using LACP or static type link aggregation, be sure that both sides of the connection are identical in speed and duplex settings.

delete link_aggregation group_id	
Purpose	Used to delete a previously configured 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	*<value 1–32>* – 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 and Operator-level users can issue this command.

Example usage:

To delete a link aggregation group:

```
DGS-3426:5#delete link_aggregation group_id 6
Command: delete link_aggregation group_id 6

Success.

DGS-3426:5#
```

config link_aggregation group_id	
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]} (1)**
Description	This command is used to configure a link aggregation group that was created with the **create link_aggregation** command above. The Switch supports link aggregation cross box, which specifies that link aggregation groups may be spread over multiple switches in the switching stack. Up to eight ports can be set per link aggregation group.
Parameters	*group _id <value 32>* – Specifies the group ID. The Switch allows up to 32 link aggregation groups to be configured. The group number identifies each of the groups. *master_port <port>* – Master port ID. Specifies which port (by port number) of the link aggregation group will be the master port. All of the ports in a link aggregation group will share the port configuration with the master port. The port is specified by listing the switch number and the port number on that switch, separated by a colon. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. *ports <portlist>* – Specifies a range of ports that will belong to the link aggregation group. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3–2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. Non–contiguous portlist entries are separated by a comma. (ex: 1:1–1:3,1:7–1:9) Ports may be listed in only one port aggregation group, that is, link aggregation groups may not overlap. Up to eight ports can be set per link aggregation group. *state [enable* | *disable]* – Allows users to enable or disable the specified link aggregation group.
Restrictions	Only Administrator and Operator-level users can issue this command. Link aggregation groups may not overlap.

Example usage:

To define a load–sharing group of ports, group – ID 1, master port 5 with group members ports 5 – 7 plus port 9:

```
DGS-3426:5#config link_aggregation group_id 1 master_port 1:5 ports 1:5-1:7,1:9
Command: config link_aggregation group_id 1 master_port 1:5 ports 1:5-1:7,1:9

Success.

DGS-3426:5#
```

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 is used to configure the part of the packet examined by the Switch when selecting the egress port for transmitting load–sharing data. This feature is only available using the address–based load–sharing algorithm.
Parameters	*mac_source* – Indicates that the Switch should examine the MAC source address. *mac_destination* – Indicates that the Switch should examine the MAC destination address. *mac_source_dest* – Indicates that the Switch should examine the MAC source and destination addresses *ip_source* – Indicates that the Switch should examine the IP source address. *ip_destination* – Indicates that the Switch should examine the IP destination address. *ip_source_dest* – Indicates that the Switch should examine the IP source address and the destination address.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

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

```
DGS-3426:5#config link_aggregation algorithm mac_source_dest
Command: config link_aggregation algorithm mac_source_dest

Success.

DGS-3426:5#
```

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 is used to display the current link aggregation configuration of the Switch.
Parameters	*<value 1–32>* – Specifies the group ID. The Switch allows up to 32 link aggregation groups to be configured. The group number identifies each of the groups. *algorithm* – Allows the display of link aggregation to be specified by the algorithm in use.
Restrictions	None.

Example usage:

To display the Link Aggregation configuration:

```
DGS-3426:5#show link_aggregation
Command: show link_aggregation

Link Aggregation Algorithm = MAC-source-dest

Group ID        : 1
Type            : LACP
Master Port     : 1:5
Member Port     : 1:5-1:7,1:9
Active Port     :
Status          : Disabled
Flooding Port   :

DGS-3426:5#
```

config lacp_port

Purpose	Used to configure settings for LACP compliant ports.
Syntax	**config lacp_port <portlist> mode [active | passive]**
Description	This command is used to configure ports that have been previously designated as LACP ports (see **create link_aggregation**).
Parameters	*<portlist>* – Specifies a port or range of ports to be configured. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3–2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. *mode* – Select the mode to determine if LACP ports will process LACP control frames. • *active* – Active LACP ports are capable of processing and sending LACP control frames. This allows LACP compliant devices to negotiate the aggregated link so the group may be changed dynamically as needs require. In order to utilize the ability to change an aggregated port group, that is, to add or subtract ports from the group, at least one of the participating devices must designate LACP ports as active. Both devices must support LACP. • *passive* – LACP ports that are designated as passive can only process LACP control frames and cannot actively send these frames. In order to allow the linked port group to negotiate adjustments and make changes dynamically, at one end of the connection must have “active” LACP ports (see above).
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure LACP port mode settings:

```
DGS-3426:5#config lacp_port 1:1-1:12 mode active
Command: config lacp_port 1:1-1:12 mode active

Success.

DGS-3426:5#
```

show lacp_port	
Purpose	Used to display current LACP port mode settings.
Syntax	**show lacp_port {<portlist>}**
Description	This command is used to display the LACP mode settings as they are currently configured.
Parameters	*<portlist>* – Specifies a port or range of ports to be displayed. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3–2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. Non–contiguous portlist entries are separated by a comma. (ex: 1:1–1:3,1:7–1:9) If no parameter is specified, the system will display the current LACP status for all ports.
Restrictions	None.

Example usage:

To display LACP port mode settings:

```
DGS-3426:5#show lacp_port 1:1-1:10
Command: show lacp_port 1:1-1:10

Port     Activity
---- - -     --------
1:1          Active
1:2          Active
1:3          Active
1:4          Active
1:5          Active
1:6          Active
1:7          Active
1:8          Active
1:9          Active
1:10         Active

DGS-3426:5#
```

19

IP–MAC-PORT BINDING (IMPB) COMMANDS

The IP network layer uses a four–byte IP address. The Ethernet link layer uses a six–byte MAC address. Binding these two address types together allows the transmission of data between the layers. The primary purpose of IP–MAC-Port Binding is to restrict the access to a switch to a number of authorized users. Only the authorized client can access the Switch’s port by checking the pair of IP–MAC addresses with the pre–configured white list. 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 xStack® DGS–3400 Series, the maximum number of IP–MAC-Port Binding entries is 511. The creation of authorized IP-MAC pairs can be manually configured by CLI or Web, or can be leaned automatically when DHCP snooping is enabled. The function is port–based, meaning a user can enable or disable the function on the individual port.

ACL Mode

Due to some special cases that have arisen with the IP–MAC-Port Binding, this Switch has been equipped with a special ACL Mode for IP–MAC-Port Binding. 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 window. All others will be discarded. The function is port–based, meaning a user can enable or disable the function on the individual port.

To configure the ACL mode, the user must first set up IP-MAC-Port binding using the **create address_binding ip_mac ipaddress** command to create an entry. Then the user must enable the mode by entering the **config address_binding ports <portlist> mode acl** command.

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 manual.

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]}
config address_binding ip_mac ipaddress	<ipaddr> mac_address <macaddr> {ports [<portlist> | all]}
config address_binding ip_mac ports	[<portlist>| all] {state [enable {[strict | loose]} | disable] |allow_zeroip [enable | disable] |forward_dhcppkt [enable | disable] |mode [arp | acl] |stop_learning_threshold <value 0-500>} (1)
show address_binding	[ip_mac {[all | ipaddress <ipaddr> mac_address <macaddr>]} | blocked {[all | vlan_name <vlan_name> mac_address <macaddr>]} | ports <portlist>]}
delete address_binding	[ip_mac [ipaddress <ipaddr> mac_address <macaddr> | all] | blocked [all | vlan_name <vlan_name> mac_address <macaddr>]]
enable address_binding trap_log	
disable address_binding trap_log	
debug address_ binding	[event | dhcp |all]
no debug address_binding	
enable address_binding dhcp_snoop	
disable address_binding dhcp_snoop	
clear address_binding dhcp_snoop binding_entry	ports [<portlist>|all]
show address_binding dhcp_snoop	{[max_entry { ports <portlist>} | binding_entry {port <port>}]}
config address_binding dhcp_snoop max_entry ports	[<portlist> | all] limit [<value 1-50> | no_limit]
config address_binding recover_learning ports	[<portlist> | all]

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 in the white list.
Syntax	**create address_binding ip_mac ipaddress <ipaddr> mac_address <macaddr> {ports [<portlist> | all]}**
Description	This command is used to create an IP–MAC-Port Binding entry.
Parameters	*<ipaddr>* – The IP address of the device where the IP–MAC-Port Binding is made. *<macaddr>* – The MAC address of the device where the IP–MAC-Port binding is made. *<portlist>* – Specifies a port or range of ports to be configured for address binding. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3–2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. Non–contiguous portlist entries are separated by a comma. (ex: 1:1–1:3,1:7–1:9) *all* – Specifies that all ports on the switch will be configured for address binding.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create address binding on the Switch:

```
DGS-3426:5#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-3426:5#
```

Once an entry has been created and some IMPB-enabled ports (ACL mode) belong to this entry, the access profile table will look like this:

```
DGS-3426:5#show access_profile
Command: show access_profile

Access Profile Table

Total Unused Rule Entries:767
Total Used Rule Entries  :1

Access Profile ID: 1                                         Type : Ethernet
================================================================================
Owner       : IP-MAC-PORT Binding
MASK Option :
Ethernet type
-------------

Access ID : 1              Mode: Deny
Ports: 2:16
-------------
0x800
================================================================================
Unused Entries: 127

DGS-3426:5#
```

The **show access_profile** command will display the two access profiles created and their corresponding rules for every port on the Switch.

config address_binding ip_mac ipaddress	
Purpose	Used to configure an IP–MAC-Port Binding entry.
Syntax	**config address_binding ip_mac ipaddress <ipaddr> mac_address <macaddr> {ports [<portlist> | all]}**
Description	This command is used to configure an IP–MAC-Port Binding entry.
Parameters	*<ipaddr>* – The IP address of the device where the IP–MAC-Port binding is made. *<macaddr>* – The MAC address of the device where the IP–MAC-Port binding is made. *ports [<portlist>* | *all]* – Used to specify the ports where the IP–MAC-Port binding entry applies. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3–2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. Non–contiguous portlist entries are separated by a comma. (ex: 1:1–1:3,1:7–1:9) *all* – Specifies that all ports on the switch will be configured for address binding.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure address binding on the Switch:

```
DGS-3426:5#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-3426:5#
```

config address_binding ip_mac ports	
Purpose	Used to configure IMPB settings for specified ports.
Syntax	**config address_binding ip_mac ports [<portlist>| all] {state [enable {[strict | loose]} | disable] |allow_zeroip [enable | disable] |forward_dhcppkt [enable | disable] |mode [arp | acl] |stop_learning_threshold <value 0-500>} (1)**
Description	This command is used to configure the per-port state of IP-MAC binding on the Switch. If a port has been configured as a group member of an aggregated link, then it cannot enable the IP-MAC binding function. When IMPB is enabled on a port, IP packets and/or ARP packets received by this port will be checked depending on the setting. The packet will be dropped if its IP-MAC pair does not match the IMPB white list. IMPB allows the user to choose either ARP or ACL mode. In ARP Mode, a switch performs ARP Packet Inspection in which it checks the IP-MAC pairs in ARP packets with the IMPB white list and denies unauthorized ones. An advantage of ARP mode is that it does not consume any ACL rules on the Switch. Nonetheless, since the switch only checks ARP packets, it cannot block unauthorized clients who do not send out ARP packets. In ACL Mode, a switch performs IP Packet Inspection in addition to ARP Packet Inspection. ACL rules will be used to permit statically configured IMPB entries and deny other IP packets with the incorrect IP-MAC pairs. The distinct advantage of ACL Mode is that it ensures better security by checking both ARP Packets and IP Packets. However, doing so requires the use of ACL rules. ACL Mode can be viewed as an enhanced version of ARP Mode because ARP Mode is enabled by default when ACL Mode is selected. There are also two port states: Strict and Loose, and only one state can be selected per port. If a port is set to Strict state, all packets sent to the port are denied (dropped) by default. The Switch will continuously compare all IP and ARP packets it receives on that

config address_binding ip_mac ports	
	port with its IMPB entries. If the IP-MAC pair in the packet matches the IMPB entry, the MAC address will be unblocked and subsequent packets sent from this client will be forwarded. On the other hand, if a port is set to Loose state, all packets entering the port are permitted (forwarded) by default. The Switch will continuously compare all ARP packets it receives on that port with its IMPB entries. If the IP-MAC pair in the ARP packet does not match the IMPB white list, the MAC address will be blocked and subsequent packets sent from this client will be dropped.
Parameters	*state* – Configures the address binding port state to enable or disable. When the state is enabled, the port will perform the binding check. *strict* – This state provides a stricter method of control. If the user selects this mode, all packets are blocked by the Switch by default. The Switch will compare all incoming ARP and IP Packets and attempt to match them against the IMPB white list. If the IP-MAC pair matches the white list entry, the packets from that MAC address are unblocked. If not, the MAC address will stay blocked. While the Strict state uses more CPU resources from checking every incoming ARP and IP packet, it enforces better security and is thus the recommended setting. The packet isn't found by the entry, the MAC will be set to block. Other packets will be dropped. The default mode is strict if not specified. *loose* – This mode provides a looser way of control. If the user selects loose mode, the Switch will forward all packets by default. However, it will still inspect incoming ARP packets and compare them with the Switch's IMPB white list entries. If the IP-MAC pair of a packet is not found in the white list, the Switch will block the MAC address. A major benefit of Loose state is that it uses less CPU resources because the Switch only checks incoming ARP packets. However, it also means that Loose state cannot block users who send only unicast IP packets. An example of this is that a malicious user can perform DoS attacks by statically configuring the ARP table on their PC. In this case, the Switch cannot block such attacks because the PC will not send out ARP packets. *allow_zeroip* – Specifies whether to allow ARP packets with Source IP address 0.0.0.0. When enabled on a port, all ARP packets with a source IP address of 0.0.0.0 is forwarded; when set to disable, they are blocked. *forward_dhcppkt* – By default, the Switch will forward all DHCP packets. However, if the port state is set to Strict, all DHCP packets will be dropped. In that case, enable *forward_dhcppkt* so that the port will forward DHCP packets even under Strict state. Enabling this feature also ensures that DHCP snooping works properly. *mode* – select to port to use *ARP* mode or *ACL* mode. When a port is under ACL mode, the switch will create ACL access entry corresponding to the entries of this port. If the port mode changes to ARP, all the ACL access entries will be deleted automatically. The default mode of the port is ARP mode. *stop_learning_threshold<int>* – Enter a stop learning threshold between *0* and *500*. Entering 500 means the port will enter the stop learning state after 500 illegal MAC entries and will not allow additional MAC entries, both legal or illegal, to be learned on this port. In the stop learning state, the port will also automatically purge all blocked MAC entries on this port. Traffic from legal MAC entries are still forwarded. Entering *0* means no limit has been set and the port will keep learning illegal MAC addresses. <*portlist*> – Specifies a port or range of port to be configured. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3–2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. Non–contiguous portlist entries are separated by a comma. (ex: 1:1–1:3,1:7–1:9) *all* – Specifies all ports on the switch.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure address binding on the Switch:

```
DGS-3426:5#config address_binding ip_mac ports 1:2 state enable
Command: config address_binding ip_mac ports 1:2 state enable

Success.

DGS-3426:5#
```

show address_binding

Purpose	Used to display IP–MAC-Port Binding entries.
Syntax	**show address_binding [ip_mac {[all | ipaddress <ipaddr> mac_address <macaddr>]} | blocked {[all | vlan_name <vlan_name> mac_address <macaddr>]} | ports]**
Description	This command is used to display IP–MAC-Port Binding entries. Three different kinds of information can be viewed. • *ip_mac* – Address Binding entries can be viewed by entering the MAC and IP addresses of the device. • *blocked* – Blocked address binding entries (bindings between VLAN names and MAC addresses) can be viewed by entering the VLAN name and the MAC address of the device. • *ports* – Specifies a port or range of ports to be displayed information.
Parameters	*all* – Displays all IP-MAC-Port binding entries; for Blocked Address Binding entries, *all* specifies all the blocked VLANs and their bound MAC addresses. *<ipaddr>* – The IP address of the device where the IP–MAC-Port binding is made. *<macaddr>* – The MAC address of the device where the IP–MAC-Port binding is made. *<vlan_name>* – The VLAN name of the VLAN that is bound to a MAC address in order to block a specific device on a known VLAN.
Restrictions	None.

Example usage:

To display IP–MAC-Port Binding on the Switch:

```
DGS-3426:5#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


IP Address     MAC Address             Mode         Ports
------------   ---------------      ----------   --------------
10.1.1.8       00-00-00-00-00-12       Static         1:1-1:24

Total entries : 1

DGS-3426:5#
```

delete address_binding

Purpose	Used to delete IP–MAC-Port Binding entries.
Syntax	**delete address_binding [ip_mac [ipaddress <ipaddr> {mac_address <macaddr>} | all] | blocked [all | vlan_name <vlan_name> mac_address <macaddr>]]**
Description	This command is used to delete IP–MAC-Port Binding entries. Two different kinds of information can be deleted. • *ip_mac* – Individual Address Binding entries can be deleted by entering the MAC and IP addresses of the device. Toggling to *all* will delete all the Address Binding entries. • *blocked* – Blocked address binding entries (bindings between VLAN names and MAC addresses) can be deleted by entering the VLAN name and the MAC address of the device. To delete all the Blocked Address Binding entries, toggle *all.*
Parameters	<*ipaddr*> – The IP address of the device where the IP–MAC-Port Binding is made. <*macaddr*> – The MAC address of the device where the IP–MAC-Port Binding is made. <*vlan_name*> – The VLAN name of the VLAN that is bound to a MAC address in order to block a specific device on a known VLAN. *all* – For IP-MAC-Port Binding *all* specifies all the IP–MAC-Port Binding entries; for Blocked Address Binding entries *all* specifies all the blocked VLANs and their bound physical addresses.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete an IP–MAC-Port Binding entry on the Switch:

```
DGS-3426:5#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-3426:5#
```

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 IMPB. When enabled, the Switch will send a trap/log message when an ARP packet is received that doesn’t match the IMPB white list.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable the sending of IP–MAC-Port Binding trap/log messages on the Switch:

```
DGS-3426:5#enable address_binding trap_log
Command: enable address_binding trap_log

Success.

DGS-3426:5#
```

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 IMPB. When disabled, the Switch will not send trap/log messages.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable the sending of IP–MAC-Port Binding trap/log messages on the Switch:

```
DGS-3426:5#disable address_binding trap_log
Command: disable address_binding trap_log

Success.

DGS-3426:5#
```

debug address_binding

Purpose	Used to configure the address binding debugging feature on the Switch.
Syntax	**debug address_binding [event | dhcp | all]**
Description	This command is used to configure the IPMB debugging feature. The debugging feature is disabled by default.
Parameters	*event* – The Switch will print out the debug messages when an IMPB module receives ARP/IP packets. *dhcp* –The Switch will print out the debug messages when the IMPB module receives the DHCP packets. *all* –The Switch will print out all debugging messages.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable debugging of IMP IP packets:

```
DGS-3426:5#debug address_binding event
Command: debug address_binding event

Success.

DGS-3426:5#
```

no debug address_binding

Purpose	Used to disable IMPB debugging on the Switch.
Syntax	**no debug address_binding**
Description	This command is used to disable IMPB debugging on the Switch.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To disable IMPB debugging on the Switch:

```
DGS-3426:5#no debug address_binding
Command: no debug address_binding

Success.


DGS-3426:5#
```

enable address_binding dhcp_snoop

Purpose	To enable the DHCP snooping option for IMPB.
Syntax	**enable address_binding dhcp_snoop**
Description	If DHCP snooping is enabled, the Switch learns IP-MAC pairs by snooping DHCP packets automatically and then saves them to the IP-MAC-Port Binding white list. This enables a hassle-free configuration because the administrator does not need to manually enter each IMPB entry. A prerequisite for this is that the valid DHCP server's IP-MAC pair must be configured on the Switch's IMPB while list first; otherwise the DHCP server packets will be dropped. DHCP snooping is generally considered to be more secure because it enforces all clients to acquire IP through the DHCP server. Additionally, it makes IP Information auditable because clients cannot manually configure their own IP address. Each DHCP-snooped entry is associated with a lease time. When the lease time expires, the expired entry will be removed from this port. The auto-learned binding entry can be moved from one port to another port if the DHCP snooping function has learned that the MAC address is moved to a different port. In order to avoid conflict where both static entry and DHCP Snooping entry are the same, DHCP Snooping entries will not be created if the IP-MAC entry has already been statically configured.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable the address binding auto mode:

```
DGS-3426:5#enable address_binding dhcp_snoop
Command: enable address_binding dhcp_snoop

Success.

DGS-3426:5#
```

disable address_binding dhcp_snoop

Purpose	To disable the DHCP snooping option for IMPB.
Syntax	**disable address_binding dhcp_snoop**
Description	When the DHCP snoop function is disabled, all of the auto-learned binding entries will be removed.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable the address binding auto mode:

```
DGS-3426:5#disable address_binding dhcp_snoop
Command: disable address_binding dhcp_snoop

Success.

DGS-3426:5#
```

clear address_binding dhcp_snoop binding_entry

Purpose	This command is used to clear DHCP-snooped entries on specified ports.
Syntax	**clear address_binding dhcp_snoop binding_entry ports [<portlist> | all]**
Description	This command is used to clear the DHCP-snooped entries learned for the specified ports.
Parameters	*ports* – Specifies the list of ports on which to cleare the DHCP snoop learned entry.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To clear address binding auto mode:

```
DGS-3426:5#clear address_binding dhcp_snoop binding_entry ports 1-3
Command: clear address_binding dhcp_snoop binding_entry ports 1:1-1:3

Success.

DGS-3426:5#
```

show address_binding dhcp_snoop

Purpose	To show DHCP-snooped entries on the Switch.
Syntax	**show address_binding dhcp_snoop {[max_entry { ports <portlist>} | binding_entry {port <port>}]}**
Description	This command is used to display all DHCP snooping entries.
Parameters	*ports* – Specifies the list of ports to be displayed from the DHCP snoop learned entry.
Restrictions	None.

Example usage:

To display address binding DHCP snooping:

```
DGS-3426:5#show address_binding dhcp_snoop
Command: show address_binding dhcp_snoop

DHCP_Snoop : Enabled

DGS-3426:5#
```

To display an address binding DHCP snoop binding entry:

Note: “Inactive” indicated that the entry is currently inactive due to port link down.

```
DGS-3426:5#show address_binding dhcp_snoop binding_entry
Command: show address_binding dhcp_snoop binding_entry

IP Address       MAC Address                Lease Time(secs)     Port       Status
--------------   --------------------      ----------------     --------   ---------
10.62.58.35     00-0B-5D-05-34-0B        35964               1         Active
10.33.53.82     00-20-c3-56-b2-ef        2590                2         Inactive

Total entries : 2

DGS-3426:5#
```

To display the address_binding dhcp_snoop max_entry.

```
DGS-3426:5# show address_binding dhcp_snoop max_entry
Command: show address_binding dhcp_snoop max_entry

Port  Max Entry
----  ---------
1:1   no_limit
1:2   no_limit
1:3   no_limit
1:4   no_limit
1:5   no_limit
1:6   no_limit
1:7   no_limit
1:8   no_limit
1:9   no_limit
1:10  no_limit
1:11  no_limit
1:12  no_limit
1:13  no_limit
1:14  no_limit
1:15  no_limit
1:16  no_limit
1:17  no_limit
1:18  no_limit
1:19  no_limit
1:20  no_limit

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

config address_binding dhcp_snoop max_entry ports

Purpose	Specifies the maximum number of entries which can be dynamically learned (DHCP snooped) by the specified ports.
Syntax	**config address_binding dhcp_snoop max_entry ports [<portlist> | all] limit [<value 1-50> | no_limit]**
Description	This command is used to specify the maximum number of DHCP snooping entries on specified ports. By default, the per-port maximum entry has no limit.
Parameters	*portlist* – Specifies the list of ports to be configured for the DHCP snoop maximum learned entry.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To set the maximum number of entries that ports 1-23 can learn to 10:

```
DGS-3426:5#config address_binding dhcp_snoop max_entry ports 1-3 limit 10
Command: config address_binding dhcp_snoop max_entry ports 1:1-1:3 limit 10

Success.

DGS-3426:5#
```

config address_binding recover_learning ports

Purpose	To recover a port from the stop learning state to the normal state.
Syntax	**config address_binding recover_learning ports [<portlist> | all]**
Description	This command is used to recover the port back to normal state, under which the port will start learning both illegal and legal MAC addresses again.
Parameters	*portlist* – Specifies the list of ports to recover from stopped learning mode..
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure address binding recover learning ports:

```
DGS-3426:5#config address_binding recover_learning ports 6-7
Command: config address_binding recover_learning ports 1:6-1:7

Success.

DGS-3426:5#
```

20

IP COMMANDS (INCLUDING IPV6)

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

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

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

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> {state [enable | disable]}**
Description	This command is used to create an IP interface.
Parameters	*<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. *<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). *<vlan_name 32>* – The name of the VLAN that will be associated with the above IP interface. *state [enable | disable]* – Allows the user to enable or disable the IP interface.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create the IP interface, p1 on VLAN Tiberius:

```
DGS-3426:5#create ipif p1 10.1.1.1/8 Tiberius state enable
Command: create ipif p1 10.1.1.1/8 Tiberius state enable

Success.

DGS-3426:5#
```

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]} (1) | 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	*<ipif_name 12>* – Enter an alphanumeric string of up to 12 characters to identify this IP interface. *ipaddress <network_address>* – IP address and netmask of the IP interface to be created. Users can specify the address and mask information using the traditional format (for example, 10.1.2.3/255.0.0.0 or in CIDR format, 10.1.2.3/8). Only one IPv4 address can be configured per interface. *<vlan_name 32>* – The name of the VLAN corresponding to the IP interface. *state [enable | disable]* – Allows users to enable or disable the IP interface. *bootp* – Allows the selection of the BOOTP protocol for the assignment of an IP address to the Switch's System IP interface. 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. *dhcp* – Allows the selection of the DHCP protocol for the assignment 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 and Operator-level users can issue this command.

Example usage:

To configure the IPv4 interface System:

```
DGS-3426:5#config ipif System ipaddress 10.48.74.122/8
Command: config ipif System ipaddress 10.48.74.122/8

Success.

DGS-3426:5#
```

Example usage:

To configure the IPv6 address for IP interface Tiberius:

```
DGS-3426:5#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-3426:5#
```

show ipif

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

Example usage:

To display IP interface settings:

```
DGS-3426:5#show ipif System
Command: show ipif System

Interface Name              : System
VLAN Name                   : default
Interface Admin State       : Enabled
IPv4 Address                : 10.48.74.122/8    (MANUAL)
IPv6 Link-Local Address     : FE80::217:9AFF:FEBA:72CB/128

Interface Name              : Zira
VLAN Name                   : Tiberius
Interface Admin State       : Enabled
 IPv4 Address               : 0.0.0.0/0    (MANUAL)
 IPv6 Link-Local Address    : FE80::217:9AFF:FEBA:72CB/128
 IPv6 Global Unicast Address : 3FFE:501:FFFF:100::1/64

Total Entries : 2

DGS-3426:5#
```

enable ipif

Purpose	Used to enable an IP interface on the Switch.
Syntax	**enable ipif {<ipif_name 12> | all}**
Description	This command is used to enable the IP interface function on the Switch.
Parameters	*<ipif_name 12>* – The name of a previously configured IP interface to enable. Enter an alphanumeric entry of up to twelve characters to define the IP interface. *all* – Entering this parameter will enable all the IP interfaces currently configured on the Switch.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable the IPIF function on the Switch:

```
DGS-3426:5#enable ipif s2
Command: enable ipif s2

Success.

DGS-3426:5#
```

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 is used to 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. *all* – Entering this parameter will disable all the IP interfaces currently configured on the Switch.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable the IP interface named "s2":

```
DGS-3426:5#disable ipif s2
Command: disable ipif s2

Success.

DGS-3426:5#
```

delete ipif

Purpose	Used to delete the configuration of an IP interface on the Switch.
Syntax	**delete ipif {<ipif_name 12> | 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. *all* – Entering this parameter will delete all the IP interfaces currently configured on the Switch.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete the IP interface named s2:

```
DGS-3426:5#delete ipif s2
Command: delete ipif s2

Success.

DGS-3426:5#
```

enable autoconfig

Purpose	Used to activate the auto-configuration function for the Switch. This will load a configuration file for current use.
Syntax	**enable autoconfig**
Description	When auto-configuration 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 auto-configuration 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.

Example usage:

To enable auto-configuration on the Switch:

```
DGS-3426:5#enable autoconfig
Command: enable autoconfig

Success.

DGS-3426:5#
```

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

disable autoconfig

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

Example usage:

To disable the auto-configuration function: .

```
DGS-3426:5#disable autoconfig
Command:disable autoconfig

Success.

DGS-3426:5#
```

show autoconfig

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

Example usage:

To display the auto-configuration status:

```
DGS-3426:5#show autoconfig
Command: show autoconfig

Autoconfig State: Disabled

DGS-3426:5#
```

enable ipif_ipv6_link_local_auto

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

Example usage:

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

```
DGS-3426:5#enable ipif_ipv6_link_local_auto all
Command: enable ipif_ipv6_link_local_auto all

Success.

DGS-3426:5#
```

disable ipif_ipv6_link_local_auto

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

Example usage:

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

```
DGS-3426:5#disable ipif_ipv6_link_local_auto System
Command: disable ipif_ipv6_link_local_auto System

Success.

DGS-3426:5#
```

show ipif_ipv6_link_local_auto

Purpose	Displays the link local address automatic configuration state.
Syntax	**show ipif_ipv6_link_local_auto {<ipif_name 12>}**
Description	This command is used to display the link local address automatic configuration state.
Parameters	*<ipif_name 12>* – The name created for the IP interface.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To display the link local address automatic configuration state:

```
DGS-3426:5#show ipif_ipv6_link_local_auto
Command: show ipif_ipv6_link_local_auto

 IPIF: System     Automatic Link Local Address: Disabled

DGS-3426:5#
```

21

IPv6 Neighbor Discovery 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 Discovery 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>} (1)
config ipv6 nd ra prefix_option ipif	<ipif_name 12> <ipv6networkaddr> {preferred_life_time <uint 0–4294967295> | valid_life_time <value 0–4294967295> | on_link_flag [enable | disable] | autonomus_flag [enable | disable]} (1)
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	*<ipif_name 12>* – Enter the IPv6 interface name previously created using the **create ipif** and **config ipif** commands. *<ipv6addr>* – Enter the IPv6 address of the neighbor device to be added as an IPv6 neighbor of the IP interface previously entered in this command. *<macaddr>* – Enter the MAC address of the neighbor device to be added as an IPv6 neighbor of the IP interface previously entered in this command.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create a static IPv6 neighbor:

```
DGS-3426:5#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-3426:5#
```

delete ipv6 neighbor_cache ipif

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

Example usage:

To delete a static IPv6 neighbor:

```
DGS-3426:5# delete ipv6 neighbor_cache 3FFC::1
Command: delete ipv6 neighbor_cache 3FFC::1

Success.

DGS-3426:5#
```

show ipv6 neighbor_cache ipif

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

Example usage:

To display the IPv6 neighbors of a configured IP interface:

```
DGS-3426:5# show ipv6 neighbor_cache ipif Triton
Command: show ipv6 neighbor_cache ipif Triton

Neighbor                       Linklayer Address     Interface        State
FE80::20B:6AFF:FECF:7EC6      00:0B:6A:CF:7E:C6      Triton             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-3426:5#
```

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>} (1)**
Description	This command is used to configure the settings for router advertisement packets being sent from the switch.
Parameters	*<ipif_name 12>* – Enter the IPv6 interface name that will be dispatching these router advertisements. *state {enable* | *disable}* – Use this parameter to enable or disable the sending of router advertisement packets from the IPv6 interface name previously stated. *life_time <value 0–9000>* – 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. *reachable_time <value 0–3600000>* – 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 36000000 milliseconds with a default setting of 1200000 milliseconds. A very low value is not recommended. *retrans_time <uint 0–4294967295>* – 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. *hop_limit <value 0–255>* – 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 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 then 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 and Operator-level users can issue this command.

Example usage:

To configure the parameters for the Router Advertisements:

```
DGS-3426:5#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-3426:5#
```

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 <value 0–4294967295> | on_link_flag [enable | disable] | autonomus_flag [enable | disable]} (1)**
Description	This command is used to 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	*<ipif_name 12>* – Enter the IPv6 interface name that will be dispatching these router advertisements. *<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. *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 <value 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 and Operator-level users can issue this command.

Example usage:

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

```
DGS-3426:5#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
autonomous_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
autonomous_flag enable


Success.

DGS-3426:5#
```

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 <uint 0–4294967295>**
Description	This command is used to 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 seconds 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 and Operator-level users can issue this command.

Example usage:

To configure IPv6 ND Neighbor Soliciatation messages:

```
DGS-3426:5# config ipv6 nd ns ipif Zira retrans_time 1000000
Command: config ipv6 nd ns ipif Zira retrans_time 1000000

Success.

DGS-3426:5#
```

show ipv6 nd

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

Example usage:

To display the neighbor detection parameters for IPv6:

```
DGS-3426:5#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-3426:5#
```

22

IGMP SNOOPING COMMANDS

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

Command	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] | report_suppression [enable | disable]} (1)
config igmp_snooping querier	[vlan <vlan_name 32> |all] { query_interval <sec 1-65535> | max_respons e_time <sec 1-25> | robustness_variable <value 1-255> | last_member_query_interval <sec 1-25> | state [enable|disable] |version <value 1-3>} (1)
create igmp_snooping static_group	[vlan <vlan_name 32> | vlanid <vidlist>] <ipaddr>
config igmp_snooping static_group	[vlan <vlan_name 32> | vlanid <vidlist>] <ipaddr> [add | delete] <portlist>
delete igmp_snooping static_group	[vlan <vlan_name 32> | vlanid <vidlist>] <ipaddr>
show igmp_snooping static_group	{[vlan <vlan_name 32>| vlanid <vidlist>] < ipaddr >}
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]}

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] | report_suppression [enable | disable]} (1)**
Description	This command is used to configure IGMP snooping on the Switch.
Parameters	*vlan <vlan_name 32>* – The name of the VLAN for which IGMP snooping is to be configured. *host_timeout <sec 1–16711450>* – 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. **Note:** This parameter is configurable, but will not take effect. The parameter remains in order to be compatible with the older version of the CLI. *router_timeout <sec 1–16711450>* – Specifies the maximum amount of time a route can be a member of a multicast group without the Switch receiving a host membership report. The default is 260 seconds. **Note:** This parameter is configurable, but will not take effect. The parameter remains in order to be compatible with the older version of the CLI. *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. **Note:** This parameter is configurable, but will not take effect. The parameter remains in order to be compatible with the older version of the CLI. *state [enable | disable]* – Allows users 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. *report_suppression [enable|disable]* – This parameter allows the user to disable or enable the report suppression function. When report suppression is enabled, the Switch sends the first IGMP report from all hosts for a group to all the multicast routers. The Switch does not send the remaining IGMP reports for the group to the multicast routers. This feature prevents duplicate reports from being sent to the multicast devices.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure IGMP snooping:

```
DGS-3426:5# config igmp_snooping vlan default host_timeout 250 state enable
Command: config igmp_snooping vlan default host_timeout 250 state enable

Success.

DGS-3426:5#
```

config igmp_snooping querier

Purpose	Used to configure the 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] |version <value 1-3>} (1)**
Description	This command is 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	*vlan <vlan_name 32>* – The name of the VLAN for which IGMP snooping querier is to be configured. *query_interval <sec 1–65535>* – Specifies the amount of time in seconds between general query transmissions. The default setting is 125 seconds. *max_response_time <sec 1–25>* – Specifies the maximum time in seconds to wait for reports from members. The default setting is 10 seconds. *robustness_variable <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: • Group member interval—Amount of time that must pass before a multicast router decides there are no more members of a group on a network. This interval is calculated as follows: (robustness variable x query interval) + (1 x query response interval). • Other querier present interval—Amount of time that must pass before a multicast router decides that there is no longer another multicast router that is the querier. This interval is calculated as follows: (robustness variable x query interval) + (0.5 x query response interval). • Last member query count—Number of group–specific queries sent before the router assumes there are no local members of a group. The default number is the value of the robustness variable. • By default, the robustness variable is set to 2. You might want to increase this value if you expect a subnet to be lossy. Although 1 is specified as a valid entry, the roubustness 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. *version <value 1-3>* – Configure the IGMP version of the query packet which will be sent by the router.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the IGMP snooping querier:

```
DGS-3426:5#config igmp_snooping querier vlan default query_interval 123 version
3
Command: config igmp_snooping querier vlan default query_interval 123 version 3

Success.

DGS-3426:5#
```

create igmp_snooping static_group

Purpose	Used to create IGMP snooping static group information on the Switch.
Syntax	**create igmp_snooping static_group [vlan <vlan_name 32> | vlanid <vidlist>] <ipaddr>**
Description	This command allows the creation of an IGMP snooping static group. Member ports can be added to the static group. The static member and the dynamic member port form the member ports of a group. The static group will only take effect when IGMP snooping is enabled on the VLAN. For those static member ports, the device needs to emulate the IGMP protocol operation to the querier, and forward the traffic destined to the multicast group to the member ports. For a layer 3 device, the device is also responsible to route the packet destined for this specific group to static member ports. The static member port will only affect V2 IGMP operation. The Reserved IP multicast address 224.0.0.X must be excluded from the configured group. The VLAN must be created first before a static group can be created.
Parameters	*vlan <vlan_name 32>* – The name of the VLAN for which to create IGMP snooping static group information. *vlanid < vidlist >* – The list of the VLAN IDs for which to create IGMP snooping static group information. *<ipaddr>* – The static group address for which to create IGMP snooping static group information.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create a static group 226.1.1.1 for VID 1:

```
DGS-3426:5#create igmp_snooping static_group vlanid 1 226.1.1.1
Command: create igmp_snooping static_group vlanid 1 226.1.1.1

Success.

DGS-3426:5#
```

config igmp_snooping static_group

Purpose	Used to configure the current IGMP snooping static group on the Switch.
Syntax	**config igmp_snooping static_group [vlan <vlan_name 32> | vlanid <vidlist>] <ipaddr> [add | delete] <portlist>**
Description	This command is used to add or delete ports to/from the given static group.
Parameters	*vlan <vlan_name 32>* – The name of the VLAN for which to configure IGMP snooping static group information. *vlanid < vidlist >* – The list of the VLAN IDs for which to configure IGMP snooping static group information. *< ipaddr >* – The static group address for which to configure IGMP snooping static group information. *[add | delete] <portlist>* – Portlist to add or delete.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To add port 5 to static group 226.1.1.1 on VID 1:

```
DGS-3426:5#config igmp_snooping static_group vlanid 1 226.1.1.1 add 5
Command: config igmp_snooping static_group vlanid 1 226.1.1.1 add 5

Success.

DGS-3426:5#
```

delete igmp_snooping static_group

Purpose	Used to delete the current IGMP snooping static group on the Switch.
Syntax	**delete igmp_snooping static_group [vlan <vlan_name 32> | vlanid <vidlist>] <ipaddr>**
Description	This command is used to delete an IGMP snooping static group. It will not affect the IGMP snooping dynamic member ports of a group.
Parameters	*vlan <vlan_name 32>* – The name of the VLAN for which to delete IGMP snooping static group information. *vlanid < vidlist >* – The list of the VLAN IDs for which to delete IGMP snooping static group information. *<ipaddr>* – The static group address for which to delete IGMP snooping static group information.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete a static group 226.1.1.1 on VID 1:

```
DGS-3426:5#delete igmp_snooping static_group vlanid 1 226.1.1.1
Command: delete igmp_snooping static_group vlanid 1 226.1.1.1

Success.

DGS-3426:5#
```

show igmp_snooping static_group

Purpose	Used to display the current IGMP snooping static group information on the Switch.
Syntax	**show igmp_snooping static_group {[vlan <vlan_name 32>| vlanid <vidlist>] < ipaddr >}**
Description	This command is used to display the current IGMP snooping static group information on the Switch.
Parameters	*vlan <vlan_name 32>* – The name of the VLAN for which to view IGMP snooping static group information, if not specified, all static groups will be displayed. *vlanid < vidlist >* – The list of the VLAN IDs for which to view IGMP snooping static group information, if not specified, all static groups will be displayed. *< ipaddr >* – The static group address for which to view IGMP snooping static group information.
Restrictions	None.

Example usage:

To view the current IGMP snooping static group information:

```
DGS-3426:5#show igmp_snooping static_group
Command: show igmp_snooping static_group

VLAN ID/Name                   IP Address       Static Member Ports
----------------------------   --------------   ---------------
1/default                      225.1.1.1        1-3

 Total Entries : 1

DGS-3426:5#
```

config router_ports

Purpose	Used to configure ports as static router ports.
Syntax	**config router_ports <vlan_name 32> [add | delete] <portlist>**
Description	This command is used to designate a range of ports as being connected to multicast–enabled routers. This will ensure that all packets with such a router as its destination will reach the multicast–enabled router – regardless of protocol, etc.
Parameters	<*vlan_name 32*> – The name of the VLAN on which the router port resides. *add / delete* – Use these parameters to either add or delete router ports to the specified VLAN. <*portlist*> – Specifies a port or range of ports that will be configured as router ports. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3–2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. Non–contiguous portlist entries are separated by a comma. (ex: 1:1–1:3,1:7–1:9)
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To set up static router ports:

```
DGS-3426:5#config router_ports default add 1:1-1:10
Command: config router_ports default add 1:1-1:10

Success.

DGS-3426:5#
```

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 is used to designate a port or range of ports as being forbidden to multicast–enabled routers. This will ensure that multicast packets will not be forwarded to this port – regardless of protocol, etc.
Parameters	<*vlan_name 32*> – The name of the VLAN on which the router port resides. *[add* | *delete]* – Specifies whether to add or delete forbidden ports of the specified VLAN. <*portlist*> – Specifies a range of ports that will be configured as forbidden router ports. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3–2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. Non–contiguous portlist entries are separated by a comma. (ex: 1:1–1:3,1:7–1:9)
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To set up forbidden router ports:

```
DGS-3426:5#config router_ports_forbidden default add 1:2-1:10
Command: config router_ports_forbidden default add 1:2-1:10

Success.

DGS-3426:5#
```

enable igmp_snooping

Purpose	Used to enable IGMP snooping on the Switch.
Syntax	**enable igmp_snooping {forward_mcrouter_only}**
Description	This command is used to enable IGMP snooping on the Switch. If *forward_mcrouter_only* is specified, the Switch will forward all multicast traffic to the multicast router only. Otherwise, the Switch forwards all multicast traffic to any IP router.
Parameters	*forward_mcrouter_only* – 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 and Operator-level users can issue this command.

Example usage:

To enable IGMP snooping on the Switch:

```
DGS-3426:5#enable igmp_snooping
Command: enable igmp_snooping

Success.

DGS-3426:5#
```

disable igmp_snooping

Purpose	Used to disable IGMP snooping on the Switch.
Syntax	**disable igmp_snooping {forward_mcrouter_only}**
Description	This command is used to disable IGMP snooping on the Switch. IGMP snooping can be disabled only if IP multicast routing is not being used. Disabling IGMP snooping allows all IGMP and IP multicast traffic to flood within a given IP interface.
Parameters	*forward_mcrouter_only* – 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 and Operator-level users can issue this command.

Example usage:

To disable IGMP snooping on the Switch:

```
DGS-3426:5#disable igmp_snooping
Command: disable igmp_snooping

Success.

DGS-3426:5#
```

Example usage:

To disable forwarding all multicast traffic to a multicast–enabled router:

```
DGS-3426:5#disable igmp_snooping forward_mcrouter_only
Command: disable igmp_snooping forward_mcrouter_only

Success.

DGS-3426:5#
```

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 is used to display the current IGMP snooping configuration on the Switch.
Parameters	*vlan <vlan_name 32>* – The name of the VLAN for which to view the IGMP snooping configuration.
Restrictions	None.

Example usage:

To display IGMP snooping:

```
DGS-3426:5#show igmp_snooping
Command: show igmp_snooping

IGMP Snooping Global State : Enabled
 Multicast router Only      : Enabled

 VLAN  Name                 : default
 Query Interval             : 40
 Max Response Time          : 10
 Robustness Value           : 2
 Last Member Query Interval : 5
 Host Timeout               : 90
 Router Timeout             : 90
 Leave Timer                : 10
 Querier State              : Enabled
 Querier Router Behavior    : Querier
 State                      : Enabled
 Fast Leave                 : Enabled
 Report Suppression         : Disabled
 Receive Query Count        : 2220
 Send Query Count           : 2445
 Version                    : 3

Total Entries: 1

DGS-3426:5#
```

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 is used to display the router ports currently configured on the Switch.
Parameters	*vlan <vlan_name 32>* – The name of the VLAN on which the router port resides. *static* – Displays router ports that have been statically configured. *dynamic* – Displays router ports that have been dynamically configured. *forbidden* – Displays ports that are forbidden from becoming router ports.
Restrictions	None.

Example usage:

To display the router ports.

```
DGS-3426:5#show router_ports
Command: show router_ports

 VLAN Name             : default
 Static router port    :
 Dynamic router port   : 3:2
 Forbidden router port :

DGS-3426:5#
```

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 is used to display the current IGMP Snooping Group configuration setup currently configured on the Switch.
Parameters	*<vlan_name 32>* – The name of the VLAN for which to view IGMP snooping group information.
Restrictions	None.

Example usage:

To view the current IGMP snooping group:

```
DGS-3426:5#show igmp_snooping group
Command: show igmp_snooping group

 Source/Group   : NULL  / 226.1.1.1
 VLAN Name/VID  : default/1
 Port Member    : 8
 Mode           : EXCLUDE



 Total Entries : 1


DGS-3426:5#
```

23

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 a 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]} (1)
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] | version <value 1-2>} (1)
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]}

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	*forward_mcrouter_only* – 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 and Operator-level users can issue this command.

Example usage:

To enable MLD snooping globally on the Switch:

```
DGS-3426:5#enable mld_snooping
Command: enable mld_snooping

Success.

DGS-3426:5#
```

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	*forward_mcrouter_only* – 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 and Operator-level users can issue this command.

Example usage:

To disable MLD snooping globally on the Switch:

```
DGS-3426:5#disable mld_snooping
Command: disable mld_snooping

Success.

DGS-3426:5#
```

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]} (1)**
Description	This command is used to configure MLD snooping on the Switch.
Parameters	*vlan <vlan_name 32>* – The name of the VLAN for which MLD snooping is to be configured. *all* – Entering this parameter will configure MLD snooping for all VLANs on the Switch. *node_timeout <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. **Note:** This parameter is configurable, but will not take effect. The parameter remains in order to be compatible with the older version of the CLI. *router_timeout <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. **Note:** This parameter is configurable, but will not take effect. The parameter remains in order to be compatible with the older version of the CLI. *done_timer <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. **Note:** This parameter is configurable, but will not take effect. The parameter remains in order to be compatible with the older version of the CLI. *state [enable* | *disable]* – Allows users to enable or disable MLD snooping for the specified VLAN. *fast_done [enable* | *disable]* – This parameter allows the user to enable the *fast done* function. Enabled, this function will allow members of a multicast group to leave the group immediately when a *done* message is received by the Switch.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure MLD snooping:

```
DGS-3426:5#config mld_snooping vlan default node_timeout 250 state enable
Command : config mld_snooping vlan default node_timeout 250 state enable

Success.

DGS-3426:5#
```

config mld_snooping mrouter_ports

Purpose	Used to configure ports as static router ports on the Switch.
Syntax	**config mld_snooping mrouter_ports <vlan_name 32> [add | delete] <portlist>**
Description	This command is used 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	*vlan <vlan_name 32>* – The name of the VLAN on which the router port resides. *add* | *delete* – Specify to add or delete ports as router ports. *<portlist>* – Specify a port or range of ports to be configured as router ports. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3–2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. Non–contiguous portlist entries are separated by a comma. (ex: 1:1–1:3,1:7–1:9)
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure MLD snooping multicast router ports:

```
DGS-3426:5#config mld_snooping mrouter_ports default add 1:1-1:10
Command : config mld_snooping mrouter_ports default add 1:1-1:10

Success.

DGS-3426:5#
```

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 is used 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	*vlan <vlan_name 32>* – The name of the VLAN on which the router port will be forbidden. *add* | *delete* – Specify to add or delete ports as forbidden router ports. *<portlist>* – Specify a port or range of ports to be configured as forbidden router ports. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3–2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. Non–contiguous portlist entries are separated by a comma. (ex: 1:1–1:3,1:7–1:9)
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure MLD snooping forbidden multicast router ports:

```
DGS-3426:5#config mld_snooping mrouter_ports_forbidden default add 1:11-1:20
Command : config mld_snooping mrouter_ports_forbidden default add 1:11-1:20

Success

DGS-3426:5#
```

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] | version <value 1-2>} (1)**
Description	This command is used to configure the time between general query transmissions, the maximum time to wait for reports from listeners and the permitted packet loss guaranteed by MLD snooping.
Parameters	*vlan <vlan_name 32>* – The name of the VLAN for which to configure the MLD querier. *all* – Specifies all VLANs are to be configured for the MLD querier. *query_interval <sec 1–65535>* – 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. *max_response_time <sec 1–25>* – The maximum time to wait for reports from listeners. The user may specify a time between 1 and 25 seconds with a default setting of 10 seconds. *robustness_variable <value 1–255>* – Provides fine–tuning to allow for expected packet loss on a subnet. The user may choose a value between 1 and 255 with a default setting of 2. If a subnet is expected to be lossy, the user may wish to increase this interval. *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 disabled. *version <value 1-2>* – Configure the MLD version of the query packet which will be sent by the router. The default is 2.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the MLD snooping querier:

```
DGS-3426:5#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-3426:5#
```

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 is used to display the current status of the MLD snooping function on the Switch.
Parameters	*vlan <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-3426:5#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
Version                      : 2

Total Entries: 1

DGS-3426:5#
```

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 is used to display MLD snooping group configurations on the Switch.
Parameters	*vlan <vlan_name 32>* – 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-3426:5#show mld_snooping group
Command: show mld_snooping group

 Source/Group   : 2001::1         / FF1E::1
 VLAN Name/VID  : default/1
 Port Member    : 11
 Mode           : INCLUDE


 Source/Group   : 2001::2         / FF1E::1
 VLAN Name/VID  : default/1
 Port Member    : 11
 Mode           : INCLUDE


 Source/Group   : 2001::3         / FF1E::1
 VLAN Name/VID  : default/1
 Port Member    : 11
 Mode           : INCLUDE

 Total Entries : 3

DGS-3426:5#
```

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 is used to display the current router ports set on the Switch.
Parameters	*vlan <vlan_name 32>* – The name of the VLAN on which the router port resides. *static* – Displays router ports that have been statically configured. *dynamic* – Displays router ports that have been dynamically configured. *forbidden* – Displays router ports that have been configured as forbidden. If no parameter is specified, the Switch will display all currently configured router ports on the Switch.
Restrictions	None.

Example usage:

To display the MLD snooping multicast router port settings:

```
DGS-3426:5#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-3426:5#
```

24

LIMITED IP MULTICAST ADDRESS (IGMP FILTERING)

The Limited IP Multicast Address (IGMP Filtering) commands allow users to specify which multicast address(es) reports are to be received on specified ports on the switch. This function will therefore limit the number of reports received and the number of multicast groups configured on the switch. The user may set an IP address or range of IP addresses to accept reports (Permit) or deny reports (Deny) coming into the specified switch ports. The Limited IP Multicast Address 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]} (1)
delete limited multicast address	[all | <portlist>]
show limited multicast address	{<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]} (1)**
Description	This command is used to configure the multicast address range, access level, and state.
Parameters	*<portlist>* – A port or range of ports to config the limited multicast address. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3–2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. Non–contiguous portlist entries are separated by a comma. (ex: 1:1–1:3,1:7–1:9) *from <multicast_ipaddr>* – Enter the lowest multicast IP address of the range. *to <multicast_ipaddr>* – Enter the highest multicast IP address of the range. *access* – Choose either *permit* or *deny* to limit or grant access to a specified range of Multicast addresses on a particular port or range of ports. *state* – This parameter allows the user to *enable* or *disable* the limited multicast address range on a specific port or range of ports.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the limited multicast address on ports 1–3:

```
DGS-3426:5#config limited multicast address 1:1-1:3 from 224.1.1.1 to 224.1.1.2
access permit state enable
Command: config limited multicast address 1:1-1:3 from 224.1.1.1 to 224.1.1.2
access permit state enable

Success.

DGS-3426:5#
```

delete limited multicast address

Purpose	Used to delete Limited IP multicast address range.
Syntax	**delete limited multicast address [all | <portlist>]**
Description	This command is used to delete all multicast address ranges or a selected range based on which port or ports the range has been assigned.
Parameters	*all* – Allows the user to delete all limited multicast addresses that have been configured on the Switch. *<portlist>* – Allows the user to delete only those multicast address ranges that have been assigned to a particular port or range of ports. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3–2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete the limited multicast address on ports 1–3:

```
DGS-3426:5#delete limited multicast address 1:1-1:3
Command: delete limited multicast address 1:1-1:3

Success.

DGS-3426:5#
```

show limited multicast address

Purpose	Used to show per – port Limited IP multicast address range.
Syntax	**show limited multicast address {<portlist>}**
Description	This command is used to display multicast address range by ports.
Parameters	*<portlist>* – A port or range of ports on which the limited multicast address range to be shown has been assigned. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3–2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. Non–contiguous portlist entries are separated by a comma. (ex: 1:1–1:3,1:7–1:9)
Restrictions	None.

Example usage:

To display the limited multicast address on ports 1–3 of module 1:

```
DGS-3426:5#show limited multicast address 1:1-1:3
Command: show limited multicast address 1:1-1:3

Port       From            To              Access     Status
----      --------------   -------------   -------    -------
1:1        224.1.1.1       224.1.1.2       permit     enable
1:2        224.1.1.1       224.1.1.2       permit     enable
1:3        224.1.1.1       224.1.1.2       permit     enable

DGS-3426:5#
```

25

802.1X COMMANDS

The xStack® DGS–3400 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. The switch also supports 802.1X extensions, which means that as well as granting simple access rights, some controlling parameters can be passed from the authentication server to fine tune the management for the authenticated port/host.

The 802.1X commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameters
enable 802.1x	
disable 802.1x	
show 802.1x	
show 802.1x auth_state ports	{<portlist>}
show 802.1x auth_configuration ports	{<portlist>}
config 802.1x auth_protocol	[local | radius_eap]
create 802.1x user	<username 15>
delete 802.1x user	<username 15>
show 802.1x user	
show auth_statistics	{ports <portlist | all>}
show auth_diagnostics	{ports <portlist | all>}
show auth_session_statistics	{ports <portlist | all>}
show auth_client	
show acct_client	
config 802.1x capability ports	[<portlist> | all] [authenticator | none]
config 802.1x auth_parameter ports	[<portlist> | all] [default | {direction [both | in] | port_control [force_unauth | auto | force_auth] | quiet_period <sec 0-65535> | tx_period <sec 1-65535> | supp_timeout <sec 1-65535> | server_timeout <sec 1-65535> | max_req <value 1-10> | reauth_period <sec 1-65535> | max_users [<value 1-128> | no_limit] | enable_reauth [enable | disable]}] (1)
config 802.1x 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> | timeout <int 1-255> | retransmit <int 1-20>} (1)]
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 > | timeout <int 1-255> |retransmit <int 1-20>} (1)
show radius	

Command	Parameters
create 802.1x guest_vlan	<vlan_name 32>
config 802.1x guest_vlan ports	[<portlist> | all] state [enable | disable]
delete 802.1x guest_vlan	{<vlan_name 32>}
show 802.1x guest_vlan	
config 802.1x auth_failover	[enable | disable]
config 802.1x fwd_pdu system	[enable | disable]
config 802.1x fwd_pdu ports	[<portlist>|all] [enable | disable]
config 802.1x authorization network radius	[enable | disable]
config 802.1x max_users	[<value 1 – 4000> | no_limit]
config accounting service	[network | shell | system] state [enable | disable]
show accounting service	

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

enable 802.1x	
Purpose	Used to enable the 802.1X server on the Switch.
Syntax	**enable 802.1x**
Description	This command is used to enable the 802.1X Network Access control server application on the Switch. To select between port–based or MAC–based, use the **config 802.1x auth_mode** command.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable 802.1X switch wide:

```
DGS-3426:5#enable 802.1x
Command: enable 802.1x

Success.

DGS-3426:5#
```

disable 802.1x	
Purpose	Used to disable the 802.1X server on the Switch.
Syntax	**disable 802.1x**
Description	This command is used to disable the 802.1X Network Access control server application on the Switch. To select between port–based or MAC–based, use the **config 802.1x auth_mode** command.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable 802.1X on the Switch:

```
DGS-3426:5#disable 802.1x
Command: disable 802.1x

Success.

DGS-3426:5#
```

show 802.1x

Purpose	Used to display the 802.1X general configurations on the Switch.
Syntax	**show 802.1x**
Description	This command is used to display the 802.1X general configurations on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display the 802.1X general authentication configuration:

```
DGS-3426:5#  show 802.1x
Command: show 802.1x

802.1X                     : Enabled
Authentication Mode        : Port_based
Authentication Protocol    : RADIUS_EAP
Authentication Failover    : Enabled
Forward EAPOL PDU          : Enabled
Max Users                  : No Limit
RADIUS Authorization       : Enabled

DGS-3426:5#
```

show 802.1x auth_configuration ports	
Purpose	Used to display the current configuration of the 802.1X server on the Switch.
Syntax	**show 802.1x auth_configuration ports <portlist>**
Description	This command is used to display the 802.1X Port–based or MAC–based Network Access control local users currently configured on the Switch.
Parameters	*<portlist>* – Specifies a port or range of ports to view. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3–2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. Non–contiguous portlist entries are separated by a comma. (ex: 1:1–1:3,1:7–1:9) The following details are displayed: 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. Max _users: Specifies per port maximum number of users. The range is 1 to 128. The default value is 16. Forward EAPOL PDU On Port: Needs to be configured if the port will forward EAPOL PDU when 802.1X functionality is disabled.
Restrictions	None.

Example usage:

To display the 802.1X authentication configuration:

```
DGS-3426:5#show 802.1x auth_configuration ports 1:1
Command: show 802.1x auth_configuration ports 1:1

Port number     : 1:1
Capability      : None
AdminCrlDir     : Both
OpenCrlDir      : Both
Port Control    : Auto
QuietPeriod     : 60 sec
TxPeriod        : 30 sec
SuppTimeout     : 30 sec
ServerTimeout   : 30 sec
MaxReq          : 2 times
ReAuthPeriod    : 3600  sec
ReAuthenticate  : Disabled
Forward EAPOL PDU On Port : Disabled
Max Users On port : 16

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

show 802.1x auth_state ports

Purpose	Used to display the current authentication state of the 802.1X server on the Switch.
Syntax	**show 802.1x auth_state ports <portlist>**
Description	This 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	*<portlist>* – Specifies a port or range of ports to be viewed. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3–2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. Non–contiguous portlist entries are separated by a comma. (ex: 1:1–1:3,1:7–1:9) The following details what is displayed: Ports – Shows the physical port number on the Switch.
Restrictions	None.

Example usage:

To display the 802.1X authentication state

If port 1 is in host-based mode:

MAC 00-00-00-00-00-01 is authenticated without VLAN assigned (may be the specified target VLAN does not exist or target VLAN has not been specified at all), the ID of RX VLAN will be displayed (RX VLAN ID is 4004 in this example).

MAC 00-00-00-00-00-02 is authenticated with target VLAN assigned, the ID of target VLAN will be displayed (target VLAN ID is 1234 in this example)

MAC 00-00-00-00-00-03 failed to pass authentication, the VID field will be shown as “-” indicating that packets with SA 00-00-00-00-00-03 will be dropped no matter which VLAN these packets are from.

MAC 00-00-00-00-00-04 attempts to start authentication, the VID field will be shown as “-“ until authentication completed.

If port 2 is in port-based mode:

MAC 00-00-00-00-00-10 is the MAC which made port 2 pass authentication, MAC address is followed by “(P)” to indicate the port-based mode authentication.

If port 3 is linked_down.

Supposed that port 4 is in port-based mode:

MAC 00-00-00-00-00-20 attempts to start authentication, MAC address is followed by “(P)” to indicate the port-based mode authentication.

MAC 00-00-00-00-00-21 failed to pass authentication, MAC address is followed by “(P)” to indicate the port-based mode authentication.

Note: In port-based mode, the VLAN ID field is displayed in the same way as host-based mode.

```
DGS-3426:5# show 802.1x auth_state ports 1-4
Command: show 802.1x auth_state ports 1-4

Port MAC Address            State          VID   Assigned
                                                 Priority
---- ------------------- ------------- -------  --------
1    00-00-00-00-00-01     Authenticated   4004      3
1    00-00-00-00-00-02     Authenticated   1234      -
1    00-00-00-00-00-03     Blocked           -       -
1    00-00-00-00-00-04     Authenticating    -       -
2           -        (P)  Authenticated   1234      -
4           -        (P)  Authenticating    -       -
4           -        (P)  Blocked           -       -

Total Authenticating Hosts :2
Total Authenticated Hosts  :3

DGS-3426:5#
```

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	This command is used to enable either the port–based or MAC–based 802.1X authentication feature on the Switch.
Parameters	*[port_based* | *mac_based]* – The Switch allows users to authenticate 802.1X by either port or MAC address.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure 802.1X authentication by MAC address:

```
DGS-3426:5#config 802.1x auth_mode mac_based
Command: config 802.1x auth_mode mac_based

Success.

DGS-3426:5#
```

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]**
Description	This command has four capabilities that can be set for each port. Authenticator, Supplicant, Authenticator and Supplicant, and None.
Parameters	*<portlist>* – Specifies a port or range of ports to be configured. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3–2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. Non–contiguous portlist entries are separated by a comma. (ex: 1:1–1:3,1:7–1:9) *all* – Specifies all of the ports on the Switch. *authenticator* – A user must pass the authentication process to gain access to the network. *none* – The port is not controlled by the 802.1X functions.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure 802.1X capability on ports 1 to 10 of module 1:

```
DGS–3426:5#config 802.1x capability ports 1:1 – 1:10 authenticator
Command: config 802.1x capability ports 1:1 – 1:10 authenticator

Success.

DGS–3426:5#
```

config 802.1x auth_parameter ports

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 [<portlist> | all] [default | {direction [both | in] | port_control [force_unauth | auto | force_auth] | quiet_period <sec 0-65535> | tx_period <sec 1-65535> | supp_timeout <sec 1-65535> | server_timeout <sec 1-65535> | max_req <value 1-10> | reauth_period <sec 1-65535> | max_users [<value 1-128> | no_limit] | enable_reauth [enable | disable]}] (1)**
Description	This command is used to configure the 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	*<portlist>* – Specifies a port or range of ports to be configured. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3–2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. Non–contiguous portlist entries are separated by a comma. (ex: 1:1–1:3,1:7–1:9) *all* – Specifies all of the ports on the Switch. *default* – Returns all of the ports in the specified range to their 802.1X default settings. *direction [both* | *in]* – Determines whether a controlled port blocks communication in both the receiving and transmitting directions, or just the receiving direction. *port_control* – Configures the administrative control over the authentication process for the range of ports. The user has the following authentication options: • *force_auth* – Forces the Authenticator for the port to become authorized. Network access is allowed. • *auto* – Allows the port's status to reflect the outcome of the authentication process. • *force_unauth* – Forces the Authenticator for the port to become unauthorized. Network access 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. *max_users <value 1-128>* |*no_limit*- Specifies per port maximum number of users. The range is 1 to 128. The default value is 16. *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 and Operator-level users can issue this command.

Example usage:

To configure 802.1X authentication parameters for ports 1 to 20 on module 1:

```
DGS–3426:5#config 802.1x auth_parameter ports 1:1–1:20 direction both
Command: config 802.1x auth_parameter ports 1:1–1:20 direction both

Success.

DGS–3426:5#
```

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	This 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	*port_based* – This instructs the Switch to initialize 802.1X functions based only on the port number. Ports approved for initialization can then be specified. *mac_based* – This instructs the Switch to initialize 802.1X functions based only on the MAC address. MAC addresses approved for initialization can then be specified. *ports <portlist>* – Specifies a port or range of ports to be configured. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3–2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. Non–contiguous portlist entries are separated by a comma. (ex: 1:1–1:3,1:7–1:9) *all* – Specifies all of the ports on the Switch. *mac_address <macaddr>* – Enter the MAC address to be initialized.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To initialize the authentication state machine of all ports:

```
DGS–3426:5# config 802.1x init port_based ports all
Command: config 802.1x init port_based ports all

Success.

DGS–3426:5#
```

config 802.1x reauth	
Purpose	Used to configure the 802.1X re–authentication feature of the Switch.
Syntax	**config 802.1x reauth {port_based ports [<portlist> | all] | mac_based [ports] [<portlist> | all] {mac_address <macaddr>}]**
Description	This command is used to re–authenticate a previously authenticated device based on port number.
Parameters	*port_based* – This instructs the Switch to re–authorize 802.1X functions based only on the port number. Ports approved for re–authorization can then be specified. *mac_based* – This instructs the Switch to re–authorize 802.1X functions based only on the MAC address. MAC addresses approved for re–authorization can then be specified. *ports <portlist>* – Specifies a port or range of ports to be re–authorized. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3–2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. *all* – Specifies all of the ports on the Switch. *mac_address <macaddr>* – Enter the MAC address to be re–authorized.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure 802.1X reauthentication for ports 1:1–1:18:

```
DGS-3426:5#config 802.1x reauth port_based ports 1:1-1:18
Command: config 802.1x reauth port_based ports 1:1-1:18

Success.

DGS-3426:5#
```

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> | timeout <int 1-255> | retransmit <int 1-20>}(1)]**
Description	This command is used to configure the settings the Switch will use to communicate with a RADIUS server.
Parameters	*<server_index 1–3>* – Assigns a number to the current set of RADIUS server settings. Up to three groups of RADIUS server settings can be entered on the Switch. *<server_ip>* – The IP address of the RADIUS server. *key* – Specifies that a password and encryption key will be used between the Switch and the Radius server. *<passwd 32>* – The shared–secret key used by the RADIUS server and the Switch. Up to 32 characters can be used. *default* – Uses the default UDP port number in both the “auth_port” and “acct_port” settings. *auth_port <udp_port_number 1–65535>* – The UDP port number for authentication requests. The default is 1812. *acct_port <udp_port_number 1–65535>* – The UDP port number for accounting requests. The default is 1813. *timeout <int 1-255>* - The time in second for waiting server reply. The default is 5 seconds. *retransmit <int 1-20>* - The count for re-transmit. The default is 2.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the RADIUS server communication settings:

```
DGS-3426:5#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-3426:5#
```

config radius delete

Purpose	Used to delete a previously entered RADIUS server configuration.
Syntax	**config radius delete <server_index 1–3>**
Description	This command is used to delete a previously entered RADIUS server configuration.
Parameters	*<server_index 1–3>* – Assigns a number to the current set of RADIUS server settings. Up to three groups of RADIUS server settings can be entered on the Switch.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete previously configured RADIUS server communication settings:

```
DGS-3426:5#config radius delete 1
Command: config radius delete 1

Success.

DGS-3426:5#
```

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 >|timeout <int 1-255> |retransmit <int 1-20>}(1)**
Description	This command is used to configure the Switch’s RADIUS settings.
Parameters	*<server_index 1–3>* – Assigns a number to the current set of RADIUS server settings. Up to three groups of RADIUS server settings can be entered on the Switch. *ipaddress <server_ip>* – The IP address of the RADIUS server. *key* – Specifies that a password and encryption key will be used between the Switch and the RADIUS server. • *<passwd 32>* – The shared–secret key used by the RADIUS server and the Switch. Up to 32 characters can be used. *auth_port <udp_port_number 1–65535>* – The UDP port number for authentication requests. The default is 1812. *acct_port <udp_port_number 1–65535>* – The UDP port number for accounting requests. The default is 1813. *timeout <int 1-255>* – The time in seconds, that will wait for a reply from the server. If the corresponding global parameter is supported, by default, the value will follow the global settings. Otherwise, the default value is 5 seconds. *retransmit <int 1-20>* – The count for re-transmit. If the corresponding global parameter is supported, by default, the value will follow the global settings. Otherwise, the default value is 2.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the RADIUS settings:

```
DGS-3426:5#config radius 1 auth_port 60 retransmit 1
Command: config radius 1 auth_port 60 retransmit 1

Success.

DGS-3426:5#
```

show radius

Purpose	Used to display the current RADIUS configurations on the Switch.
Syntax	**show radius**
Description	This command is used to display the current RADIUS configurations on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display RADIUS settings on the Switch:

```
DGS-3426:5#show radius
Command: show radius

Index  IP Address       Auth-Port Acct-Port Timeout Retransmit Key
                                            (secs)
---    ---------------  --------- --------- ------- ---------- -------------
1      10.1.1.1         1812      1813      5       2          switch
1      20.1.1.1         1812      1813      4       2          swkey
1      30.1.1.1         1812      1813      5       3          dgs3426

Total Entries : 3

DGS-3426:5#
```

create 802.1x user

Purpose	Used to create a new 802.1X user.
Syntax	**create 802.1x user <username 15>**
Description	This command is used to create new 802.1X users.
Parameters	*<username 15>* – A username of up to 15 alphanumeric characters in length.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create an 802.1X user:

```
DGS-3426:5#create 802.1x user RG
Command: create 802.1x user RG

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

DGS-3426:5#
```

show 802.1x user

Purpose	Used to display the 802.1X user accounts on the Switch.
Syntax	**show 802.1x user**
Description	This 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-3426:5#show 802.1x user
Command: show 802.1x user

 Current Accounts:
 Username         Password
 --------------   --------------
 1                  123

 Total Entries:1

DGS-3426:5#
```

delete 802.1x user

Purpose	Used to delete an 802.1X user account on the Switch.
Syntax	**delete 802.1x user <username 15>**
Description	This 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 and Operator-level users can issue this command.

Example usage:

To delete 802.1X users:

```
DGS-3426:5# delete 802.1x user Rob
Command: delete 802.1x user Rob

Are you sure to delete the user?(y/n)
Success.

DGS-3426:5#
```

config 802.1x auth_protocol

Purpose	Used to configure the 802.1X authentication protocol on the Switch.
Syntax	**config 802.1x auth_protocol [local | radius_eap]**
Description	This command enables configuration of the authentication protocol.
Parameters	*[local* | *radius_eap]* – Specify the type of authentication protocol desired.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the authentication protocol on the Switch:

```
DGS-3426:5# config 802.1x auth_protocol local
Command: config 802.1x auth_protocol local

Success.

DGS-3426:5#
```

show acct_client

Purpose	Used to display the current RADIUS accounting client.
Syntax	**show acct_client**
Description	This command is used to display the current RADIUS accounting client currently configured on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To view the current RADIUS accounting client:

```
DGS-3426:5#show acct_client
Command: show acct_client

 radiusAcctClient ==>
 radiusAcctClientInvalidServerAddresses   0
 radiusAcctClientIdentifier

 radiusAuthServerEntry ==>
 radiusAccServerIndex : 1

 radiusAccServerAddress                   0.0.0.0
 radiusAccClientServerPortNumber          0
 radiusAccClientRoundTripTime             0
 radiusAccClientRequests                  0
 radiusAccClientRetransmissions           0
 radiusAccClientResponses                 0
 radiusAccClientMalformedResponses        0
 radiusAccClientBadAuthenticators         0
 radiusAccClientPendingRequests           0
 radiusAccClientTimeouts                  0
 radiusAccClientUnknownTypes              0
 radiusAccClientPacketsDropped            0

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

show auth_client

Purpose	Used to display the current RADIUS authentication client.
Syntax	**show auth_client**
Description	This command is used to display the current RADIUS authentication client currently configured on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To view the current RADIUS authentication client:

```
DGS-3426:5#show auth_client
Command: show auth_client

radiusAuthClient ==>
 radiusAuthClientInvalidServerAddresses   0
 radiusAuthClientIdentifier

 radiusAuthServerEntry ==>
 radiusAuthServerIndex :1

 radiusAuthServerAddress                  0.0.0.0
 radiusAuthClientServerPortNumber         0
 radiusAuthClientRoundTripTime            0
 radiusAuthClientAccessRequests           0
 radiusAuthClientAccessRetransmissions    0
 radiusAuthClientAccessAccepts            0
 radiusAuthClientAccessRejects            0
 radiusAuthClientAccessChallenges         0
 radiusAuthClientMalformedAccessResponses 0
 radiusAuthClientBadAuthenticators        0
 radiusAuthClientPendingRequests          0
 radiusAuthClientTimeouts                 0
 radiusAuthClientUnknownTypes             0
 radiusAuthClientPacketsDropped           0

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

show auth_diagnostics

Purpose	Used to display the current authentication diagnostics.
Syntax	**show auth_diagnostics {ports [<portlist> | all]}**
Description	This command is used to display the current authentication diagnostics of the Switch on a per port basis.
Parameters	*ports <portlist>* – Specifies a range of ports. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3–2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. Non–contiguous portlist entries are separated by a comma. (ex: 1:1–1:3,1:7–1:9) *all* – Specifies that all ports will be viewed.
Restrictions	None.

Example usage:

To display the current authentication diagnostics for port 16 of module 1:

```
DGS-3426:5#show auth_diagnostics ports 1:16
Command: show auth_diagnostics ports 1:16

 Port number : 1:16

 EntersConnecting                                        0
 EapLogoffsWhileConnecting                               0
 EntersAuthenticating                                    0
 SuccessWhileAuthenticating                              0
 TimeoutsWhileAuthenticating                             0
 FailWhileAuthenticating                                 0
 ReauthsWhileAuthenticating                              0
 EapStartsWhileAuthenticating                            0
 EapLogoffWhileAuthenticating                            0
 ReauthsWhileAuthenticated                               0
 EapStartsWhileAuthenticated                             0
 EapLogoffWhileAuthenticated                             0
 BackendResponses                                        0
 BackendAccessChallenges                                 0
 BackendOtherRequestsToSupplicant                        0
 BackendNonNakResponsesFromSupplicant                    0
 BackendAuthSuccesses                                    0
 BackendAuthFails                                        0

CTRL+C ESC q Quit SPACE n Next Page 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	This command is used to display the current authentication session statistics of the Switch on a per port basis.
Parameters	*ports <portlist>* – Specifies a range of ports. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3–2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. Non–contiguous portlist entries are separated by a comma. (ex: 1:1–1:3,1:7–1:9) *all* – Specifies that all ports will be viewed.
Restrictions	None.

Example usage:

To display the current authentication session statistics for port 16 of module 1:

```
DGS-3426:5#show auth_session_statistics ports 1:16
Command: show auth_session_statistics ports 1:16

 Port number : 1:16

 SessionOctetsRx                    0
 SessionOctetsTx                    0
 SessionFramesRx                    0
 SessionFramesTx                    0
 SessionId
 SessionAuthenticMethod    Remote Authentication Server
 SessionTime                        0
 SessionTerminateCause     SupplicantLogoff
 SessionUserName           Trinity

CTRL+C ESC q Quit SPACE n 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	This command is used to display the current authentication statistics of the Switch on a per port basis.
Parameters	*ports <portlist>* – Specifies a range of ports. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3–2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. Non–contiguous portlist entries are separated by a comma. (ex: 1:1–1:3,1:7–1:9) *all* – Specifies that all ports will be viewed.
Restrictions	None.

Example usage:

To display the current authentication statistics for port 1:16:

```
DGS-3426:5#show auth_statistics ports 1:16
Command: show auth_statistics ports 1:16

 Port number : 1:16

 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 guest_vlan

Purpose	Used to configure a pre–existing VLAN as a 802.1X Guest VLAN.
Syntax	**create 802.1x guest_vlan <vlan_name 32>**
Description	This command is used to configure a pre–defined VLAN as a 802.1X Guest VLAN. 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	*<vlan_name 32>* – Enter an alphanumeric string of no more than 32 characters to define a pre–existing VLAN as a 802.1X Guest VLAN. This VLAN must have first been created with the **create vlan** command mentioned earlier in this manual.
Restrictions	Only Administrator and Operator-level users can issue this command. Users must have already previously created a VLAN 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-3426:5#create 802.1x guest_vlan Tiberius
Command: create 802.1x guest_vlan Tiberius

Success.

DGS-3426:5#
```

config 802.1x guest_vlan ports

Purpose	Used to configure ports for a pre–existing 802.1X guest VLAN.
Syntax	**config 802.1x guest_vlan ports [<portlist> | all] state [enable | disable]**
Description	This command is used to configure ports to be enabled or disabled for the 802.1X guest VLAN.
Parameters	*<portlist>* – Specify a port or range of ports to be configured for the 802.1X Guest VLAN. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3–2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. Non–contiguous portlist entries are separated by a comma. (ex: 1:1–1:3,1:7–1:9) *all* – Specify this parameter to configure all ports for the 802.1X Guest VLAN. *state [enable | disable]* – Use these parameters to enable or disable port listed here as enabled or disabled for the 802.1X Guest VLAN.
Restrictions	Only Administrator and Operator-level users can issue this command. Users must have already previously created a VLAN 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-3426:5#config 802.1x guest_vlan ports 1:1-1:5 state enable
Command: config 802.1x guest_vlan ports 1:1-1:5 state enable

Warning! The ports are moved to Guest VLAN!

Success.

DGS-3426:5#
```

show 802.1x guest_vlan

Purpose	Used to view the configurations for a 802.1X Guest VLAN.
Syntax	**show 802.1x guest_vlan**
Description	This command is used to display the settings for the VLAN that has been enabled as an 802.1X Guest VLAN. 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 configure the configurations for a previously created 802.1X Guest VLAN.

```
DGS-3426:5#show 802.1x guest_vlan
Command: show 802.1x guest_vlan

Guest VLAN Setting
-------------------------------------------------------
Guest VLAN : Tiberius
Enable guest VLAN ports: 1:5-1:8

DGS-3426:5#
```

delete 802.1x guest_vlan

Purpose	Used to delete a 802.1X Guest VLAN.
Syntax	**delete 802.1x guest_vlan {<vlan_name 32>}**
Description	This command is used to delete an 802.1X Guest VLAN. 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	*<vlan_name 32>* – Enter the VLAN name of the Guest 802.1X VLAN to be deleted.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete a previously created 802.1X Guest VLAN.

```
DGS-3426:5#delete 802.1x guest_vlan Tiberius
Command: delete 802.1x guest_vlan Tiberius

Success.

DGS-3426:5#
```

config 802.1x auth_failover

Purpose	Used to configure 802.1X authentication failover.
Syntax	**config 802.1x auth_failover [enable | disable]**
Description	When the authentication failover is disabled, if the RADIUS servers are unreachable, the authentication will fail. When the authentication failover is enabled, if the RADIUS server's authentication is unreachable, the local database will be used to do the authentication. By default, the state is disabled.
Parameters	*enable* – Enables the protocol authentication failover. *disable* – Disables the protocol authentication failover.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the 802.1X authentication failover

```
DGS-3426:5#config 802.1x auth_failover enable
Command: config 802.1x auth_failover enable

Success.

DGS-3426:5#
```

config 802.1x fwd_pdu system

Purpose	Used to configure the forwarding of EAPOL PDU when 802.1X is disabled.
Syntax	**config 802.1x fwd_pdu system [enable | disable]**
Description	This is a global setting to control the forwarding of EAPOL PDU. When 802.1X functionality is disabled globally or disabled for a specific port, and 802.1X forward PDU is enabled both globally and for the port, a received EAPOL packet on the port will be flooded in the same VLAN to those ports. The default state is disabled.
Parameters	*enable* – Enables the 802.1X forward PDU system. *disable* – Disables the 802.1X forward PDU system.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure forwarding of EAPOL PDU:

```
DGS-3426:5#config 802.1x fwd_pdu system enable
Command: config 802.1x fwd_pdu system enable

Success.

DGS-3426:5#
```

config 802.1x fwd_pdu ports

Purpose	Used to configure the forwarding of EAPOL PDU.
Syntax	**config 802.1x fwd_pdu ports [<portlilst>| all] [enable | disable]**
Description	This command is a per port setting used to control the forwarding of EAPOL PDU. When 802.1X functionality is disabled globally or disabled for a specific port, and 802.1X forward PDU is enabled both globally and for the port, a received EAPOL packet on the port will be flooded in the same VLAN to those ports. The default state is disabled.
Parameters	*<portlist>* - Specifies a port or range of ports to be re–authorized. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3–2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 - in numerical order. *all* - Specifies all of the ports on the Switch. *enable* – Enables the 802.1X forward PDU ports. *disable* – Disables the 802.1X forward PDU ports.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure 802.1X forwarding PDU for ports:

```
DGS–3426:5#config 802.1x fwd_pdu ports 1:1-1:2 enable
Command: config 802.1x fwd_pdu ports 1:1-1:2 enable

Success.

DGS–3426:5#
```

config 802.1x authorization network radius

Purpose	The enable authorization command will enable the accepting of an authorized configuration.
Syntax	**config 802.1x authorization network radius [enable | disable]**
Description	This command is used to enable or disable the accepting of an authorized configuration. When the authorization is enabled for 802.1X's RADIUS, the authorized data assigned by the RADUIS server will be accepted if the global authorization network is enabled.
Parameters	*radius* – If specified to enable, the authorization data assigned by the RADUIS server will be accepted. The default state is enabled.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the authorized data assigned from the RADIUS server.

```
DGS–3426:5#config 802.1x authorization network radius disable
Command: config 802.1x authorization network radius disable

Success.

DGS–3426:5#
```

config 802.1x max_users

Purpose	Used to configure the max number of users that can be learned via 802.1X authentication.
Syntax	**config 802.1x max_users [<value 1 –4000> | no_limit]**
Description	The setting is a global limitation on the maximum number of users that can be learned via 802.1X authentication. In addition to the global limitation, per-port maximum users is also limited. It is specified by the **config 802.1x auth_parameter** command.
Parameters	*max _users* – Specifies the maximum number of users. By default, there is no limit on the max users.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure 802.1X maximum users:

```
DGS-3426:5#config 802.1x max_users 200
Command: config 802.1x max_users 200

Success.

DGS-3426:5#
```

config accounting service

Purpose	Used to configure the state of the specified RADIUS accounting service.
Syntax	**config accounting service [network | shell | system] state [enable|disable]**
Description	This command is used to enable or disable the specified RADIUS accounting service.
Parameters	*network* – Specifies an accounting service for 802.1X port access control. By default, the service is disabled. *shell* – Accounting service for shell events: When the user logs in or logs out of the switch (via the console, Telnet, or SSH) when timeout occurs, accounting information will be collected and sent to the RADIUS server. By default, the service is disabled. *system* – Specifies accounting service for system events: reset, reboot. By default, the service is disabled. *enable* – Enables the specified accounting service. *disable* – Disables the specified accounting service.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the accounting service:

```
DGS-3426:5#config accounting service shell state enable
Command: config accounting service shell state enable

Success.

DGS-3426:5#
```

show accounting service

Purpose	Used to show the RADIUS accounting service status on the Switch.
Syntax	**show accounting service**
Description	This command is used to display the state for RADIUS accounting service.
Parameters	None.

show accounting service	
Restrictions	None.

Example usage:

To display the accounting service:

```
DGS-3426:5#show accounting service
Command: show accounting service

Accounting State
-------------------
Network : Disabled
Shell   : Enabled
System  : Disabled

DGS-3426:5#
```

26

ACCESS CONTROL LIST (ACL) COMMANDS

The xStack® DGS–3400 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 allows establishment of a 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. To restrict traffic, users 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 6 access profiles. The rules used to define the access profiles are limited to a total of 768 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 1-6> [ethernet {vlan | source_mac <macmask 000000000000-ffffffffffff> | destination_mac <macmask 000000000000-ffffffffffff> | 802.1p | ethernet_type} (1) | ip {vlan | source_ip_mask <netmask> | destination_ip_mask <netmask> | dscp | [icmp {type | code} | igmp [type} | tcp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff> | flag_mask [all | {urg | ack | psh | rst | syn | fin}]} | udp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-xffff>} | protocol_id_mask <hex 0x0-0xff> {user_define_mask <hex 0x0-0xffffffff>}]} (1) | 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>} (1) | ipv6 {[class | flowlabel} (1) | source_ipv6_mask <ipv6mask> | destination_ipv6_mask <ipv6mask>]} (1)]
delete access_profile	[profile_id <value 1–6> | all]
config access_profile profile_id	<value 1-6> [add access_id [auto_assign | <value 1-128>] [ethernet {vlan <vlan_name 32> | source_mac <macaddr 000000000000-ffffffffffff> | destination_mac <macaddr 000000000000-ffffffffffff> | 802.1p <value 0-7> | ethernet_type <hex 0x0-0xffff>} (1) port [<portlist> | all] [permit {priority <value 0-7> {replace_priority} | rx_rate {no_limit | <value 1-156249>]} | replace_dscp <value 0-63> counter [enable | 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

Command	**Parameters**
	{src_port <value 0-65535> | dst_port <value 0-65535>} | protocol_id <value 0 - 255> {user_define <hex 0x0-0xffffffff>}]} (1) port [<portlist> | all] [permit {priority <value 0-7> {replace_priority} | rx_rate {no_limit | <value 1-156249>]} |replace_dscp <value 0-63>| 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>} (1) port [<portlist> | all] [permit {priority <value 0-7> {replace_priority} | rx_rate {no_limit | <value 1-156249>]} |replace_dscp <value 0-63> | counter [enable | disable]} | mirror | deny] | ipv6 {[{class <value 0-255> | flowlabel <hex 0x0-0xfffff> | source_ipv6 <ipv6addr> | destination_ipv6 <ipv6addr>]} (1) 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 1–6>}
enable cpu_interface_filtering	
disable cpu_interface_filtering	
create cpu access_profile	[ethernet {vlan | source_mac <macaddr 000000000000–ffffffffffff> | destination_mac <macaddr 000000000000–ffffffffffff> | ethernet_type} (1) | ip {vlan | source_ip_mask <netmask> | destination_ip_mask <netmask> | dscp | [icmp {type | code} | igmp {type} | tcp {src_port_mask <hex 0x0–0xffff> | dst_port_mask <hex 0x0–0xffff> | flag_mask [all | {urg | ack | psh | rst | syn | fin} (1)]} | udp {src_port_mask <hex 0x0–0xffff> | dst_port_mask <hex 0x0–0xffff>} | protocol_id_mask {<hex 0x0–0xff> {user_define_mask <hex 0x0–0xffffffff>}]} (1) | packet_content_mask {offset 0–15 <hex 0x0–0xffffffff> <hex 0x0–0xffffffff> <hex 0x0–0xffffffff> <hex 0x0–0xffffffff>| offset 16–31 <hex 0x0–0xffffffff> <hex 0x0–0xffffffff> <hex 0x0–0xffffffff> <hex 0x0–0xffffffff> | offset 32–47 <hex 0x0–0xffffffff> <hex 0x0–0xffffffff> <hex 0x0–0xffffffff> <hex 0x0–0xffffffff> | offset 48–63 <hex 0x0–0xffffffff> <hex 0x0–0xffffffff> <hex 0x0–0xffffffff> <hex 0x0–0xffffffff> | offset 64–79 <hex 0x0–0xffffffff> <hex 0x0–0xffffffff> <hex 0x0–0xffffffff> <hex 0x0–0xffffffff>} (1) ipv6 {[class | flowlabel] (1) | source_ipv6_mask <ipv6mask> | destination_ipv6_mask <ipv6mask>]} (1) profile_id <value 1–5>
delete cpu access_profile	[profile_id <value 1–5> | all]
config cpu access_profile	profile_id <value 1–5> [add access_id <value 1–100> [ethernet {vlan <vlan_name 32> | source_mac <macaddr 000000000000–ffffffffffff> | destination_mac <macaddr 000000000000–ffffffffffff> | ethernet_type <hex 0x0–0xffff>} (1) | 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>}]} (1) | packet_content {offset_0–15 <hex 0x0–0xffffffff> <hex 0x0–0xffffffff> <hex 0x0–0xffffffff> <hex 0x0–0xffffffff>| offset_16–31 <hex 0x0–0xffffffff> <hex 0x0–0xffffffff> <hex 0x0–0xffffffff> <hex 0x0–0xffffffff> | offset_32–47 <hex 0x0–0xffffffff> <hex 0x0–0xffffffff> <hex 0x0–0xffffffff> <hex 0x0–0xffffffff> | offset_48–63 <hex 0x0–0xffffffff> <hex 0x0–0xffffffff> <hex 0x0–0xffffffff> <hex 0x0–0xffffffff> | offset_64–79 <hex 0x0–0xffffffff> <hex 0x0–0xffffffff> <hex 0x0–0xffffffff> <hex 0x0–0xffffffff>} (1) | ipv6 {[{class <value 0-255> | flowlabel <hex 0x0-0xfffff>} (1) | source_ipv6 <ipv6addr> | destination_ipv6 <ipv6addr>]} (1)] port [<portlist> | all] [permit | deny] {time_range <range_name 32>} | delete access_id <value 1–100>]
show cpu access_profile	{profile_id <value 1–5>}

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 1–6> [ethernet {vlan | source_mac <macmask 000000000000–ffffffffffff> | destination_mac <macmask 000000000000–ffffffffffff> | 802.1p | ethernet_type} (1)**
Description	This command is used 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	*profile_id <value 1–6>* – Specifies an index number between 1 and 6 that will identify the access profile being created with this command. *ethernet* – Specifies that the Switch will examine the layer 2 part of each packet header with emphasis on one or more of the following: • *vlan* – Specifies that the Switch will examine the VLAN part of each packet header. • *source_mac <macmask>* – Specifies a MAC address mask for the source MAC address. This mask is entered in the following hexadecimal format: 000000000000–FFFFFFFFFFFF • *destination_mac <macmask>* – Specifies a MAC address mask for the destination MAC address in the following format: 000000000000–FFFFFFFFFFFF • *802.1p* – Specifies that the Switch will examine the 802.1p priority value in the frame’s header. • *ethernet_type* – Specifies that the Switch will examine the Ethernet type value in each frame’s header.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create an Ethernet access profile:

```
DGS–3426:5# create access_profile profile_id 1 ethernet vlan 802.1p
Command: create access_profile profile_id 1 ethernet vlan 802.1p

Success.

DGS–3426:5#
```

config access_profile profile_id (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	**config access_profile profile_id <value 1-6> [add access_id [auto_assign | <value 1-128> [ethernet {vlan <vlan_name 32> | source_mac <macaddr 000000000000-ffffffffffff> | destination_mac <macaddr 000000000000-ffffffffffff> | 802.1p <value 0-7> | ethernet_type <hex 0x0-0xffff>} (1) | port [<portlist> | all] [permit {priority <value 0-7> {replace_priority} | rx_rate {no_limit | <value 1-156249>]} | replace_dscp <value 0-63> | 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	*profile_id <value 1–6>* – Enter an integer between 1 and 6 that is used to identify the access profile that will be configured with this command. This value is assigned to the

config access_profile profile_id (for Ethernet)	
	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. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3–2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. Up to 128 rules may be configured for each port. The user may select all ports by entering the *all* parameter. Non–contiguous portlist entries are separated by a comma. (ex: 1:1–1:3,1:7–1:9) *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 if you want 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 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. *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 many 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* – Select *mirror* to specify that packets match the access profile are mirrored to a port defined in the **config mirror port** command. Port Mirroring must be enabled and a

config access_profile profile_id (for Ethernet)

	target port must be set. *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 1–128*> – 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 and Operator-level users can issue this command.

Example usage:

To configure a rule for the Ethernet access profile:

```
DGS-3426:5#config access profile profile_id 1 add access_id 1 ethernet vlan
Trinity 802.1p 1 port 1:1 permit priority 1 replace priority
Command: config access profile profile_id 1 add access_id 1 ethernet vlan
Trinity 802.1p 1 port 1:1 permit priority 1 replace priority

Success.

DGS-3426:5#
```

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 1-6> 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}]} (1)**
Description	This command is used 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	*ip* – Specifies that the Switch will look into the IP fields in each packet with special emphasis on one or more of the following: • *profile_id* <*value 1–6*> – Specifies an index number between 1 and 6 that will identify the access profile being created with this command. • *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.

create access_profile (IP)	
Parameters	• *type* – Specifies that the Switch will examine each frame’s IGMP Type field. • *tcp* – Specifies that the Switch will examine each frames 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 Universal 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* – Specifies that the Switch will examine each frame’s Protocol ID field. • *<hex 0x0–0xff>* – Enter a hexadecimal value that will identify the protocol to be discovered in the packet header. • *user_define <hex 0x0–0xffffffff>* – Enter a hexadecimal value that will identify the user defined protocol to be discovered in the packet header.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure a rule for the IP access profile:

```
DGS-3426:5# 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-3426:5#
```

config access_profile profile_id (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 1-6> [add access_id [auto_assign | <value 1-128> 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}]} (1) | port [<portlist> | all] [permit {priority <value 0-7> {replace_priority} | rx_rate {no_limit | <value 1-156249>]} | replace_dscp <value 0-63> | 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.

config access_profile profile_id (IP)

Parameters

profile_id <value 1–6> – Enter an integer between 1 and 6 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 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)
  - *psh*: TCP control flag (push)
  - *rst*: TCP control flag (reset)
  - *syn*: TCP control flag (synchronize)
  - *fin*: TCP control flag (finish)
- *udp* – Specifies that the Switch will examine the 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. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3–2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. Up to 128 rules may be configured for each port. Selecting *all* will configure this rule for all ports on the Switch. Non–contiguous portlist entries are separated by a comma. (ex: 1:1–1:3,1:7–1:9)

config access_profile profile_id (IP)	
	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 if you want 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 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. *replace_dscp <value 0–63>* – Allows you 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 many 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 conter command here will be overridden and therefore will not count packets. This command is optional and the default setting is disabled. *mirror* – Select *mirror* to specify that packets 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 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 and Operator-level users can issue this command.

Example usage:

To configure a rule for the IP access profile:

```
DGS-3426:5#config access_profile profile_id 2 add access_id 2 ip protocol_id 2
port 1:2 deny
Command: config access_profile profile_id 2 add access_id 2 ip protocol_id 2
port 1:2 deny

Success.

DGS-3426:5#
```

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 users command. Specific values for the rules are entered using the **config access_profile** command, below.
Syntax	**create access_profile profile_id <value 1-6> packet_content_mask {offset_chunk_1 <value 0-31> <hex 0x0-0xffffffff> | offset_chunk_2 <value 0-31> <hex 0x0-0xffffffff> | offset_chunk_3 <value 0-31> <hex 0x0-0xffffffff> | offset_chunk_4 <value 0-31> <hex 0x0-0xffffffff>} (1)**
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	*packet_content_mask* – The offset field is used to examine the packet header which 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 1-6>* – Specifies an index number between *1* and *6* that will identify the access profile being created with this command.
Restrictions	Only Administrator 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 1-6> [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>} (1) port [<portlist> | all] [permit {priority <value 0-7> {replace_priority} | rx_rate {no_limit | <value 1-156249>]} | replace_dscp <value 0-63> | counter [enable | disable]} | mirror | deny} {time_range <range_name 32>} | delete access_id <value 1-128>]**

config access_profile profile_id (packet content)

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

profile_id <value 1-6> – Enter an integer between *1* and *6* 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 – Adds an additional rule to the above specified access profile.

- *auto_assign* – 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.

offset_chunk_1 – The offset field is used to examine the packet header which is divided up 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.

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 1-4, 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 many 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 conter command here will be overridden and therefore will not count packets. This command is optional and the default setting is *disabled*.

mirror – Select *mirror* to specify that packets 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 (packet content)

	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 1-128>* – 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 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 1–6> ipv6 {[{class | flowlabel | source_ipv6_mask <ipv6mask> | destination_ipv6_mask <ipv6mask>]} (1)]**
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	*profile_id <value 1–6>* – Specifies an index number between 1 and 6 that will identify the access profile being created with this command. *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 address. • *destination_ipv6_mask <ipv6mask>* – Specifies an IP address mask for the destination IPv6 address.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create an access profile based on IPv6 classification:

```
DGS-3426:5#create access_profile profile_id 4 ipv6 class flowlabel
Command: create access_profile profile_id 4 ipv6 class flowlabel

Success.

DGS-3426:5#
```

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 1-6> add access_id [auto_assign | <value 1-128>] ipv6 {class <value 0-255> | flowlabel <hex 0x0-0xfffff> | source_ipv6 <ipv6addr> | destination_ipv6 <ipv6addr>} (1) 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 1–6>* – Enter an integer between 1 and 6 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–fffff>* – 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. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3–2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. Up to 128 rules may be configured for each port. Selecting *all* will configure this rule for all ports on the Switch. Non–contiguous portlist entries are separated by a comma. (ex: 1:1–1:3,1:7–1:9) *permit* – Specifies that packets that match the access profile are permitted to be forwarded by the Switch.

config access_profile profile_id (ipv6)	
	• *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. *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 many select a value between 1– 156249 or *no_limit*. The default setting is *no_limit*. *deny* – Specifies that packets that match the access profile are not permitted to be forwarded by the Switch and will be filtered. *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 conter 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. *{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 and Operator-level users can issue this command.

Example usage:

To configure a previously created access profile based on IPv6 classification:

```
DGS-3426:5#config access_profile profile_id 4 add access_id 1 ipv6 class 1
flowlabel 0xABCD port 1:4 deny
Command: config access_profile profile_id 4 add access_id 1 ipv6 class 1
flowlabel 0xABCD port 1:4 deny

Success.

DGS-3426:5#
```

delete access_profile

Purpose	Used to delete a previously created access profile.
Syntax	**delete access_profile {profile_id <value 1–6> | all}**
Description	This command is used to delete a previously created access profile on the Switch.
Parameters	*profile_id <value 1–6>* – Enter an integer between 1 and 6 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. *all* – Using this parameter will delete all IP profiles currently configured on the switch, except for those automatically created using the IP–MAC binding commands.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete the access profile with a profile ID of 1:

```
DGS-3426:5#delete access_profile profile_id 1
Command: delete access_profile profile_id 1

Success.

DGS-3426:5#
```

show access_profile

Purpose	Used to display the currently configured access profiles on the Switch.
Syntax	**show access_profile {profile_id <value 1–6>}**
Description	This command is used to display the currently configured access profiles.
Parameters	*profile_id <value 1–6>* – Enter an integer between 1 and 6 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** 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-3426:5#show access_profile
Command: show access_profile

Access Profile Table

Access Profile ID: 1                             TYPE : Ethernet
====================================================================
MASK Option :
VLAN         802.1p
-----------      ------

Access ID : 3              Mode: Permit(replaced) priority: 1   RX Rate(64Kbps):
no_limit
Ports: 1:1
-----------   ------
Trinity      1
======================================================================
Access Profile ID: 2                              TYPE : IP
======================================================================
MASK Option :
Protocol ID

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

Access ID : 2              Mode: Deny
Ports: 1:2
--------------------
2
======================================================================
Access Profile ID: 3                              TYPE : Packet Content
======================================================================
MASK Option :
Offset  0-15 : 0xFFFFFFFF 0xFFFFFFFF 0xFFFFFFFF 0xFFFFFFFF
Offset 16-31 : 0x0000FFFF 0xFFFF0000 0x0000000F 0x0F000000

Access ID : 1              Mode: Deny
Ports: 1:1
Offset  0-15 : 0x11111111 0x11111111 0x11111111 0x11111111
Offset 16-31 : 0x00001111 0x11110000 0x00000001 0x01000000
======================================================================

Total Entries: 3

DGS-3426:5#
```

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 [ethernet {vlan | source_mac <macaddr 000000000000–ffffffffffff> | destination_mac <macaddr 000000000000–ffffffffffff> | ethernet_type} (1) | ip {vlan | source_ip_mask <netmask> | destination_ip_mask <netmask> | dscp | [icmp {type | code} | igmp {type} | tcp {src_port_mask <hex 0x0–0xffff> | dst_port_mask <hex 0x0–0xffff> | flag_mask [all | {urg | ack | psh | rst | syn | fin} (1)]} | udp {src_port_mask <hex 0x0–0xffff> | dst_port_mask <hex 0x0–0xffff>} | protocol_id_mask {<hex 0x0–0xff> {user_define_mask <hex 0x0–0xffffffff>}]} (1) | packet_content_mask {offset 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**

create cpu access_profile

0x0–0xffffffff> <hex 0x0–0xffffffff> <hex 0x0–0xffffffff> <hex 0x0–0xffffffff> | offset 64–79 <hex 0x0–0xffffffff> <hex 0x0–0xffffffff> <hex 0x0–0xffffffff> <hex 0x0–0xffffffff>} (1) ipv6 {[class | flowlabel] (1) | source_ipv6_mask <ipv6mask> | destination_ipv6_mask <ipv6mask>]} (1) profile_id <value 1–5>

Description

This command is used to create an access profile used only for CPU Interface Filtering. Masks can be entered that will be combined with the values the Switch finds in the specified frame header fields. Specific values for the rules are entered using the **config cpu access_profile** command, below.

Parameters

ethernet – Specifies that the Switch will examine the layer 2 part of each packet header.

- *vlan* – Specifies that the Switch will examine the VLAN part of each packet header.
- *source_mac <macaddr 000000000000–ffffffffffff>* – Specifies to examine the source MAC address mask. MAC address entries may be made in the following format: **000000000000–FFFFFFFFFFFF**
- *destination_mac <macaddr 000000000000–ffffffffffff>* – 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 frames 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 Universal Datagram Protocol (UDP) field.
  - *src_port_mask <hex 0x0–0xffff>* – Specifies a UDP port mask for the source port.
  - *dst_port_mask <hex 0x0–0xffff>* – Specifies a UDP port mask for the destination port.
- *protocol_id_mask <hex 0x0–0xffffffff>* – Specifies that the Switch will examine each frame’s Protocol ID field using the hex form entered here.
  - *user_define_mask <hex 0x0–0xff>* – 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:

create cpu access_profile

	• *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* – 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 0x0–0xfffff>* – 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. *profile_id <value 1–5>* – Enter an integer between *1* and *5* that is used to identify the CPU access profile to be deleted with this command.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create a CPU access profile:

```
DGS-3426:5# 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-3426:5#
```

delete cpu access_profile

Purpose	Used to delete a previously created access profile or cpu access profile.
Syntax	**delete cpu access_profile [profile_id <value 1–5> | all]**
Description	This command is used to delete a previously created CPU access profile.
Parameters	*profile_id <value 1–5>* – Enter an integer between 1 and 5 that is used to identify the CPU access profile to be deleted with this command. This value is assigned to the access profile when it is created with the **create cpu access_profile** command. *all* – Entering this parameter will delete all CPU access profiles currently set on the Switch.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete the CPU access profile with a profile ID of 1:

```
DGS-3426:5#delete cpu access_profile profile_id 1
Command: delete cpu access_profile profile_id 1

Success.

DGS-3426:5#
```

config cpu access_profile profile_id

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 operation, 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–ffffffffffff> | destination_mac <macaddr 000000000000–ffffffffffff> | ethernet_type <hex 0x0–0xffff>} (1) | 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>}]} (1) | packet_content {offset_0–15 <hex 0x0–0xffffffff> <hex 0x0–0xffffffff> <hex 0x0–0xffffffff> <hex 0x0–0xffffffff>| offset_16–31 <hex 0x0–0xffffffff> <hex 0x0–0xffffffff> <hex 0x0–0xffffffff> <hex 0x0–0xffffffff> | offset_32–47 <hex 0x0–0xffffffff> <hex 0x0–0xffffffff> <hex 0x0–0xffffffff> <hex 0x0–0xffffffff> | offset_48–63 <hex 0x0–0xffffffff> <hex 0x0–0xffffffff> <hex 0x0–0xffffffff> <hex 0x0–0xffffffff> | offset_64–79 <hex 0x0–0xffffffff> <hex 0x0–0xffffffff> <hex 0x0–0xffffffff> <hex 0x0–0xffffffff>} (1) | ipv6 {[{class <value 0-255> | flowlabel <hex 0x0-0xfffff>} (1) | source_ipv6 <ipv6addr> | destination_ipv6 <ipv6addr>]} (1)] port [<portlist> | all] [permit | deny] {time_range <range_name 32>} | delete access_id <value 1–100>]

Description

This command is used to configure a CPU access profile for CPU Interface Filtering and to enter specific values that will be combined, using a logical AND operational method, with masks entered with the **create cpu access_profile** command, above.

Parameters

profile_id <value 1–5> – Enter an integer used to identify the access profile that will be configured with this command. This value is assigned to the access profile when it is created with the create access_profile command. The profile ID sets the relative priority for the profile and specifies an index number that will identify the access profile being created with this command. Priority is set relative to other profiles where the lowest profile ID has the highest priority.

- *add access_id <value 1–100>* – Adds an additional rule to the above specified access profile. The value is used to index the rule created.

ethernet – Specifies that the Switch will look only into the layer 2 part of each packet.

- *vlan <vlan_name 32>* – Specifies that the access profile will apply to only to this VLAN.
- *source_mac <macaddr 000000000000–ffffffffffff>* – Specifies that the access profile will apply to this source MAC address.
- *destination_mac <macaddr 000000000000–ffffffffffff>* – Specifies that the access profile will apply to this destination MAC address.
- *ethernet_type <hex 0x0–0xffff>* – Specifies that the access profile will apply only to packets with this hexadecimal 802.1Q Ethernet type value in the packet header.

ip – Specifies that the Switch will look into the IP fields in each packet.

- *vlan <vlan_name 32>* – Specifies that the access profile will apply to only this VLAN.

config cpu access_profile profile_id	
Parameters	• *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 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 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. • *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 examine the IPv6 address in each frame’s header. • *class<value 0-255>* – Choosing this parameter will instruct the Switch to examine the *class* field of the IPv6 header. • *flowlabel <hex 0x0-0xfffff>*– Choosing 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 <ipv6addr>* – Specifies an IPv6 address mask for the source IPv6

config cpu access_profile profile_id

	address. • *destination_ipv6 <ipv6addr>* – Specifies an IPv6 address mask for the destination IPv6 address. *<portlist>*| *all* – Enter the port or ports to which this access profile applies. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3–2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. Entering all will denote all profiles on the switch or in the switch stack. Non–contiguous portlist entries are separated by a comma. (ex: 1:1–1:3,1:7–1:9) *permit* | *deny* – Specify that the packet matching the criteria configured with command will either be permitted entry to the cpu or denied entry to the CPU. *{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 and Operator-level users can issue this command.

Example usage:

To configure CPU access list entry:

```
DGS-3426:5#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
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 deny

Success.

DGS-3426:5#
```

show cpu_access_profile

Purpose	Used to view the CPU access profile entry currently set in the Switch.
Syntax	**show cpu_access_profile {profile_id <value 1–5>}**
Description	This command is used view the current CPU interface filtering entries set on the Switch.
Parameters	*profile_id <value 1–5>* – Enter an integer between 1 and 5 that is used to identify the CPU access profile to be deleted with this command. This value is assigned to the access profile when it is created with the **create cpu access_profile** command
Restrictions	None.

Example usage:

To show the CPU filtering state on the Switch:

```
DGS-3426:5#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          802.1p
----------  ------
Access ID: 2              Mode: Permit
---------------------
default
===========================================================================
Total Entries: 1

DGS-3426:5#
```

27

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 following chapter, **Time and SNTP Commands**.

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	*range_name 32* – 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. *hours* – This parameter is used to set the time in the day that this time range is to be set using the following parameters: • *start_time <time hh:mm:ss>* – Use this parameter to identify the starting time of the time range, in hours, minutes and seconds, based on the 24–hour time system. • *end_time <time hh:mm:ss>* – Use this parameter to identify the ending time of the time range, in hours, minutes and seconds, based on the 24–hour time system. *weekdays* – Use this parameter to determine the days of the week to set this time range. • *<daylist>* – 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). *delete* – Use this parameter to delete a previously configured time range from the system.
Restrictions	Only Administrator 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-3426:5#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-3426:5#
```

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 and Operator-level users can issue this command.

Example usage:

To view the current time range settings.

```
DGS-3426:5#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-3426:5#
```

28

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.
Parameters	*state [enable* | *disable]* – Select the running state of the Safeguard Engine function as enable or disable. *utilization* – Select this option to trigger the Safeguard Engine function to enable based on the following determinates: • *rising <value 20–100>* – The user can set a percentage value of the rising CPU utilization which will trigger the Safeguard Engine function. Once the CPU utilization rises to this percentage, the Safeguard Engine mechanism will initiate. • *falling <value 20–100>* – The user can set a percentage value of the falling CPU utilization which will trigger the Safeguard Engine function to cease. Once the CPU utilization falls to this percentage, the Safeguard Engine mechanism will shut down. *trap_log [enable* | *disable]* – Choose whether to enable or disable the sending of messages to the device's SNMP agent and switch log once the Safeguard Engine has been activated by a high CPU utilization rate. *mode* – 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: • *strict* – If selected, this function will instruct the Switch to minimize the IP and ARP traffic flow to the CPU by dynamically allotting an even bandwidth to all traffic flows. • *fuzzy* – If selected, this function will stop accepting all ARP packets not intended for the Switch, and will stop receiving all unnecessary broadcast IP packets, until the storm has subsided.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the safeguard engine for the Switch:

```
DGS-3426:5#config safeguard_engine state enable utilization rising 45
Command: config safeguard_engine state enable utilization rising 45

Success.

DGS-3426:5#
```

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-3426:5#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-3426:5#
```

29

TRAFFIC SEGMENTATION COMMANDS

Traffic segmentation allows you to further sub–divide VLANs into smaller groups of ports that will help to reduce traffic on the VLAN. The VLAN rules take precedence, and then the traffic segmentation rules are applied.

Command	Parameters
config traffic_segmentation	[<portlist> | all] forward_list [null | all | <portlist>]
show traffic_segmentation	{<portlist>}

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

config traffic_segmentation	
Purpose	Used to configure traffic segmentation on the Switch.
Syntax	**config traffic_segmentation [<portlist> | all] forward_list [null | all | <portlist>]**
Description	This command is used to configure traffic segmentation on the Switch.
Parameters	*<portlist>* – Specifies a port or range of ports that will be configured for traffic segmentation. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3–2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. Non–contiguous portlist entries are separated by a comma. (ex: 1:1–1:3,1:7–1:9) *all* – Specifies all ports on the Switch. Non–contiguous portlist entries are separated by a comma. (ex: 1:1–1:3,1:7–1:9) *forward_list* – Specifies a port or range of ports that will receive forwarded frames from the ports specified in the portlist, above. • *null* – No ports are specified • *all* – Specifies all ports on the Switch. • *<portlist>* – Specifies a range of ports for the forwarding list. This list must be on the same switch previously specified for traffic segmentation (i.e. following the *<portlist>* specified above for **config traffic_segmentation**). The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3–2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. Non–contiguous portlist entries are separated by a comma. (ex: 1:1–1:3,1:7–1:9)
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure ports 1 through 10 to be able to forward frames to port 11 through 15:

```
DGS-3426:5#config traffic_segmentation 1:1-1:10 forward_list 1:11-1:15
Command: config traffic_segmentation 1:1-1:10 forward_list 1:11-1:15

Success.

DGS-3426:5#
```

show traffic_segmentation

Purpose	Used to display the current traffic segmentation configuration on the Switch.
Syntax	**show traffic_segmentation {<portlist>}**
Description	This command is used to display the current traffic segmentation configuration on the Switch.
Parameters	*<portlist>* – Specifies a port or range of ports for which the current traffic segmentation configuration on the Switch will be displayed. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3–2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. Non–contiguous portlist entries are separated by a comma. (ex: 1:1–1:3,1:7–1:9)
Restrictions	None.

Example usage:

To display the current traffic segmentation configuration on the Switch.

```
DGS-3426:5#show traffic_segmentation
Command: show traffic_segmentation

Traffic Segmentation Table

Port    Forward Portlist
------ ----------------------------------------
1:1       1:1-1:24
1:2       1:1- 1:24
1:3       1:1- 1:24
1:4       1:1- 1:24
1:5       1:1- 1:24
1:6       1:1- 1:24
1:7       1:1- 1:24
1:8       1:1- 1:24
1:9       1:1- 1:24
1:10      1:1- 1:24
1:11      1:1- 1:24
1:12      1:1- 1:24
1:13      1:1- 1:24
1:14      1:1- 1:24
1:15      1:1- 1:24
1:16      1:1- 1:24
1:17      1:1- 1:24
1:18      1:1- 1:24

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

30

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	This command is used to configure SNTP service from an SNTP server. SNTP must be enabled for this command to function (See **enable sntp**).
Parameters	*primary* – This is the primary server the SNTP information will be taken from. ▪ *<ipaddr>* – The IP address of the primary server. *secondary* – This is the secondary server the SNTP information will be taken from in the event the primary server is unavailable. ▪ *<ipaddr>* – The IP address for the secondary server. *poll–interval <int 30–99999>* – This is the interval between requests for updated SNTP information. The polling interval ranges from 30 to 99,999 seconds.
Restrictions	Only Administrator and Operator-level users can issue this command. SNTP service must be enabled for this command to function (*enable sntp*).

Example usage:

To configure SNTP settings:

```
DGS-3426:5#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-3426:5#
```

show sntp

Purpose	Used to display the SNTP information.
Syntax	**show sntp**
Description	This command is used to 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-3426:5#show sntp
Command: show sntp

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

DGS-3426:5#
```

enable sntp

Purpose	To enable SNTP server support.
Syntax	**enable sntp**
Description	This command is used to enable SNTP support. SNTP service must be separately configured (see **config sntp**). Enabling and configuring SNTP support will override any manually configured system time settings.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command. SNTP settings must be configured for SNTP to function (**config sntp**).

Example usage:

To enable the SNTP function:

```
DGS-3426:5#enable sntp
Command: enable sntp

Success.

DGS-3426:5#
```

disable sntp

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

Example usage:

To disable SNTP:

```
DGS-3426:5#disable sntp
Command: disable sntp

Success.

DGS-3426:5#
```

config time

Purpose	Used to manually configure system time and date settings.
Syntax	**config time <date ddmthyyyy> <time hh:mm:ss>**
Description	This command is used to configure the system time and date settings. These will be overridden if SNTP is configured and enabled.
Parameters	*date* – Express the date using two numerical characters for the day of the month, three alphabetical characters for the name of the month, and four numerical characters for the year. For example: 03aug2003. *time* – Express the system time using the format hh:mm:ss, that is, two numerical characters each for the hour using a 24–hour clock, the minute and second. For example: 19:42:30.
Restrictions	Only Administrator and Operator-level users can issue this command. Manually configured system time and date settings are overridden if SNTP support is enabled.

Example usage:

To manually set system time and date settings:

```
DGS-3426:5#config time 30jun2003 16:30:30
Command: config time 30jun2003 16:30:30

Success.

DGS-3426:5#
```

config time_zone

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

Example usage:

To configure time zone settings:

```
DGS-3426:5#config time_zone operator + hour 2 min 30
Command: config time_zone operator + hour 2 min 30

Success.

DGS-3426:5#
```

config dst	
Purpose	Used to enable and configure time adjustments to allow for the use of Daylight Savings Time (DST).
Syntax	**config dst [disable | repeating {s_week <start_week 1–4,last> | s_day <start_day sun–sat> | s_mth <start_mth 1–12> | s_time start_time hh:mm> | e_week <end_week 1–4,last> | e_day <end_day sun–sat> | e_mth <end_mth 1–12> | e_time <end_time hh:mm> | offset [30 | 60 | 90 | 120]} | annual {s_date start_date 1–31> | s_mth <start_mth 1–12> | s_time <start_time hh:mm> | e_date <end_date 1–31> | e_mth <end_mth 1–12> | e_time <end_time hh:mm> | offset [30 | 60 | 90 | 120]}]**
Description	This command is used to enable and configure DST. When enabled this will adjust the system clock to comply with any DST requirement. DST adjustment effects system time for both manually configured time and time set using SNTP service.
Parameters	*disable* – Disable the DST seasonal time adjustment for the Switch. *repeating* – Using repeating mode will enable DST seasonal time adjustment. Repeating mode requires that the DST beginning and ending date be specified using a formula. For example, specify to begin DST on Saturday during the second week of April and end DST on Sunday during the last week of October. *annual* – Using annual mode will enable DST seasonal time adjustment. Annual mode requires that the DST beginning and ending date be specified concisely. For example, specify to begin DST on April 3 and end DST on October 14. *s_week* – Configure the week of the month in which DST begins. • *<start_week 1–4,last>* – The number of the week during the month in which DST begins where 1 is the first week, 2 is the second week and so on, last is the last week of the month. *e_week* – Configure the week of the month in which DST ends. • *<end_week 1–4,last>* – The number of the week during the month in which DST ends where 1 is the first week, 2 is the second week and so on, last is the last week of the month. *s_day* – Configure the day of the week in which DST begins. • *<start_day sun–sat>* – The day of the week in which DST begins expressed using a three character abbreviation (sun, mon, tue, wed, thu, fri, sat) *e_day* – Configure the day of the week in which DST ends. • *<end_day sun–sat>* – The day of the week in which DST ends expressed using a three character abbreviation (sun, mon, tue, wed, thu, fri, sat) *s_mth* – Configure the month in which DST begins. • *<start_mth 1–12>* – The month to begin DST expressed as a number. *e_mth* – Configure the month in which DST ends. • *<end_mth 1–12>* – The month to end DST expressed as a number. *s_time* – Configure the time of day to begin DST. • *<start_time hh:mm>* – Time is expressed using a 24–hour clock, in hours and minutes. *e_time* – Configure the time of day to end DST. • *<end_time hh:mm>* – Time is expressed using a 24–hour clock, in hours and minutes. *s_date* – Configure the specific date (day of the month) to begin DST. • <start_date 1–31> – The start date is expressed numerically**.**

config dst

Parameters	*e_date* – Configure the specific date (day of the month) to begin DST. • *<end_date 1–31>* – The end date is expressed numerically. *offset [30* | *60* | *90* | *120]* – Indicates number of minutes to add or to subtract during the summertime. The possible offset times are 30,60,90,120. The default value is 60.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure daylight savings time on the Switch:

```
DGS-3426:5#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-3426:5#
```

show time

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

Example usage:

To display the time currently set on the Switch’s System clock:

```
DGS-3426:5#show time
Command: show time

Current Time Source  : System Clock
Boot Time            : 4 May 2006  10:21:22
Current Time         : 4 May 2006  15:01:32
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-3426:5#
```

31

DHCP RELAY COMMANDS

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

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

Each command is listed in detail in the following sections.

config dhcp_relay

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

Example usage:

To config DHCP relay:

```
DGS-3$00:4#config dhcp_relay hops 2 time 23
Command: config dhcp_relay hops 2 time 23

Success.

DGS-3426:5#
```

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 is used to add an IP address as a destination to forward (relay) DHCP/BOOTP relay packets to.
Parameters	*<ipif_name 12>* – The name of the IP interface in which DHCP relay is to be enabled. *<ipaddr>* – The DHCP server IP address.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To add an IP destination to the DHCP relay table:

```
DGS-3426:5#config dhcp_relay add ipif System 10.58.44.6
Command: config dhcp_relay add ipif System 10.58.44.6

Success.

DGS-3426:5#
```

config dhcp_relay delete ipif

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

Example usage:

To delete an IP destination from the DHCP relay table:

```
DGS-3426:5#config dhcp_relay delete ipif System 10.58.44.6
Command: config dhcp_relay delete ipif System 10.58.44.6

Success.

DGS-3426:5#
```

config dhcp_relay option_82 state

Purpose	Used to configure the state of DHCP relay agent information option 82 of the switch.
Syntax	**config dhcp_relay option_82 state [enable | disable]**
Description	This command is used to configure the state of DHCP relay agent information option 82 of the switch.
Parameters	*enable* – When this field is toggled to *Enabled* the relay agent will insert and remove DHCP relay information (option 82 field) in messages between DHCP server and client. When the relay agent receives the DHCP request, it adds the option 82 information, and the IP address of the relay agent (if the relay agent is configured), to the packet. Once the option 82 information has been added to the packet it is sent on to the DHCP server. When the DHCP server receives the packet, if the server is capable of option 82, it can implement policies like restricting the number of IP addresses that can be assigned to a single remote ID or circuit ID. Then the DHCP server echoes the option 82 field in the DHCP reply. The DHCP server unicasts the reply to the back to the relay agent if the request was relayed to the server by the relay agent. The switch verifies that it originally inserted the option 82 data. Finally, the relay agent removes the option 82 field and forwards the packet to the switch port that connects to the DHCP client that sent the DHCP request. *disable* – If the field is toggled to *disable* the relay agent will not insert and remove DHCP relay information (option 82 field) in messages between DHCP servers and clients, and the check and policy settings will have no effect.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure DHCP relay option 82 state:

```
DGS-3426:5#config dhcp_relay option_82 state enable
Command: config dhcp_relay option_82 state enable

Success.

DGS-3426:5#
```

config dhcp_relay option_82 check

Purpose	Used to configure the checking mechanism of DHCP relay agent information option 82 of the switch.
Syntax	**config dhcp_relay option_82 check [enable | disable]**
Description	This command is used to configure the checking mechanism of DHCP/BOOTP relay agent information option 82 of the switch.
Parameters	*enable* – When the field is toggled to *enable*, the relay agent will check the validity of the packet's option 82 field. If the switch receives a packet that contains the option 82 field from a DHCP client, the switch drops the packet because it is invalid. In packets received from DHCP servers, the relay agent will drop invalid messages. *disable* – When the field is toggled to *disable*, the relay agent will not check the validity of the packet's option 82 field.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure DHCP relay option 82 check:

```
DGS-3426:5#config dhcp_relay option_82 check enable
Command: config dhcp_relay option_82 check enable

Success.

DGS-3426:5#
```

config dhcp_relay option_82 policy

Purpose	Used to configure the reforwarding policy of relay agent information option 82 of the switch.
Syntax	**config dhcp_relay option_82 policy [replace | drop | keep]**
Description	This command is used to configure the reforwarding policy of DHCP relay agent information option 82 of the switch.
Parameters	*replace* – The option 82 field will be replaced if the option 82 field already exists in the packet received from the DHCP client. *drop* – The packet will be dropped if the option 82 field already exists in the packet received from the DHCP client. *keep* – The option 82 field will be retained if the option 82 field already exists in the packet received from the DHCP client.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure DHCP relay option 82 policy:

```
DGS-3426:5#config dhcp_relay option_82 policy replace
Command: config dhcp_relay option_82 policy replace

Success.

DGS-3426:5#
```

show dhcp_relay

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

Example usage:

To show the DHCP relay configuration:

```
DGS-3426:5#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-3426:5#
```

Example usage:

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

```
DGS-3426:5#show dhcp_relay ipif System
Command: show dhcp_relay ipif System

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-3426:5#
```

enable dhcp_relay

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

Example usage:

To enable DHCP relay:

```
DGS-3426:5#enable dhcp_relay
Command: enable dhcp_relay

Success.

DGS-3426:5#
```

disable dhcp_relay

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

Example usage:

To disable DHCP relay:

```
DGS-3426:5#disable dhcp_relay
Command: disable dhcp_relay

Success.

DGS-3426:5#
```

config dhcp_relay option_60 state

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

Example usage:

To configure DHCP relay option 60 state:

```
DGS-3426:5#config dhcp_relay option_60 state enable
Command: config dhcp_relay option_60 state enable

Success.

DGS-3426:5#
```

config dhcp_relay option_60 add

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

Example usage:

To configure a new dhcp relay with option 60:

```
DGS–3426:5#config dhcp_relay option_60 add string "abc" relay 10.90.90.1 exact-match
Command: config dhcp_relay option_60 add string "abc" relay 10.90.90.1 exact-match

Success.

DGS–3426:5#
```

config dhcp_relay option_60 default

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

Example usage:

To configure the DHCP relay default option 60:

```
DGS–3426:5#config dhcp_relay option_60 default mode drop
Command: config dhcp_relay option_60 default mode drop

Success.

DGS–3426:5#
```

config dhcp_relay option_60 delete

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

Example usage:

To delete the DHCP relay option 60:

```
DGS-3426:5#config dhcp_relay option_60 delete all
Command: config dhcp_relay option_60 delete all

Success.

DGS-3426:5#
```

show dhcp_relay option_60

Purpose	This command is used to display DHCP relay option 60 entries.
Syntax	**show dhcp_relay option_60 {[string <mutiword 255>| ipaddress <ipaddr>| default]}**
Description	This command is used to display the DHCP relay option 60 entry by the user specified.
Parameters	*ipaddress* – Shows the entry whose ipaddress is equal to the specified ipaddress. *default* – Shows the default behaviour of dhcp_relay option60. *string* – Shows the entry whose string is equal to the string of a specified user.
Restrictions	None.

Example usage:

To display the DHCP relay option 60:

```
DGS-3426:5#show dhcp_relay option_60
Command: show dhcp_relay option_60

Default Processing Mode: Drop

Default Servers:

Matching Rules:

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

Total Entries : 1

DGS-3426:5#
```

config dhcp_relay option_61 state

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

Example usage:

To configure the state of DHCP relay option 61:

```
DGS-3426:5#config dhcp_relay option_61 state enable
Command: config dhcp_relay option_61 state enable

Success.

DGS-3426:5#
```

config dhcp_relay option_61 add

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

Example usage:

To configure the DHCP relay option 61:

```
DGS-3426:5#config dhcp_relay option_61 add mac_address 00-01-22-33-44-55 drop
Command: config dhcp_relay option_61 add mac_address 00-01-22-33-44-55 drop

Success.

DGS-3426:5#
```

config dhcp_relay option_61 default

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

Example usage:

To configure the DHCP relay option 61 default:

```
DGS-3426:5#config dhcp_relay option_61 default drop
Command: config dhcp_relay option_61 default drop

Success.

DGS-3426:5#
```

config dhcp_relay option_61 delete

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

Example usage:

To delete the DHCP relay option 61 rules:

```
DGS–3426:5#config dhcp_relay option_61 delete mac_address 00-11-22-33-44-55
Command: config dhcp_relay option_61 delete mac_address 00-11-22-33-44-55

Success

DGS–3426:5#
```

show dhcp_relay option_61

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

Example usage:

To display the DHCP relay option 61:

```
DGS–3426:5#show dhcp_relay option_61
Command: show dhcp_relay option_61

Default Relay Rule:Drop

Matching Rules:

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

Total Entries : 1

DGS–3426:5#
```

32

ROUTING TABLE COMMANDS

The Switch supports only static routing for IPv4 and IPv6 formatted addressing. Users can create up to 128 static route entries for IPv4 and IPv6 combined. Manually configured static and the local route can route IP packets. For each device that is a part of the DGS–3400 network, users may only configure one IP address as a primary or backup route.

For IPv4 static routes, once a static route has been set, the Switch will send an ARP request packet to the next hop router that has been set by the user. Once an ARP response has been retrieved by the switch from that next hop, the route becomes enabled. If a response is not received from the next hop device after three ARP requests have been sent, the configured static route will remain in a link–down status.

The Switch also supports a floating static route, which means that the user may create an alternative static route to a different next hop device located in the same network. This secondary next hop device route is considered as a backup static route for when the primary static route is down. If the primary route is lost, the backup route will uplink and its status will become Active.

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>] <ipaddr> {<metric 1–65535>} {[primary | backup]}
delete iproute	[default | <network_address>] <ipaddr>
show iproute	{[<network_address> |<ipaddr>]} {static}
create ipv6route	[default |<ipv6networkaddr>] [<ipif_name 12> <ipv6addr>| <ipv6addr>] {<metric 1-65535>}
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>] <ipaddr> {<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	*default* – Specifies to create an IP route entry. *<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). *<ipaddr>* – The gateway IP address for the next hop router. *<metric 1–65535>* – Allows the entry of a routing protocol metric entry, representing the number of routers between the Switch and the IP address above. The default setting is 1. *[primary | backup]* – The user may choose between Primary and Backup. If the Primary Static Route fails, the Backup Route will support the entry. Please take note that the Primary and Backup entries cannot have the same Gateway.
Restrictions	Only Administrator 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-3426:5#create iproute 10.48.74.121/8 10.1.1.255 primary
Command: create iproute 10.48.74.121/8 10.1.1.255 primary

Success.

DGS-3426:5#
```

delete iproute	
Purpose	Used to delete an IP route entry from the Switch’s IP routing table.
Syntax	**delete iproute [default |<network_address>] <ipaddr>**
Description	This command is used to delete an existing entry from the Switch’s IP routing table.
Parameters	*default* – Specifies to delete a default IP route entry. *<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). *<ipaddr>* – The gateway IP address for the next hop router.
Restrictions	Only Administrator 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–3426:5#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–3426:5#
```

show iproute	
Purpose	Used to display the Switch’s current IP routing table.
Syntax	**show iproute {[<network_address> |<ipaddr>]} {static}**
Description	This command is used to display the Switch’s current IP routing table.
Parameters	*<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). *<ipaddr>* – Specifies the IP address of the destination of the route. *{static}* – Add this parameter to display all statically configured IP routes set on the switch.
Restrictions	None.

Example usage:

To display the contents of the IP routing table:

```
DGS-3426P:5#show iproute static
Command: show iproute static


Routing Table

IP Address/Netmask  Gateway       Cost  Protocol  Backup    Status
------------------  ------------- ----- --------  --------  --------
10.0.0.0/8          10.1.1.255    1     Static    Primary   Inactive

Total Entries : 1


DGS-3426P: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>}**
Description	This command is used to create an IP route entry to the Switch’s IP routing table.
Parameters	*default*– Use this parameter to create a default static IPv6 route entry in the Switch’s IP routing table. *<ipv6networkaddr>* – 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). *<ipif name 12>* – Enter the corresponding IPIF name of the IPv6 addres. *<ipv6addr>* – IPv6 address for the next hop router. *<metric 1–65535>* – Allows the entry of a routing protocol metric entry, representing the number of routers between the Switch and the IP address above. The default setting is 1.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To add a single static IPv6 entry in IPv6 format:

```
DGS–3426:5#create ipv6route 1234::5D7F/32 2D30::AC21
Command: create ipv6route 1234::5D7F/32 2D30::AC21

Success.

DGS–3426:5#
```

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 is used to delete an existing static IPv6 entry from the Switch's IP routing table.
Parameters	*default* – Use this parameter to delete an existing static IPv6 entry in the Switch's IP routing table. *<ipv6networkaddr>* – 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). *<ipif name 12>* – Enter the corresponding IP interface name of the IPv6 address to be deleted here. *<ipv6addr>* – IPv6 address for the next hop router. *all* – This will delete all IPv6 static entries.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete a static IPv6 entry from the routing table:

```
DGS-3426:5# delete ipv6route 1234::5D7F/32 2D30::AC21
Command: delete ipv6route 1234::5D7F/32 2D30::AC21

Success.

DGS-3426:5#
```

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 is used to display the Switch's current static IPv6 routing table or a specific IPv6 entry.
Parameters	*<ipv6networkaddr>* – 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–3426:5# show ipv6route
Command: show ipv6route

Routing Table

IPv6 Prefix: 1234::/32                        Protocol: Static  Metric: 1
Next Hop   : 2D30::AC21                       IPIF    :
Status     : Inactive
Total Entries: 1

DGS–3426:5#
```

33

MAC NOTIFICATION COMMANDS

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

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

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

enable mac_notification

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

Example Usage:

To enable MAC notification without changing basic configuration:

```
DGS-3426:5#enable mac_notification
Command: enable mac_notification

Success.

DGS-3426:5#
```

disable mac_notification

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

Example Usage:

To disable MAC notification without changing basic configuration:

```
DGS-3426:5#disable mac_notification
Command: disable mac_notification

Success.

DGS-3426:5#
```

config mac_notification

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

Example usage:

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

```
DGS-3426:5#config mac_notification interval 1 historysize 500
Command: config mac_notification interval 1 historysize 500

Success.

DGS-3426:5#
```

config mac_notification ports

Purpose	Used to configure MAC address notification status settings.
Syntax	**config mac_notification ports [<portlist | all] [enable | disable]**
Description	This command is used to monitor MAC addresses learned and entered into the FDB.
Parameters	*<portlist>* – Specify a port or range of ports to be configured. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3–2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. Non–contiguous portlist entries are separated by a comma. (ex: 1:1–1:3,1:7–1:9) *all* – Entering this command will set all ports on the system. *[enable* | *disable]* – These commands will enable or disable MAC address table notification on the Switch.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable port 7 for MAC address table notification:

```
DGS-3426:5#config mac_notification ports 1:7 enable
Command: config mac_notification ports 1:7 enable

Success.

DGS-3426:5#
```

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-3426:5#show mac_notification
Command: show mac_notification

Global MAC Notification Settings

State         : Enabled
Interval      : 1
History Size  : 1

DGS-3426:5#
```

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 range of ports to be configured. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3–2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. Non–contiguous portlist entries are separated by a comma. (ex: 1:1–1:3,1:7–1:9) 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-3426:5#show mac_notification ports
Command: show mac_notification ports

Port #  MAC Address Table Notification State
------ -------------------------------------------
1:1                               Disabled
1:2                               Disabled
1:3                               Disabled
1:4                               Disabled
1:5                               Disabled
1:6                               Disabled
1:7                               Disabled
1:8                               Disabled
1:9                               Disabled
1:10                              Disabled
1:11                              Disabled
1:12                              Disabled
1:13                              Disabled
1:14                              Disabled
1:15                              Disabled
1:16                              Disabled
1:17                              Disabled
1:18                              Disabled
1:19                              Disabled
1:20                              Disabled

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

34

ACCESS AUTHENTICATION CONTROL COMMANDS

The TACACS / XTACACS / TACACS+ / RADIUS commands allows users 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} (1)
delete authen_login method_list_name	<string 15>
show authen_login	{default | method_list_name <string 15> | all}
create authen_enable method_list_name	<string 15>
config authen_enable	[default | method_list_name <string 15>] method {tacacs | xtacacs | tacacs+ | radius | server_group <string 15> | local_enable | none} (1)
delete authen_enable method_list_name	<string 15>
show authen_enable	[default | method_list_name <string 15> | all]
config authen application	{console | telnet | ssh | http | all] [login | enable] [default | method_list_name <string 15>]
show authen application	
create authen server_group	<string 15>
config authen server_group	[tacacs | xtacacs | tacacs+ | radius | <string 15>] [add | delete] server_host <ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius]
delete authen server_group	<string 15>
show authen server_group	<string 15>
create authen server_host	<ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius] {port <int 1–65535> | key [<key_string 254> | none] | timeout <int 1–255> | retransmit <int 1–20>}
config authen server_host	<ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius] {port <int 1–65535> | key [<key_string 254> | none] | timeout <int 1–255> | retransmit <int 1–20>} (1)
delete authen server_host	<ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius]
show authen server_host	
config authen parameter response_timeout	<int 0–255>
config authen parameter attempt	<int 1–255>
show authen parameter	
enable admin	
config admin local_enable	

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

enable authen_policy

Purpose	Used to enable system access authentication policy.
Syntax	**enable authen_policy**
Description	This command is used to 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-3426:5#enable authen_policy
Command: enable authen_policy

Success.

DGS-3426:5#
```

disable authen_policy

Purpose	Used to disable system access authentication policy.
Syntax	**disable authen_policy**
Description	This command is used to 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-3426:5#disable authen_policy
Command: disable authen_policy

Success.

DGS-3426:5#
```

show authen_policy

Purpose	Used to display the system access authentication policy status on the Switch.
Syntax	**show authen_policy**
Description	This command is used to display the current status of the access authentication policy on the Switch.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To display the system access authentication policy:

```
DGS-3426:5#show authen_policy
Command: show authen_policy

Authentication Policy: Enabled

DGS-3426:5#
```

create authen_login method_list_name

Purpose	Used to create a user defined method list of authentication methods for users logging on to the Switch.
Syntax	**create authen_login method_list_name <string 15>**
Description	This command is used to create a list for authentication techniques for user login. The Switch can support up to eight method lists, but one is reserved as a default and cannot be deleted. Multiple method lists must be created and configured separately.
Parameters	*<string 15>* – Enter an alphanumeric string of up to 15 characters to define the given *method list*.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To create the method list “Tiberius.”:

```
DGS-3426:5#create authen_login method_list_name Tiberius
Command: create authen_login method_list_name Tiberius

Success.

DGS-3426:5#
```

config authen_login

Purpose	Used to configure a user–defined or default method list of authentication methods for user login.
Syntax	**config authen_login [default | method_list_name <string 15>] method {tacacs | xtacacs | tacacs+ | radius | server_group <string 15> | local | none} (1)**
Description	This command is used to configure a user–defined or default method list of authentication methods for users logging on to the Switch. The sequence of methods implemented in this command will affect the authentication result. For example, if a user enters a sequence of methods like *tacacs – xtacacs – local,* the Switch will send an authentication request to the first *tacacs* host in the server group. If no response comes from the server host, the Switch will send an authentication request to the second *tacacs* host in the server group and so on, until the list is exhausted. At that point, the Switch will restart the same sequence with the following protocol listed, *xtacacs*. If no authentication takes place using the *xtacacs* list, the *local* account database set in the Switch is used to authenticate the user. When the local method is used, the privilege level will be dependant on the local account privilege configured on the Switch. Successful login using any of these methods will give the user a “user” privilege only. If the user wishes to upgrade his or her status to the administrator level, the user must implement the *enable admin* command, followed by a previously configured password. (*See the **enable admin** part of this section for more detailed information, concerning the **enable admin** command.)*
Parameters	*default* – The default method list for access authentication, as defined by the user. The user may choose one or a combination of up to four of the following authentication methods: ▪ *tacacs* – Adding this parameter will require the user to be authenticated using

config authen_login	
Parameters	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 “Tiberius” with authentication methods tacacs, xtacacs and local, in that order.

```
DGS-3426:5#config authen_login method_list_name Tiberius method tacacs xtacacs
local
Command: config authen_login method_list_name Tiberius method tacacs xtacacs
local

Success.

DGS-3426:5#
```

Example usage:

To configure the default method list with authentication methods xtacacs, tacacs+ and local, in that order:

```
DGS-3426:5#config authen_login default method xtacacs tacacs+ local
Command: config authen_login default method xtacacs tacacs+ local

Success.

DGS-3426:5#
```

delete authen_login method_list_name

Purpose	Used to delete a previously configured user defined method list of authentication methods for users logging on to the Switch.
Syntax	**delete authen_login method_list_name <string 15>**
Description	This command is used to delete a list for authentication methods for user login.
Parameters	*<string 15>* – Enter an alphanumeric string of up to 15 characters to define the given *method list* to delete.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete the method list name "Tiberius":

```
DGS-3426:5#delete authen_login method_list_name Tiberius
Command: delete authen_login method_list_name Tiberius

Success.

DGS-3426:5#
```

show authen_login

Purpose	Used to display a previously configured user defined method list of authentication methods for users logging on to the Switch.
Syntax	**show authen_login [default | method_list_name <string 15> | all]**
Description	This command is used to show a list of authentication methods for user login.
Parameters	*default* – Entering this parameter will display the default method list for users logging on to the Switch. *method_list_name <string 15>* – Enter an alphanumeric string of up to 15 characters to define the given *method list* the user wishes to view. *all* – Entering this parameter will display all the authentication login methods currently configured on the Switch. The window will display the following parameters: ▪ Method List Name – The name of a previously configured method list name. ▪ Priority – Defines which order the method list protocols will be queried for authentication when a user attempts to log on to the Switch. Priority ranges from 1(highest) to 4 (lowest). ▪ Method Name – Defines which security protocols are implemented, per method list name. ▪ Comment – Defines the type of Method. *User–defined Group* refers to server group defined by the user. *Built–in Group* refers to the TACACS, XTACACS, TACACS+ and RADIUS security protocols which are permanently set in the Switch. *Keyword* refers to authentication using a technique INSTEAD of TACACS / XTACACS / TACACS+ / RADIUS which are local (authentication through the user account on the Switch) and none (no authentication necessary to access any function on the Switch).
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To view the authentication login method list named Tiberius:

```
DGS-3426:5#show authen_login method_list_name Tiberius
Command: show authen_login method_list_name Tiberius

Method List Name   Priority  Method Name     Comment
----------------   --------  -----------     ------------------
Tiberius             1         tacacs+       Built-in Group
                     2         tacacs        Built-in Group
                     3         ctsnow        User–defined Group
                     4         local         Keyword

DGS-3426:5#
```

create authen_enable method_list_name

Purpose	Used to create a user–defined method list of authentication methods for promoting normal user level privileges to Administrator level privileges on the Switch.
Syntax	**create authen_enable method_list_name <string 15>**
Description	This command is used to promote users with normal level privileges to Administrator level privileges using authentication methods on the Switch. Once a user acquires normal user level privileges on the Switch, he or she must be authenticated by a method on the Switch to gain administrator privileges on the Switch, which is defined by the Administrator. A maximum of eight enable method lists can be implemented on the Switch.
Parameters	*<string 15>* – Enter an alphanumeric string of up to 15 characters to define the given *enable method list* to create.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To create a user–defined method list, named “Permit” for promoting user privileges to Administrator privileges:

```
DGS-3426:5#create authen_enable method_list_name Permit
Command: show authen_login method_list_name Permit

Success.

DGS-3426:5#
```

config authen_enable

Purpose	Used to configure a user–defined method list of authentication methods for promoting normal user level privileges to Administrator level privileges on the Switch.
Syntax	**config authen_enable [default | method_list_name <string 15>] method {tacacs | xtacacs | tacacs+ | radius | server_group <string 15> | local_enable | none} (1)**
Description	This command is used to promote users with normal level privileges to Administrator level privileges using authentication methods on the Switch. Once a user acquires normal user level privileges on the Switch, he or she must be authenticated by a method on the Switch to gain administrator privileges on the Switch, which is defined by the Administrator. A maximum of eight enable method lists can be implemented simultaneously on the Switch. The sequence of methods implemented in this command will affect the authentication result. For example, if a user enters a sequence of methods like *tacacs – xtacacs – local_enable,* the Switch will send an authentication request to the first *TACACS* host in the server group. If no verification is found, the Switch will send an authentication request to the second *TACACS* host in the server group and so on, until the list is exhausted. At

config authen_enable	
	that point, the Switch will restart the same sequence with the following protocol listed, *xtacacs*. If no authentication takes place using the *xtacacs* list, the *local_enable* password set in the Switch is used to authenticate the user. Successful authentication using any of these methods will give the user an "Admin" level privilege.
Parameters	*default* – The default method list for administration rights authentication, as defined by the user. The user may choose one or a combination of up to four of the following authentication methods: ▪ *tacacs* – Adding this parameter will require the user to be authenticated using the *TACACS* protocol from the remote TACACS *server hosts* of the TACACS *server group* list. ▪ *xtacacs* – Adding this parameter will require the user to be authenticated using the *XTACACS* protocol from the remote XTACACS *server hosts* of the XTACACS *server group* list. ▪ *tacacs+* – Adding this parameter will require the user to be authenticated using the *TACACS+* protocol from the remote TACACS+ *server hosts* of the TACACS+ *server group* list. ▪ *radius* – Adding this parameter will require the user to be authenticated using the *RADIUS* protocol from the remote RADIUS *server hosts* of the RADIUS *server group* list. ▪ *server_group <string 15>* – Adding this parameter will require the user to be authenticated using a user–defined server group previously configured on the Switch. ▪ *local_enable* – Adding this parameter will require the user to be authenticated using the local *user account* database on the Switch. ▪ *none* – Adding this parameter will require no authentication to access the Switch. *method_list_name* – Enter a previously implemented method list name defined by the user (*create authen_enable*). The user may add one, or a combination of up to four 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-3426:5#config authen_enable method_list_name Tiberius method tacacs xtacacs
local
Command: config authen_enable method_list_name Tiberius method tacacs xtacacs
local

Success.

DGS-3426:5#
```

Example usage:

To configure the default method list with authentication methods XTACACS, TACACS+ and local, in that order:

```
DGS-3426:5#config authen_enable default method xtacacs tacacs+ local
Command: config authen_enable default method xtacacs tacacs+ local

Success.

DGS-3426:5#
```

delete authen_enable method_list_name

Purpose	Used to delete a user–defined method list of authentication methods for promoting normal user level privileges to Administrator level privileges on the Switch.
Syntax	**delete authen_enable method_list_name <string 15>**
Description	This command is used to delete a user–defined method list of authentication methods for promoting user level privileges to Administrator level privileges.
Parameters	*<string 15>* – Enter an alphanumeric string of up to 15 characters to define the given *enable method list* to delete.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete the user–defined method list “Permit”

```
DGS-3426:5#delete authen_enable method_list_name Permit
Command: delete authen_enable method_list_name Permit

Success.

DGS-3426:5#
```

show authen_enable

Purpose	Used to display the method list of authentication methods for promoting normal user level privileges to Administrator level privileges on the Switch.
Syntax	**show authen_enable [default | method_list_name <string 15> | all]**
Description	This command is used to delete a user–defined method list of authentication methods for promoting user level privileges to Administrator level privileges.
Parameters	*default* – Entering this parameter will display the default method list for users attempting to gain access to Administrator level privileges on the Switch. *method_list_name <string 15>* – Enter an alphanumeric string of up to 15 characters to define the given *method list* to view. *all* – Entering this parameter will display all the authentication login methods currently configured on the Switch. The window will display the following parameters: ▪ Method List Name – The name of a previously configured method list name. ▪ Priority – Defines which order the method list protocols will be queried for authentication when a user attempts to log on to the Switch. Priority ranges from 1(highest) to 4 (lowest). ▪ Method Name – Defines which security protocols are implemented, per method list name. ▪ Comment – Defines the type of Method. *User–defined Group* refers to *server groups* defined by the user. *Built–in Group* refers to the TACACS, XTACACS, TACACS+ and RADIUS security protocols which are permanently set in the Switch. *Keyword* refers to authentication using a technique INSTEAD of TACACS/XTACACS/TACACS+/RADIUS which are local (authentication through the *local_enable* password on the Switch) and none (no authentication necessary to access any function on the Switch).
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To display all method lists for promoting user level privileges to administrator level privileges.

```
DGS-3426:5#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-3426:5#
```

config authen application

Purpose	Used to configure various applications on the Switch for authentication using a previously configured method list.
Syntax	**config authen application [console | telnet | ssh | http | all] [login | enable] [default | method_list_name <string 15>]**
Description	This command is used to configure Switch configuration applications (console, Telnet, SSH, Web) for login at the user level and at the administration level (**authen_enable**) utilizing a previously configured method list.
Parameters	*application* – Choose the application to configure. The user may choose one of the following five options to configure. ▪ *console* – Choose this parameter to configure the command line interface login method. ▪ *telnet* – Choose this parameter to configure the telnet login method. ▪ *ssh* – Choose this parameter to configure the Secure Shell login method. ▪ *http* – Choose this parameter to configure the web interface login method. ▪ *all* – Choose this parameter to configure all applications (console, Telnet, SSH, web) login method. *login* – Use this parameter to configure an application for normal login on the user level, using a previously configured method list. *enable* – Use this parameter to configure an application for upgrading a normal user level to administrator privileges, using a previously configured method list. *default* – Use this parameter to configure an application for user authentication using the default method list. *method_list_name <string 15>* – Use this parameter to configure an application for user authentication using a previously configured method list. Enter an alphanumeric string of up to 15 characters to define a previously configured method list.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the default method list for the web interface:

```
DGS-3426:5#config authen application http login default
Command: config authen application http login default

Success.

DGS-3426:5#
```

show authen application

Purpose	Used to display authentication methods for the various applications on the Switch.
Syntax	**show authen application**
Description	This command will display all of the authentication method lists (login, enable administrator privileges) for Switch configuration applications (console, Telnet, SSH, web) currently configured on the Switch.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To display the login and enable method list for all applications on the Switch:

```
DGS-3426:5#show authen application
Command: show authen application

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

DGS-3426:5#
```

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 < 1–20>}**
Description	This command is used to create an authentication server host for the TACACS/XTACACS/TACACS+/RADIUS security protocols on the Switch. When a user attempts to access the Switch with authentication protocol enabled, the Switch will send authentication packets to a remote TACACS/XTACACS/TACACS+/RADIUS server host on a remote host. The TACACS/XTACACS/TACACS+/RADIUS server host will then verify or deny the request and return the appropriate message to the Switch. More than one authentication protocol can be run on the same physical server host but, remember that TACACS/XTACACS/TACACS+/RADIUS are separate entities and are not compatible with each other. The maximum supported number of server hosts is 16.
Parameters	*server_host <ipaddr>* – The IP address of the remote server host to add. *protocol* – The protocol used by the server host. The user may choose one of the following: ▪ *tacacs* – Enter this parameter if the server host utilizes the TACACS protocol. ▪ *xtacacs* – Enter this parameter if the server host utilizes the XTACACS protocol. ▪ *tacacs+* – Enter this parameter if the server host utilizes the TACACS+ protocol. ▪ *radius* – Enter this parameter if the server host utilizes the RADIUS protocol. *port <int 1–65535>* – Enter a number between *1* and *65535* to define the virtual port number of the authentication protocol on a server host. The default port number is *49* for TACACS/XTACACS/TACACS+ servers and *1812* and *1813* for RADIUS servers but the user may set a unique port number for higher security. *key <key_string 254>* – Authentication key to be shared with a configured TACACS+ or RADIUS server only. Specify an alphanumeric string up to 254 characters. *timeout <int 1–255>* – Enter the time in seconds the Switch will wait for the server host to reply to an authentication request. The default value is *5* seconds. *retransmit <int 1–20>* – 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-3426:5#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-3426:5#
```

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 < 1–20>} (1)**
Description	This command is used to configure a user–defined authentication server host for the TACACS/XTACACS/TACACS+/RADIUS security protocols on the Switch. When a user attempts to access the Switch with the authentication protocol enabled, the Switch will send authentication packets to a remote TACACS/XTACACS/TACACS+/RADIUS server host on a remote host. The TACACS/XTACACS/TACACS+/RADIUS server host will then verify or deny the request and return the appropriate message to the Switch. More than one authentication protocol can be run on the same physical server host but, remember that TACACS/XTACACS/TACACS+/RADIUS are separate entities and are not compatible with each other. The maximum supported number of server hosts is 16.
Parameters	*server_host <ipaddr>* – The IP address of the remote server host the user wishes to alter. *protocol* – The protocol used by the server host. The user may choose one of the following: ▪ *tacacs* – Enter this parameter if the server host utilizes the TACACS protocol. ▪ *xtacacs* – Enter this parameter if the server host utilizes the XTACACS protocol. ▪ *tacacs+* – Enter this parameter if the server host utilizes the TACACS+ protocol. ▪ *radius* – Enter this parameter if the server host utilizes the RADIUS protocol. *port <int 1–65535>* – Enter a number between *1* and *65535* to define the virtual port number of the authentication protocol on a server host. The default port number is *49* for TACACS/XTACACS/TACACS+ servers and *1812* and *1813* for RADIUS servers but the user may set a unique port number for higher security. *key <key_string 254>* – Authentication key to be shared with a configured TACACS+ or RADIUS server only. Specify an alphanumeric string up to 254 characters or choose none. *timeout <int 1–255>* – Enter the time in seconds the Switch will wait for the server host to reply to an authentication request. The default value is *5* seconds. *retransmit <int 1–20>* – Enter the value in the retransmit field to change how many times the device will resend an authentication request when the server does not respond. This field is inoperable for the TACACS+ protocol.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure a TACACS+ authentication server host, with port number 4321, a timeout value of 12 seconds and a retransmit count of 4.

```
DGS-3426:5#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-3426:5#
```

delete authen server_host

Purpose	Used to delete a user–defined authentication server host.
Syntax	**delete authen server_host <ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius]**
Description	This command is used to delete a user–defined authentication server host previously created on the Switch.
Parameters	*server_host <ipaddr>* – The IP address of the remote server host to be deleted. *protocol* – The protocol used by the server host the user wishes to delete. The user may choose one of the following: ▪ *tacacs* – Enter this parameter if the server host utilizes the TACACS protocol. ▪ *xtacacs* – Enter this parameter if the server host utilizes the XTACACS protocol. ▪ *tacacs+* – Enter this parameter if the server host utilizes the TACACS+ protocol. ▪ *radius* – Enter this parameter if the server host utilizes the RADIUS protocol.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete a user–defined TACACS+ authentication server host:

```
DGS-3426:5#delete authen server_host 10.1.1.121 protocol tacacs+
Command: delete authen server_host 10.1.1.121 protocol tacacs+

Success.

DGS-3426:5#
```

show authen server_host

Purpose	Used to view a user–defined authentication server host.
Syntax	**show authen server_host**
Description	This command is used to view user–defined authentication server hosts previously created on the Switch. The following parameters are displayed: IP Address – The IP address of the authentication server host. Protocol – The protocol used by the server host. Possible results will include TACACS, XTACACS, TACACS+ or RADIUS. Port – The virtual port number on the server host. The default value is 49. Timeout – The time in seconds the Switch will wait for the server host to reply to an authentication request. Retransmit – The value in the retransmit field denotes how many times the device will resend an authentication request when the TACACS server does not respond. This field is inoperable for the tacacs+ protocol. Key – Authentication key to be shared with a configured TACACS+ server only.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To view authentication server hosts currently set on the Switch:

```
DGS-3426:5#show authen server_host
Command: show authen server_host

IP Address    Protocol    Port  Timeout  Retransmit  Key
------------- --------    ----- ------   ---------------
10.53.13.94    TACACS      49      5         2      ----

Total Entries : 1

DGS-3426:5#
```

create authen server_group

Purpose	Used to create a user–defined authentication server group.
Syntax	**create authen server_group <string 15>**
Description	This command is used to create an authentication server group. A server group is a technique used to group TACACS/XTACACS/TACACS+/RADIUS server hosts into user defined categories for authentication using method lists. The user may add up to eight authentication server hosts to this group using the **config authen server_group** command.
Parameters	<*string 15*> – Enter an alphanumeric string of up to 15 characters to define the newly created server group.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To create the server group “group_1”:

```
DGS-3426:5#create authen server_group group_1
Command: create authen server_group group_1

Success.

DGS-3426:5#
```

config authen server_group

Purpose	Used to configure a user–defined authentication server group.
Syntax	**config authen server_group [tacacs | xtacacs | tacacs+ | radius | <string 15>] [add | delete] server_host <ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius]**
Description	This command is used to configure an authentication server group. A server group is a technique used to group TACACS/XTACACS/TACACS+/RADIUS server hosts into user defined categories for authentication using method lists. The user may define the type of server group by protocol or by previously defined server group. Up to eight authentication server hosts may be added to any particular group
Parameters	*server_group* – The user may define the group by protocol groups built into the Switch (TACACS/XTACACS/TACACS+/RADIUS), or by a user–defined group previously created using the *create authen server_group* command. ▪ *tacacs* – Use this parameter to utilize the built–in TACACS server protocol on the Switch. Only server hosts utilizing the TACACS protocol may be added to this group. ▪ *xtacacs* – Use this parameter to utilize the built–in XTACACS server protocol on the Switch. Only server hosts utilizing the XTACACS protocol may be added to this group. ▪ *tacacs+* – Use this parameter to utilize the built–in TACACS+ server protocol on the Switch. Only server hosts utilizing the TACACS+ protocol may be added to this group. ▪ *radius* – Use this parameter to utilize the built–in RADIUS server protocol on the Switch. Only server hosts utilizing the RADIUS protocol may be added to this group. ▪ *<string 15>* – Enter an alphanumeric string of up to 15 characters to define the previously created server group. This group may add any combination of server hosts to it, regardless of protocol. *add/delete* – Enter the correct parameter to add or delete a server host from a server group. *server_host <ipaddr>* – Enter the IP address of the previously configured server host to add or delete. *protocol* – Enter the protocol utilized by the server host. There are three options: ▪ *tacacs* – Use this parameter to define the protocol if the server host is using the TACACS authentication protocol. ▪ *xtacacs* – Use this parameter to define the protocol if the server host is using the XTACACS authentication protocol. ▪ *tacacs+* – Use this parameter to define the protocol if the server host is using the TACACS+ authentication protocol. ▪ *radius* – Use this parameter to define the protocol if the server host is using the RADIUS authentication protocol.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To add an authentication host to server group "group_1":

```
DGS-3426:5# config authen server_group group_1 add server_host 10.1.1.121
protocol tacacs+
Command: config authen server_group group_1 add server_host 10.1.1.121 protocol
tacacs+

Success.

DGS-3426:5#
```

delete authen server_group

Purpose	Used to delete a user–defined authentication server group.
Syntax	**delete authen server_group <string 15>**
Description	This command is used to delete an authentication server group.
Parameters	*<string 15>* – Enter an alphanumeric string of up to 15 characters to define the previously created server group to be deleted.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete the server group "group_1":

```
DGS-3426:5#delete server_group group_1
Command: delete server_group group_1

Success.

DGS-3426:5#
```

show authen server_group

Purpose	Used to view authentication server groups on the Switch.
Syntax	**show authen server_group <string 15>**
Description	This command is used to display authentication server groups currently configured on the Switch. This command will display the following fields: Group Name: The name of the server group currently configured on the Switch, including built in groups and user defined groups. IP Address: The IP address of the server host. Protocol: The authentication protocol used by the server host.
Parameters	*<string 15>* – Enter an alphanumeric string of up to 15 characters to define the previously created server group to be viewed. Entering this command without the *<string>* parameter will display all authentication server groups on the Switch.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To view authentication server groups currently set on the Switch.

```
DGS-3426:5#show authen server_group
Command: show authen server_group

Group Name    IP Address                 Protocol
------------  ---------------            --------
ctsnow         10.53.13.2                 TACACS
tacacs         10.53.13.94                TACACS
tacacs+        (This group has no entry)
------------   (This group has no entry)

Total Entries : 4

DGS-3426:5#
```

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 is used to set the time the Switch will wait for a response of authentication from the user.
Parameters	*response_timeout <int 0–255>* – Set the time, in seconds, the Switch will wait for a response of authentication from the user attempting to log in from the command line interface or telnet interface. “0” (integer zero) means there won’t be a time–out. 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–3426:5# config authen parameter response_timeout 60
Command: config authen parameter response_timeout 60

Success.

DGS–3426:5#
```

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 is used to configure the maximum number of times the Switch will accept authentication attempts. Users failing to be authenticated after the set amount of attempts will be denied access to the Switch and will be locked out of further authentication attempts. Command line interface users will have to wait 60 seconds before another authentication attempt. Telnet users will be disconnected from the Switch.
Parameters	*parameter attempt <int 1–255>* – Set the maximum number of attempts the user may try to become authenticated by the Switch, before being locked out.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To set the maximum number of authentication attempts at 5:

```
DGS–3426:5# config authen parameter attempt 5
Command: config authen parameter attempt 5

Success.

DGS–3426:5#
```

show authen parameter

Purpose	Used to display the authentication parameters currently configured on the Switch.
Syntax	**show authen parameter**
Description	This command is used to display the authentication parameters currently configured on the Switch, including the response timeout and user authentication attempts. This command will display the following fields: Response timeout – The configured time allotted for the Switch to wait for a response of authentication from the user attempting to log in from the command line interface or telnet interface. User attempts – The maximum number of attempts the user may try to become authenticated by the Switch, before being locked out.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To view the authentication parameters currently set on the Switch:

```
DGS-3426:5#show authen parameter
Command: show authen parameter

Response timeout : 60 seconds
User attempts    : 5

DGS-3426:5#
```

enable admin

Purpose	Used to promote user level privileges to administrator level privileges
Syntax	**enable admin**
Description	This command is for users who have logged on to the Switch on the normal user level, to become promoted to the administrator level. After logging on to the Switch users will have only user level privileges. To gain access to administrator level privileges, the user will enter this command and will have to enter an authentication password. Possible authentication methods for this function include TACACS, XTACACS, TACACS+, RADIUS, user defined server groups, local enable (local account on the Switch), or no authentication (*none*). Because XTACACS and TACACS do not support the enable function, the user must create a special account on the server host which has the username “enable”, and a password configured by the administrator that will support the “enable” function. This function becomes inoperable when the authentication policy is disabled.
Parameters	None.
Restrictions	None.

Example usage:

To enable administrator privileges on the Switch:

```
DGS-3426:5#enable admin
Password: ******

DGS-3426:5#
```

config admin local_enable	
Purpose	Used to configure the local enable password for administrator level privileges.
Syntax	**config admin local_enable**
Description	This command is used to configure the locally enabled password for the **enable admin** command. When a user chooses the "*local_enable*" method to promote user level privileges to administrator privileges, he or she will be prompted to enter the password configured here, that is set locally on the Switch.
Parameters	*<password 15>* – After entering this command, the user will be prompted to enter the old password, then a new password in an alphanumeric string of no more than 15 characters, and finally prompted to enter the new password again for confirmation. See the example below.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the password for the "local_enable" authentication method.

```
DGS-3426:5#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-3426:5#
```

35

SSH COMMANDS

The steps required to use the Secure Shell (SSH) protocol for secure communication between a remote PC (the SSH Client) and the Switch (the SSH Server), are as follows:

- Create a user account with admin–level access using the **create account admin <username> <password>** command. This is identical to creating any other admin–lever user account on the Switch, including specifying a password. This password is used to login to the Switch, once secure communication has been established using the SSH protocol.
- Configure the user account to use a specified authorization method to identify users that are allowed to establish SSH connections with the Switch using the config ssh user authmode command. There are three choices as to the method SSH will use to authorize the user, and they are password, publickey and hostbased.
- Configure the encryption algorithm that SSH will use to encrypt and decrypt messages sent between the SSH Client and the SSH Server.
- Finally, enable SSH on the Switch using the **enable ssh** command.

After following the above steps, users can configure an SSH Client on the remote PC and manage the Switch using secure, in–band communication.

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

Command	Parameters
enable ssh	
disable ssh	
config ssh authmode	[password | publickey | hostbased] [enable | disable]
show ssh authmode	
config ssh server	{maxsession <int 1-8>|contimeout <sec 120-600>|authfail<int 2-20>|rekey [10min|30min|60min|never]|port <tcp_port_number 1-65535>} (1)
show ssh server	
config ssh user	<username 15> authmode [hostbased [hostname <domain_name 32> | hostname_IP <domain_name 32> <ipaddr>] | password | publickey]
show ssh user authmode	
config ssh algorithm	[3DES | AES128 | AES192 | AES256 | arcfour | blowfish | cast128 | twofish128 | twofish192 | twofish256 | MD5 | SHA1 | RSA | DSA] [enable | disable]
show ssh algorithm	

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

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

Usage example:

To enable SSH:

```
DGS-3426:5#enable ssh
Command: enable ssh

TELNET will be disabled when enable SSH.
Success.

DGS-3426:5#
```

disable ssh

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

Usage example:

To disable SSH:

```
DGS-3426:5#disable ssh
Command: disable ssh

Success.

DGS-3426:5#
```

config ssh authmode

Purpose	Used to configure the SSH authentication mode setting.
Syntax	**config ssh authmode [password | publickey | hostbased] [enable | disable]**
Description	This command is used to configure the SSH authentication mode for users attempting to access the Switch.
Parameters	*password* – This parameter may be chosen if the administrator wishes to use a locally configured password for authentication on the Switch. *publickey* – This parameter may be chosen to use a publickey configuration set on a SSH server, for authentication. *hostbased* – This parameter may be chosen to use a host computer for authentication. This parameter is intended for Linux users requiring SSH authentication techniques and the host computer is running the Linux operating system with a SSH program previously installed. *[enable | disable]* – This allows users to enable or disable SSH authentication on the Switch.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable the SSH authentication mode by password:

```
DGS-3426:5#config ssh authmode password enable
Command: config ssh authmode password enable

Success.

DGS-3426:5#
```

show ssh authmode

Purpose	Used to display the SSH authentication mode setting.
Syntax	**show ssh authmode**
Description	This command is used to display the current SSH authentication set on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To view the current authentication mode set on the Switch:

```
DGS-3426:5#show ssh authmode
Command: show ssh authmode

The SSH authmode:
Password      : Enabled
Publickey     : Enabled
Hostbased     : Enabled

DGS-3426:5#
```

config ssh server

Purpose	Used to configure the SSH server.
Syntax	**{maxsession <int 1-8>|contimeout <sec 120-600>|authfail<int 2-20>|rekey [10min|30min|60min|never]|port <tcp_port_number 1-65535>} (1)**
Description	This command is used to configure parameters for the SSH server setting on the Switch.
Parameters	*maxsession <int 1–8>* – Allows the user to set the number of users that may simultaneously access the Switch. The default setting is *8*. *contimeout <sec 120–600>* – Allows the user to set the connection timeout. The user may set a time between *120* and *600* seconds. The default is *120* seconds. *authfail <int 2–20>* – Allows the administrator to set the maximum number of attempts that a user may try to logon utilizing SSH authentication. After the maximum number of attempts is exceeded, the Switch will be disconnected and the user must reconnect to the Switch to attempt another login. *rekey [10min | 30min | 60min | never]* – Sets the time period that the Switch will change the security shell encryptions. *tcp_port_number 1-65535* – Specifies the tcp port number used to listen to the connection request from the ssh client.
Restrictions	Only Administrator and Operator-level users can issue this command.

Usage example:

To configure the SSH server:

```
DGS-3426P:5#config ssh server maxsession 3 contimeout 300 authfail 2 port 1
rekey 10min
Command: config ssh server maxsession 3 contimeout 300 authfail 2 port 1 rekey
10min

Success.

DGS-3426P:5#
```

show ssh server

Purpose	Used to display the SSH server setting.
Syntax	**show ssh server**
Description	This command is used to display the current SSH server setting.
Parameters	None.
Restrictions	None.

Usage example:

To display the SSH server:

```
DGS–3426:5# show ssh server
Command: show ssh server

SSH Server Status               : Disabled
SSH Max Session                 : 8
Connection timeout              : 120 (sec)
Authenticate failed attempts    : 2
Rekey timeout                   : never
Listened Port Number            : 22

DGS–3426:5#
```

config ssh user

Purpose	Used to configure the SSH user.
Syntax	**config ssh user <username 15> authmode [hostbased [hostname <domain_name 32> | hostname_IP <domain_name 32> <ipaddr>] | password | publickey]**
Description	This command is used to configure the SSH user authentication method.
Parameters	*<username 15>* – Enter a username of no more than 15 characters to identify the SSH user. *authmode* – Specifies the authentication mode of the SSH user wishing to log on to the Switch. The administrator may choose between: *hostbased* – This parameter should be chosen to use a remote SSH server for authentication purposes. Choosing this parameter requires the user to input the following information to identify the SSH user. *hostname <domain_name 32>* – Enter an alphanumeric string of up to 32 characters identifying the remote SSH user. *hostname_IP <domain_name 32> <ipaddr>* – Enter the hostname and the corresponding IP address of the SSH user. *password* – This parameter should be 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-3426:5# config ssh user Rubio authmode Password
Command: config ssh user Rubio authmode Password

Success.

DGS-3426:5#
```

show ssh user authmode

Purpose	Used to display the SSH user setting.
Syntax	**show ssh user authmode**
Description	This command is used to display the current SSH user setting.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command..

Example usage:

To display the SSH user:

```
DGS-3426:5#show ssh user authmode
Command: show ssh user authmode

Current Accounts:
UserName       Authentication      Host Name       Host IP
------------   -----------------   -------------   ---------
Rubio          Hostbased           12334           10.45.25.8

DGS-3426:5#
```

NOTE: To configure the SSH user, the administrator must create a user account on the Switch. For information concerning configuring a user account, please see the section of this manual entitled **Basic Switch Commands** and then the command, **create account user**.

config ssh algorithm

Purpose	Used to configure the SSH algorithm.
Syntax	**config ssh algorithm [3DES | AES128 | AES192 | AES256 | arcfour | blowfish | cast128 | twofish128 | twofish192 | twofish256 | MD5 | SHA1 | RSA | DSA] [enable | disable]**
Description	This command is used to configure the desired type of SSH algorithm used for authentication encryption.
Parameters	*3DES* – This parameter will enable or disable the Triple_Data Encryption Standard encryption algorithm. *AES128* – This parameter will enable or disable the Advanced Encryption Standard AES128 encryption algorithm. *AES192* – This parameter will enable or disable the Advanced Encryption Standard AES192 encryption algorithm. *AES256* – This parameter will enable or disable the Advanced Encryption Standard AES256 encryption algorithm. *arcfour* – This parameter will enable or disable the Arcfour encryption algorithm. *blowfish* – This parameter will enable or disable the Blowfish encryption algorithm. *cast128* – This parameter will enable or disable the Cast128 encryption algorithm. *twofish128* – This parameter will enable or disable the twofish128 encryption algorithm. *twofish192* – This parameter will enable or disable the twofish192 encryption algorithm. *MD5* – This parameter will enable or disable the MD5 Message Digest encryption algorithm. *SHA1* – This parameter will enable or disable the Secure Hash Algorithm encryption. *RSA* – This parameter will enable or disable the RSA encryption algorithm. *DSA* – This parameter will enable or disable the Digital Signature Algorithm encryption. *[enable* | *disable]* – This allows users to enable or disable algorithms entered in this command, on the Switch.
Restrictions	Only Administrator and Operator-level users can issue this command.

Usage example:

To configure SSH algorithm:

```
DGS-3426:5#config ssh algorithm Blowfish enable
Command: config ssh algorithm Blowfish enable

Success.

DGS-3426:5#
```

show ssh algorithm

Purpose	Used to display the SSH algorithm setting.
Syntax	**show ssh algorithm**
Description	This command is used to display the current SSH algorithm setting status.
Parameters	None.
Restrictions	None.

Usage Example:

To display SSH algorithms currently set on the Switch:

```
DGS-3426:5#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-3426:5#
```

36

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.

The Secure Sockets Layer (SSL) commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameters
enable ssl	{ciphersuite {RSA_with_RC4_128_MD5 | RSA_with_3DES_EDE_CBC_SHA | DHE_DSS_with_3DES_EDE_CBC_SHA | RSA_EXPORT_with_RC4_40_MD5} (1) }
disable ssl	{ciphersuite {RSA_with_RC4_128_MD5 | RSA_with_3DES_EDE_CBC_SHA | DHE_DSS_with_3DES_EDE_CBC_SHA | RSA_EXPORT_with_RC4_40_MD5} (1) }
config ssl cachetimeout	<value 60–86400>
show ssl	{certificate}
show ssl cachetimeout	
download ssl certificate	<ipaddr> certfilename <path_filename 64> keyfilename <path_filename 64>

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

enable ssl

Purpose	To enable the SSL function on the Switch.
Syntax	**enable ssl {ciphersuite {RSA_with_RC4_128_MD5 | RSA_with_3DES_EDE_CBC_SHA | DHE_DSS_with_3DES_EDE_CBC_SHA | RSA_EXPORT_with_RC4_40_MD5} (1) }**
Description	This command is used to enable SSL on the Switch by implementing any one or combination of listed ciphersuites on the Switch. Entering this command without a parameter will enable the SSL status on the Switch. Enabling SSL will disable the web–manager on the Switch.
Parameters	*ciphersuite* – A security string that determines the exact cryptographic parameters, specific encryption algorithms and key sizes to be used for an authentication session. The user may choose any combination of the following: • *RSA_with_RC4_128_MD5* – This ciphersuite combines the RSA key exchange, stream cipher RC4 encryption with 128–bit keys and the MD5 Hash Algorithm. • *RSA_with_3DES_EDE_CBC_SHA* – This ciphersuite combines the RSA key exchange, CBC Block Cipher 3DES_EDE encryption and the SHA Hash Algorithm. • *DHE_DSS_with_3DES_EDE_CBC_SHA* – This ciphersuite combines the DSA Diffie Hellman key exchange, CBC Block Cipher 3DES_EDE encryption and SHA Hash Algorithm. • *RSA_EXPORT_with_RC4_40_MD5* – This ciphersuite combines the RSA Export key exchange, stream cipher RC4 encryption with 40–bit keys. The ciphersuites are enabled by default on the Switch, yet the SSL status is disabled by default. Enabling SSL with a ciphersuite will not enable the SSL status on the Switch.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable SSL on the Switch for all ciphersuites:

```
DGS-3426:5#enable ssl
Command:enable ssl

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

DGS-3426:5#
```

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} (1) }**
Description	This command is used to disable SSL on the Switch and can be used to disable any one or combination of listed ciphersuites on the Switch.
Parameters	*ciphersuite* – A security string that determines the exact cryptographic parameters, specific encryption algorithms and key sizes to be used for an authentication session. The user may choose any combination of the following: • *RSA_with_RC4_128_MD5* – This ciphersuite combines the RSA key exchange, stream cipher RC4 encryption with 128–bit keys and the MD5 Hash Algorithm. • *RSA_with_3DES_EDE_CBC_SHA* – This ciphersuite combines the RSA key exchange, CBC Block Cipher 3DES_EDE encryption and the SHA Hash Algorithm. • *DHE_DSS_with_3DES_EDE_CBC_SHA* – This ciphersuite combines the DSA Diffie Hellman key exchange, CBC Block Cipher 3DES_EDE encryption and SHA Hash Algorithm. • *RSA_EXPORT_with_RC4_40_MD5* – This ciphersuite combines the RSA Export key exchange, stream cipher RC4 encryption with 40–bit keys.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable the SSL status on the Switch:

```
DGS-3426:5#disable ssl
Command: disable ssl

Success.

DGS-3426:5#
```

To disable ciphersuite *RSA_EXPORT_with_RC4_40_MD5* only:

```
DGS-3426:5#disable ssl ciphersuite RSA_EXPORT_with_RC4_40_MD5
Command: disable ssl ciphersuite RSA_EXPORT_with_RC4_40_MD5

Success.

DGS-3426:5#
```

config ssl cachetimeout

Purpose	Used to configure the SSL cache timeout.
Syntax	**config ssl cachetimeout <value 60–86400>**
Description	This command is used to set the time between a new key exchange between a client and a host using the SSL function. A new SSL session is established every time the client and host go through a key exchange. Specifying a longer timeout will allow the SSL session to reuse the master key on future connections with that particular host, therefore speeding up the negotiation process.
Parameters	*timeout <value 60–86400>* – Enter a timeout value between *60* and *86400* seconds to specify the total time an SSL key exchange ID stays valid before the SSL module will require a new, full SSL negotiation for connection. The default cache timeout is 600 seconds
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To set the SSL cachetimeout for 7200 seconds:

```
DGS-3426:5#config ssl cachetimeout timeout 7200
Command: config ssl cachetimeout timeout 7200

Success.

DGS-3426:5#
```

show ssl cachetimeout

Purpose	Used to show the SSL cache timeout.
Syntax	**show ssl cachetimeout**
Description	This command is used to view the SSL cache timeout currently implemented on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To view the SSL cache timeout on the Switch:

```
DGS-3426:5#show ssl cachetimeout
Command: show ssl cachetimeout

Cache timeout is 600 second(s).

DGS-3426:5#
```

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	certificate – Adding this parameter will allow the user to view the SSL certificate file information currently implemented on the Switch.
Restrictions	None.

Example usage:

To view the SSL status on the Switch:

```
DGS-3426:5#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-3426:5#
```

Example usage:

To view certificate file information on the Switch:

```
DGS-3426:5#show ssl certificate
Command: show ssl certificate

Loaded with RSA Certificate!

DGS-3426:5#
```

download SSL certificate

Purpose	Used to download a certificate file for the SSL function on the Switch.
Syntax	**download SSL certificate <ipaddr> certfilename <path_filename 64> keyfilename <path_filename 64>**
Description	This command is used to download a certificate file for the SSL function on the Switch from a TFTP server. The certificate file is a data record used for authenticating devices on the network. It contains information on the owner, keys for authentication and digital signatures. Both the server and the client must have consistent certificate files for optimal use of the SSL function. The Switch only supports certificate files with .der file extensions.
Parameters	*<ipaddr>* – Enter the IP address of the TFTP server. *certfilename <path_filename 64>* – Enter the path and the filename of the certificate file to download. *keyfilename <path_filename 64>* – Enter the path and the filename of the key exchange file to download.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To download a certificate file and key file to the Switch:

```
DGS-3426:5#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-3426:5#
```

37

JUMBO FRAME COMMANDS

Certain switches can support jumbo frames (frames larger than 1536 bytes). To transmit frames of up to 9K (and 9220 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 is used to allow ethernet frames larger than 1536 bytes to be processed by the Switch. The maximum size of the jumbo frame may not exceed 9220 Bytes tagged.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable the jumbo frame function on the Switch:

```
DGS-3426:5#enable jumbo_frame
Command: enable jumbo_frame

Success.

DGS-3426:5#
```

disable jumbo_frame

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

Example usage:

To disable the jumbo frame function on the Switch:

```
DGS-3426:5#disable jumbo_frame
Command: disable jumbo_frame

Success.

DGS-3426:5#
```

show jumbo_frame

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

Usage Example:

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

```
DGS-3426:5#show jumbo_frame
Command: show jumbo_frame

Jumbo frame state : disabled
Maximum Jumbo frame size : 1536 bytes.

DGS-3426:5#
```

D–Link Single IP Management (SIM) Commands

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

- SIM is an optional feature on the Switch and can easily be enabled or disabled. SIM grouping has no effect on the normal operation of the Switch in the user's network.
- There are three classifications for switches using SIM. The Commander Switch(CS), which is the master switch of the group, Member Switch(MS), which is a switch that is recognized by the CS a member of a SIM group, and a Candidate Switch(CaS), which is a switch that has a physical link to the SIM group but has not been recognized by the CS as a member of the SIM group.
- A SIM group can only have one Commander Switch(CS).
- All switches in a particular SIM group must be in the same broadcast domain.
- A SIM group accepts up to 32 switches (numbered 0–32), including the Commander Switch (numbered 0).
- There is no limit to the number of SIM groups in the same broadcast domain, however a single switch can only belong to one group.
- If multiple VLANs are configured, the SIM group will only utilize the default VLAN on any switch.
- SIM allows intermediate devices that do not support SIM. This enables the user to manage a switch that are more than one hop away from the CS.

The SIM group is a group of switches that are managed as a single entity. The xStack® DGS–3400 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 xStack® DGS–3400, 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–3400 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 CaS 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.

Upgrade to v1.61

To better improve SIM management, the xStack® DGS–3400 series switches have been upgraded to version 1.61 in this release. Many improvements have been made, including:

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

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

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

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 is used to enable SIM globally on the Switch. SIM features and functions will not function properly unless this function is enabled.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable SIM on the Switch:

```
DGS-3426:5#enable sim
Command: enable sim

Success.

DGS-3426:5#
```

disable sim

Purpose	Used to disable Single IP Management (SIM) on the Switch.
Syntax	**disable sim**
Description	This command is used to 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-3426:5#disable sim
Command: disable sim

Success.

DGS-3426:5#
```

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 is used to display the current information regarding the SIM group on the Switch, including the following: SIM Version – Displays the current Single IP Management version on the Switch. Firmware Version – Displays the current Firmware version on the Switch. Device Name – Displays the user–defined device name on the Switch. MAC Address – Displays the MAC Address of the Switch. Capabilities – Displays the type of switch, be it Layer 2 (L2) or Layer 3 (L3). Platform – Switch Description including name and model number. SIM State –Displays the current Single IP Management State of the Switch, whether it be enabled or disabled. Role State – Displays the current role the Switch is taking, including Commander, Member or Candidate. A Stand–alone switch will always have the commander role. Discovery Interval – Time in seconds the Switch will send discovery packets out over the network. Hold time – Displays the time in seconds the Switch will hold discovery results before dropping it or utilizing it.
Parameters	*candidates <candidate_id 1–100>* – Entering this parameter will display information concerning candidates of the SIM group. To view a specific candidate, include that candidate's ID number, listed from 1 to 100. *members <member_id 1–32>* – Entering this parameter will display information concerning members of the SIM group. To view a specific member, include that member's ID number, listed from 1 to 32. *group {commander_mac <macaddr>}* – Entering this parameter will display information concerning the SIM group. To view a specific group, include the commander's MAC address of the group. *neighbor* – Entering this parameter will display neighboring devices of the Switch. A SIM neighbor is defined as a switch that is physically connected to the Switch but is not part of the SIM group. This screen will produce the following results: ▪ Port – Displays the physical port number of the commander switch where the uplink to the neighbor switch is located. ▪ MAC Address – Displays the MAC Address of the neighbor switch. ▪ Role – Displays the role(CS, CaS, MS) of the neighbor switch.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To display the SIM information in detail:

```
DGS-3426:5#show sim
Command: show sim

SIM Version        : VER-1.61
Firmware Version   : 2.35-B06
Device Name        :
MAC Address        : 00-19-5B-3D-7C-D6
Capabilities       : L2
Platform           : DGS-3426 L2 Switch
SIM State          : Disabled
Role State         : Candidate
Discovery Interval : 30 sec
Hold Time          : 100 sec

DGS-3426:5#
```

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

```
DGS-3426:5#show sim candidates 1-2
Command: show sim candidates 1-2

ID   MAC Address       Platform /           Hold     Firmware     Device Name
                       Capability           Time     Version
---   ---------------   ------------------   -----    ---------    -------------
1   00-01-02-03-04-00   DGS-3400 L2 Switch   40      2.00.B46      The Man
2   00-55-55-00-55-00   DGS-3400 L2 Switch   140     2.00.B46      default
master

Total Entries: 2

DGS-3426:5#
```

To display the member information in summary, if the member ID is specified:

```
DGS-3426:5#show sim member 1-2
Command: show sim member 1-2

ID   MAC Address      Platform /            Hold     Firmware      Device Name
                      Capability            Time     Version
---   --------------   -----------------     ----      -------      -----------
1    00-01-02-03-04-00 DGS-3400 L2 Switch    40        2.00.B46      The Man
2    00-55-55-00-55-00 DGS-3400 L2 Switch    140       2.00.B46      default
master

Total Entries: 2

DGS-3426:5#
```

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

```
DGS-3426:5#show sim group
Command: show sim group

SIM Group Name : default

ID  MAC Address        Platform /          Hold      Firmware     Device Name
                       Capability          Time      Version
---  --------------    ---------------     -----      ---------   -------------
*1  00-01-02-03-04-00  DGS-3400 L2 Switch    40      2.00.B46    Trinity
 2  00-55-55-00-55-00  DGS-3400 L2 Switch    140     2.00.B46    default master

SIM Group Name : SIM2

ID  MAC Address        Platform /          Hold      Firmware   Device Name
                       Capability          Time      Version
---  --------------    ---------------     -----      --------  --------------
*1  00-01-02-03-04-00  DGS-3400 L2 Switch   40       2.00.B46    Neo
 2  00-55-55-00-55-00  DGS-3400 L2 Switch   140      2.00.B46    default master

'*' means commander switch.

DGS-3426:5#
```

Example usage:

To view SIM neighbors:

```
DGS-3426:5#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-3426:5#
```

reconfig

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

Example usage:

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

```
DGS-3426:5#reconfig  member_id 2
Command: reconfig  member_id 2


DGS-3426:5#
Login:
```

config sim_group

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

Example usage:

To add a member:

```
DGS-3426:5#config sim_group add 2
Command: config sim_group add 2

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

Success.

DGS-3426:5#
```

To delete a member:

```
DGS-3426:5#config sim_group delete 1
Command: config sim_group delete 1

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

Success.

DGS-3426:5#
```

config sim

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

Example usage:

To change the time interval of the discovery protocol:

```
DGS-3426:5# config sim commander
Command: config sim commander

Success.

DGS-3426:5#
```

To change the hold time of the discovery protocol:

```
DGS-3426:5# config sim hold_time 120
Command: config sim hold_time 120

Success.

DGS-3426:5#
```

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

```
DGS-3426:5# config sim candidate
Command: config sim candidate

Success.

DGS-3426:5#
```

To transfer the Switch to be a CS:

```
DGS-3426:5# config sim commander
Command: config sim commander

Success.

DGS-3426:5#
```

To update the name of a group:

```
DGS-3426:5#config sim commander group_name Trinity
Command: config sim commander group_name Trinity

Success.

DGS-3426:5#
```

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 is used to download a firmware file or configuration file to a specified device from a TFTP server.
Parameters	*firmware_from_tftp* – Specify this parameter to download firmware to members of a SIM group. *configuration_from_tftp* – Specify this parameter to download a switch configuration to members of a SIM group. *<ipaddr>* – Enter the IP address of the TFTP server. *<path_filename>* – Enter the path and the filename of the firmware or switch on the TFTP server. *members* – Enter this parameter to specify the members to which to download firmware or switch configuration files. The user may specify a member or members by adding one of the following: ▪ *<mslist 1–32>* – Enter a value, or values to specify which members of the SIM group will receive the firmware or switch configuration. ▪ *all* – Add this parameter to specify all members of the SIM group will receive the firmware or switch configuration.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To download firmware:

```
DGS-3426:5# download sim_ms firmware_from_tftp 10.53.13.94 c:/dgs3426.had all
Command: download sim_ms firmware_from_tftp 10.53.13.94 c:/dgs3426.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-3426:5#
```

To download configuration files:

```
DGS-3426:5# download sim configuration_from_tftp 10.53.13.94 c:/ dgs3426.txt
all
Command: download sim configuration_from_tftp 10.53.13.94 c:/ dgs3426.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-3426:5#
```

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 is used to upload a configuration file to a TFTP server from a specified member of a SIM group.
Parameters	*configuration_to_tftp* – Specify this parameter if the user wishes to upload a switch configuration to members of a SIM group. *log_to_tftp* – Specify this parameter if the user wishes to upload a switch log to members of a SIM group. *<ipaddr>* – Enter the IP address of the TFTP server to which to upload a configuration file. *<path_filename>* – Enter a user–defined path and file name on the TFTP server to which to upload configuration files. *members* – Enter this parameter to specify the members to which to upload switch configuration or log files. The user may specify a member or members by adding one of the following: ▪ *<mslist>* – Enter a value, or values to specify which members of the SIM group will upload the switch configuration or log files. ▪ *all* – Add this parameter to specify all members of the SIM group will upload the switch configuration or log files.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To upload configuration files to a TFTP server:

```
DGS-3426:5# 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


This device is upload configuration. Please wait several minutes…


Success.


DGS-3426:5#
```

39

POE COMMANDS

The xStack® DGS–3426P supports Power over Ethernet (PoE) as defined by the IEEE 802.3af specification. Ports 1–24 supply 48 VDC power to PDs over Category 5 or Category 3 UTP Ethernet cables. The xStack® DGS–3426P follows the standard PSE pinout *Alternative A*, whereby power is sent out over pins 1, 2, 3 and 6. The xStack® DGS–3426P works with all D – Link 802.3af capable devices.

The xStack® DGS–3426P includes the following PoE features:

- The auto–discovery feature recognizes the connection of a PD (Powered Device) and automatically sends power to it.
- The auto–disable feature will occur under two conditions: first, if the total power consumption exceeds the system power limit; and second, if the per port power consumption exceeds the per port power limit.
- The active circuit protection feature automatically disables the port if there is a short. Other ports will remain active.

PDs receive power according to the following classification:

Class	**Max power used by PD**
0	0.44 to 12.95W
1	0.44 to 3.84W
2	3.84 to 6.49W
3	6.49 to 12.95W

PSE provides power according to the following classification:

Class	**Max power provided by PSE**
0	15.4W
1	4.0W
2	7.0W
3	15.4W

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

Command	Parameters
config poe system	{units [<unitlist> | all]} {power_limit <value 37–370> | power_disconnect_method [deny_next_port | deny_low_priority_port] management_mode [power_limit | auto]} (1)
config poe ports	[all | <portlist>] {state [enable | disable] | priority [critical | high | low] | power_limit [class_0 | class_1 | class_2 | class_3 | user_define <value 1000–16800>]} (1)
show poe ports	{<portlist>}
show poe system	{units <unitlist>}

Each command is listed in detail in the following sections.

config poe system

Purpose	Used to configure the parameters for the whole PoE system.
Syntax	**config poe system {units [<unitlist> | all]} {power_limit <value 37–370> | power_disconnect_method [deny_next_port | deny_low_priority_port] management_mode [power_limit | auto]} (1)**
Description	This command is used to configure the parameters for the whole PoE system.
Parameters	*units <unitlist>* – Enter the switch in the switch stack for which to configure the PoE system. This number is based on the unit ID assigned to the switch in the switch stack. The DGS–3426P is the only switch in this series with PoE capabilities. *power_limit* – The power limit parameter allows the user to configure the power budget of whole PoE system. The minimum setting is 37 W and the maximum is 370W (depending on the power supplier's capability). Default setting is 370 W. *power_disconnect_method* –This parameter is used to configure the power management disconnection method. When the total consumed power exceeds the power budget, the PoE controller initiates a port disconnection to prevent overloading the power supply. The controller uses one of the following two ways to implement the disconnection: • *deny_next_port* – After the power budget has been exceeded, the next port attempting to power up is denied, regardless of its priority. • *deny_low_priority_port* – After the power budget has been exceeded, the next port attempting to power up, causes the port with the lowest priority to shut down (to allow high - priority ports to power up). The default setting is *deny_next_port*. *management_mode* – Use this parameter to utilize the PoE management mode function of this switch. The user has two choices: • *power_limit* – Choose this option to shut down the port if the power limit on the port exceeds the limit stated by the user configured in the *power_limit* field. • *auto* – Choose this field to automatically disconnect the power from a given port when it exceeds the maximum power used, as defined by the PD's (power device) power class, stated previously in this section. When a PD is attached to a port on the Switch, the Power Class is automatically determined. If the PD's power class is unspecified or there is an error in determining the power class, it is given the power class zero (0).
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To config the PoE System on the Switch:

```
DGS-3426P:5#config poe system units 1 power_limit 300 power_disconnect_method
deny_next_port management_mode auto
Command: config poe system units 1 power_limit 300 power_disconnect_method
deny_next_port management_mode auto

Success.

DGS-3426P:5#
```

config poe ports	
Purpose	Used to configure the PoE port settings.
Syntax	**config poe ports [all | <portlist>] {state [enable | disable] | priority [critical | high | low] | power_limit [class_0 | class_1 | class_2 | class_3 | user_define <value 1000–16800>]} (1)**
Description	This command is used to configure the PoE port settings.
Parameters	*<portlist>* –Specifies a range of ports to be configured or all the ports. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3–2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. Non–contiguous portlist entries are separated by a comma. (ex: 1:1–1:3,1:7–1:9) *all* – Specifies that all ports on the Switch will be configured for PoE. *state* – Enables or disables the PoE function on the Switch. *priority* – Setting the port priority affects power – up order and shutdown order. Power–up order: When the Switch powers–up or reboots, the ports are powered up according to their priority (*critical* first, then *high* and finally *low*). Shutdown order: When the power limit has been exceeded, the ports will shut down according to their priority if the power disconnect method is set to *deny_ low_priority_port.* • *critical* – Specifying this parameter will nominate these ports has having the highest priority for all configured PoE ports. These ports will be the first ports to receive power and the last to disconnect power. • *high* – Specifying this parameter will nominate these ports as having the second highest priority for receiving power and shutting down power. • *low* – Specifying this parameter will nominate these ports as having the lowest priority for receiving and shutting down power. These ports will be the first ports to have their power disconnected if the *power_disconnect_method* chosen in the **config poe system** command is *deny_low_priority_port*. *power_limit* – Allows the user to configure the per – port power limit. If a port exceeds its power limit, the PoE system will shut down that port. The minimum user–defined setting is 1000mW and maximum is 16800mW. The default setting is 15400mW. The user may also choose to define a power class by which to set the power limit, based on the PSE table at the beginning of this section. • *class_0* – Choosing this class will set the maximum port limit at 15.4W. • *class_1* – Choosing this class will set the maximum port limit at 4.0W. • *class_2* – Choosing this class will set the maximum port limit at 7.0W. • *class_3* – Choosing this class will set the maximum port limit at 15.4.0W. • *user_define* – Choosing this parameter will allow the user to set a power limit between 1000 and 16800mW with a default value of 15400mW.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To config the Switch’s ports for PoE:

```
DGS-3426P:5#config poe ports 1:1-1:3 state enable priority critical power_limit
class_0
Command: config poe ports 1:1-1:3 state enable priority critical power_limit
class_0

Power limit has been set to 15400mW(Class 0 PD upper power limit 12.95W + power
loss on cable).
Success.

DGS-3426P:5#
```

show poe ports

Purpose	Used to display the setting and actual values of the whole PoE system.
Syntax	**show poe ports {<portlist>}**
Description	This command is used to display the settings, actual values, and port configuration of the whole PoE system.
Parameters	*ports* – Choosing this parameter will display the settings for PoE on a port–by–port basis. • *portlist* – Enter a port or range of ports to be displayed for their PoE settings. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3–2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. Non–contiguous portlist entries are separated by a comma. (ex: 1:1–1:3,1:7–1:9)
Restrictions	None.

Example usage:

To display the power settings for the switch’s ports.

```
DGS-3426P:5#show poe ports
Command: show poe ports
Port     State            Priority            Power Limit(mW)
            Class            Power(mW)     Voltage(decivolt)        Current (mA)
            Status
=================================================================================
1:1       Enabled      Critical            12000(User-defined)
            0                  0                        0
0
            OFF   : Non-standard PD connected
1:2       Enabled      Critical            12000(User-defined)
             0                  0                       0
0
            OFF   : Interim state during line detection
1:3       Enabled      Critical            12000(User-defined)
            0                   0                        0
0
            OFF   : Interim state during line detection
1:4       Enabled      Low                 15400(User-defined)
            0                   0                        0
0
            OFF   : Interim state during line detection
1:5       Enabled      Low                 15400(User-defined)
            0                   0                        0
0
            OFF   : Interim state during line detection
1:6       Enabled      Low                 15400(User-defined)
            0                  0                        0
0
            OFF   : Interim state during line detection
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

show poe system

Purpose	Used to display the setting and actual values of the whole PoE system.
Syntax	**show poe system {units <unitlist>}**
Description	This command is used to display the system settings for PoE, such as switch power limit, consumption, remaining useable power and the power disconnection method.
Parameters	*units <unitlist>* – Select the switch in the switch stack for which to show the PoE system settings. This unit number is based on the unit ID assigned to switches in the switch stack. The DGS–3426P is currently the only switch in this series with PoE capabilities.
Restrictions	None.

Example usage:

To display the power settings for the switch system:

```
DGS–3426P:5#show poe system
Command: show poe system

Unit 1    PoE System Information
---------------------------------------------------
Power Limit                      : 300 (watts)
Power Consumption                : 0 (watts)
Power Remained                   : 300 (watts)
Power Disconnection Method : deny next port

If Power Disconnection Method is set to deny next port, then the system cannot
utilize its maximum power capacity. The maximum unused watt is 19W.

DGS–3426P:5#
```

40

COMMAND HISTORY LIST

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

Command	Parameters
?	
config command_history	<value 1–40>
show command_history	

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

?	
Purpose	Used to display all commands in the Command Line Interface (CLI).
Syntax	**? {<command>}**
Description	This command is used to 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-3426:5#?
..
?
clear
clear arptable
clear attack_log
clear counters
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 init
config 802.1x reauth
config access_profile profile_id
config account
config address_binding ip_mac ipaddress
config address_binding ip_mac ports
config admin local_enable
config arpentry

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

To display the parameters for a specific command:

```
DGS-3426:5# ? 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> | fbpdu [enable | disable]
| 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-3426:5#
```

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-3426:5#config command_history 20
Command: config command_history 20

Success.

DGS-3426:5#
```

show command_history

Purpose	Used to display the command history.
Syntax	**show command_history**
Description	This command is used to display the command history.
Parameters	None.
Restrictions	None.

Example usage

To display the command history:

```
DGS–3426:5#show command_history
Command: show command_history

?
? show
show vlan
show command history

DGS–3426:5#
```

41

MODIFY BANNER AND PROMPT COMMANDS

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

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

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

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

Example usage:

To modify the banner to read “Good evening Mr. Bond.”:

```
DGS-3426:5# config greeting_message
Command: config greeting_message

Greeting Messages Editor
================================================================
                   DGS-3426 Gigabit Ethernet Switch
                        Command Line Interface

                        Firmware: Build 2.60.B26
        Copyright(C) 2009 D-Link Corporation. All rights reserved.
================================================================

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

show greeting_message

Purpose	Used to view the currently configured greeting message configured on the Switch.
Syntax	**show greeting_message**
Description	This command is used to view the currently configured greeting message on the Switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command..

Example usage:

To view the currently configured greeting message:

```
DGS-3426:5#show greeting_message
Command: show greeting_message

=========================================================================
                    DGS-3426 Gigabit Ethernet Switch
                         Command Line Interface

                        Firmware: Build 2.60.B26
            Copyright(C) 2009 D-Link Corporation. All rights reserved.
=========================================================================

DGS-3426:5#
```

config command prompt

Purpose	Used to configure the command prompt.
Syntax	**config command_prompt [<string 16> | username | default]**
Description	This command is used to change the command prompt.
Parameters	*string 16* – The command prompt can be changed by entering a new name of no more than 16 characters. *username* – The command prompt will be changed to the login username. *default* – The command prompt will reset to factory default command prompt.
Restrictions	Only Administrator and Operator-level users can issue this command. Other restrictions include: • If the “**reset**” command is executed, the modified command prompt will remain modified. However, the “**reset system/config**” command will reset the command prompt to the original factory banner.

Example usage

To modify the command prompt to “AtYourService”:

```
DGS-3426:5#config command_prompt AtYourService
Command: config command_prompt AtYourService

Success.

AtYourService:5#
```

42

JWAC COMMANDS

The Switch’s Japanese Web-based Access Control (JWAC) commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameters
enable jwac	
disable jwac	
enable jwac redirect	
disable jwac redirect	
enable jwac forcible_logout	
disable jwac forcible_logout	
enable jwac udp_filtering	
disable jwac udp_filtering	
enable jwac quarantine_server_monitor	
disable jwac quarantine_server_monitor	
config jwac quarantine_server_error_timeout	
config jwac redirect	{destination [quarantine_server | jwac_login_page] | delay_time <sec 0 – 10>}(1)
config jwac virtual_ip	<ipaddr>
config jwac quarantine_server_url	<string 128>
config jwac clear_quarantine_server_url	
config jwac update_server	[add | delete] ipaddress <network_address> { [tcp_port <tcp_port_number 1-65535> | udp_port <udp_port_number 1-65535>]}
show jwac update_server	
config jwac switch_http_port	< tcp_port_number 1–65535> {[http | https]}
config jwac ports	[<portlist> | all] {state [enable | disable] | max_authenticating_host <value 0 – 50> | aging_time [infinite | <min 1 – 1440>] | idle_time [infinite | <min 1 – 1440>] | block_time [<sec 0 – 300>] | auth_mode [host_based | port_based] } (1)
config jwac radius_protocol	[local | pap | chap | ms_chap | ms_chapv2 | eap_md5]
create jwac user	<username 15> {vlan <vlanid 1 – 4094>}
config jwac user	<username 15> {vlan <vlanid 1 – 4094>}
delete jwac	[user <username 15> | all_users]
show jwac user	
clear jwac auth_state	[ports [all | <portlist>] {authenticated | authenticating | blocked} | mac_addr <macaddr>]
show jwac	

Command	Parameters
show jwac auth_state ports	<portlist>
show jwac ports	<portlist>
config jwac auth_failover	[enable | disable]
config jwac authorization network	{radius [enable| disable]| local [enable| disable]} (1)
config jwac authenticate_page	< japanese| english >
show jwac authenticate_page element	
config jwac authentication_page element	[japanese|english] [default|page_title <desc 128>|login_window_title <desc 32>|user_name_title <desc 16>|password_title <desc 16>| logout_window_title <desc 32>]

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

enable jwac

Purpose	Used to enable the JWAC function.
Syntax	**enable jwac**
Description	JWAC and WAC are mutually exclusive functions. They cannot be enabled simultaneously. When the JWAC function is used, PC users/end–users need to pass two stages of authentication. The first stage is to authenticate with the quarantine server and the second stage is to authenticate with the switch. For the second stage, the authentication is similar to WAC, except that there is no port VLAN membership change by JWAC after a host passes authentication. The RADIUS server will share the server's configuration defined by the 802.1X command set.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable the JWAC function on the Switch:

```
DGS-3426:5#enable jwac
Command: enable jwac

Success.

DGS-3426:5#
```

disable jwac

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

Example usage:

To disable the JWAC function on the Switch:

```
DGS-3426:5#disable jwac
Command: disable jwac

Success.

DGS-3426:5#
```

enable jwac redirect

Purpose	Used to enable the JWAC redirect function.
Syntax	**enable jwac redirect**
Description	When **redirect quarantine_serve**r is enabled, the unauthenticated host will be redirected to the quarantine server when it tries to access a random URL. When **redirect jwac_login_page** is enabled, the unauthenticated host will be redirected to JWAC login page in the Switch to complete the authentication. When redirect is disabled, an unauthenticated host is only allowed access to the quarantine server and the JWAC login page, all other Web access will be denied.
Parameters	None.
Restrictions	When enabling redirect to quarantine server, a quarantine server must be configured first. Only Administrator and Operator-level users can issue this command.

Example usage:

To enable JWAC redirect on the Switch:

```
DGS-3426:5#enable jwac redirect
Command: enable jwac redirect

Success.

DGS-3426:5#
```

disable jwac redirect

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

Example usage:

To enable JWAC redirect on the Switch:

```
DGS-3426:5#disable jwac redirect
Command: disable jwac redirect

Success.

DGS-3426:5#
```

enable jwac forcible_logout

Purpose	Used to enable the JWAC forcible logout function.
Syntax	**enable jwac forcible_logout**
Description	When forcible logout is enabled, a PING packet from an authenticated host to the JWAC Switch with TTL=1 will be regarded as a logout request, and the host will be moved back to the unauthenticated state.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable JWAC forcible logout on the Switch:

```
DGS-3426:5# enable jwac forcible_logout
Command: enable jwac forcible_logout

Success.

DGS-3426:5#
```

disable jwac forcible_logout

Purpose	Used to disable the JWAC forcible logout function.
Syntax	**disable jwac forcible_logout**
Description	This command is used to disable the JWAC forcible logout function.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable JWAC forcible logout on the Switch:

```
DGS-3426:5# disable jwac forcible_logout
Command: disable jwac forcible_logout

Success.

DGS-3426:5#
```

enable jwac udp_filtering

Purpose	Used to enable the JWAC UDP filtering function.
Syntax	**enable jwac udp_filtering**
Description	When UDP filtering is enabled, all UDP and ICMP packets except DHCP and DNS packets from an unauthenticated hosts will be dropped
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable the JWAC UDP filtering function:

```
DGS-3426:5#enable jwac udp_filtering
Command: enable jwac udp_filtering

Success.

DGS-3426:5#
```

disable jwac udp_filtering

Purpose	Used to disable the JWAC UDP filtering function.
Syntax	**disable jwac udp_filtering**
Description	This command is used to disable JWAC UDP filtering
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable the JWAC UDP filtering function:

```
DGS-3426:5#disable jwac udp_filtering
Command: disable jwac udp_filtering

Success.

DGS-3426:5#
```

enable jwac quarantine_server_monitor

Purpose	Used to enable the JWAC quarantine server monitor.
Syntax	**enable jwac quarantine_server_monitor function**
Description	When the JWAC quarantine server monitor is enabled, the Switch will monitor the Quarantine Server to ensure that it is functioning properly. If the Switch does not detect the Quarantine Server, it will redirect all unauthenticated HTTP requests to the JWAC Login Page by force provided the redirect quarantine server is enabled and the redirect destination is configured as the Quarantine Server.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable the JWAC quarantine server monitor:

```
DGS-3426:5# enable jwac quarantine_server_monitor
Command: enable jwac quarantine_server_monitor

Success.

DGS-3426:5#
```

disable jwac quarantine_server_monitor

Purpose	Used to disable the JWAC quarantine server monitor.
Syntax	**disable jwac quarantine_server_monitor function**
Description	This command is used to disable the JWAC quarantine server monitor.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable the JWAC quarantine server monitor:

```
DGS-3426:5# disable jwac quarantine_server_monitor
Command: disable jwac quarantine_server_monitor

Success.

DGS-3426:5#
```

config jwac quarantine_server_error_timeout

Purpose	Used to set quarantine server error timeout.
Syntax	**config jwac quarantine_server_error_timeout <sec 5–300>**
Description	When the quarantine server error timeout is enabled, the Switch will periodically check if the server is functioning properly. If the Switch does not receive any responses from the quarantine server during the configured error timeout interval, the Switch then regards it as not working properly.
Parameters	*<sec 5–300>* – To specify the error timeout interval
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the JWAC quarantine server error timeout:

```
DGS-3426:5#config jwac quarantine_server_error_timeout 60
Command: config jwac quarantine_server_error_timeout 60

Success.

DGS-3426:5#
```

config jwac redirect

Purpose	Used to configure redirect destination and delay time before an unauthenticated host is redirected to the Quarantine Server or the JWAC login Web page.
Syntax	**config jwac redirect {destination [quarantine_server | jwac_login_page] | delay_time <sec 0 – 10>}**
Description	This command allows you to configure redirect destination and delay time before an unauthenticated host is redirected to the Quarantine Server or the JWAC login Web page. The unit of delay_time is in seconds. 0 means there is no delay in redirection.
Parameters	*destination* –To specify the destination which the unauthenticated host will be redirected to. *delay_time* – To specify the time interval after which the unauthenticated host will be redirected.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the JWAC redirect on the Switch:

```
DGS-3426:5# config jwac redirect destination jwac_login_page delay_time 5
Command: config jwac redirect_ destination jwac_login_page delay_time 5

Success.

DGS-3426:5#
```

config jwac virtual_ip

Purpose	Used to configure jwac virtual ipaddress. This IP is for accepting authentication request from unauthenticated host.
Syntax	**config jwac virtual_ip <ipaddr>**
Description	The virtual IP of JWAC is for accepting authentication requests from unauthenticated hosts. Only requests sent to this IP will get a valid response. This IP does not respond to ARP requests or ICMP packets! Do NOT set this IP on the same subnet as the client PC and the Switch’s IPIF (IP interface). Note: the IP address being set shall NOT be identical to any devices in the network, otherwise this will create problem to the original host holding that IP address.
Parameters	*<ipaddr>* – To specify the IP address of the virtual IP.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the JWAC virtual IP:

```
DGS-3426:5#config jwac virtual_ip 1.1.1.1
Command: config jwac virtual_ip 1.1.1.1

Success.

DGS-3426:5#
```

config jwac quarantine_server_url

Purpose	Used to configure JWAC Quarantine Server URL.
Syntax	**config jwac quarantine_server_url <string 128>**
Description	This command allows you to configure the URL of the quarantine server. If the redirect is enabled and the redirect destination is the quarantine server, when an HTTP request from an unauthenticated host reaches the Switch, the Switch will process this HTTP packet and response a message back to the host to ensure it access the quarantine server with the configured URL. When the PC connects to the specified URL, the quarantine server will request the PC user/End–user to input the user name and password to perform authentication.
Parameters	*<string 128>* – To specify the entire URL address of the authentication page of the quarantine server.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the JWAC quarantine server URL:

```
DGS-3426:5#config jwac quarantine_server_url http://10.90.90.88/authpage.html
Command: config jwac quarantine_server_url http://10.90.90.88/authpage.html

Success.

DGS-3426:5#
```

NOTE: If the quarantine server is linked to the JWAC enabled port on the switch, it must be added to the static FDB correctly before it can work properly.

config jwac clear_quarantine_server_url

Purpose	Used to clear the quarantine server configuration.
Syntax	**config jwac clear_quarantine_server_url**
Description	This command is used to clear the quarantine server configuration
Parameters	None
Restrictions	When JWAC is enabled and the redirect destination is the quarantine server, the quarantine server cannot be cleared. Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the JWAC clear quarantine server URL:

```
DGS-3426:5#config jwac clear_quarantine_server_url
Command: config jwac clear_quarantine_server_url

Success.

DGS-3426:5#
```

config jwac update_server

Purpose	Used to configure the servers that the PC may need to connect to in order to complete the JWAC authentication
Syntax	**config jwac update_server [add | delete] ipaddress <network_address> { [tcp_port <tcp_port_number 1-65535> | udp_port <udp_port_number 1-65535>]}**
Description	This command allows a user to add or delete server network addresses to which the traffic from unauthenticated client hosts will not be blocked by the JWAC Switch. Any servers that need ActiveX to accomplish authentication before the client passes the authentication process should be added to the Switch by their IP address. For example, the client may need to access update.microsoft.com or some Anti – Virus software company's website to check whether the OS or Anti – Virus software of the client is up–to–date; and so these IP addresses need to be added to the Switch.
Parameters	*add* – To add a network address to which the traffic will not be blocked You can add 5 network addresses at most *delete* – To delete a network address to which the traffic will not be blocked *ipaddress* – To specify the network address to add or delete To set a specific IP address, please use the format x.x.x.x/32 *tcp_port*– The accessible TCP port for the specified update server network *udp_port*– The accessible UDP port for the specified update server network
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the JWAC update server:

```
DGS-3426:5#config jwac update_server add ipaddress 10.90.90.109/24
Command: config jwac update_server add ipaddress 10.90.90.109/24

 Update server 10.90.90.0/24 is added

Success.

DGS-3426:5#
```

NOTE: If the update server is linked to the JWAC enabled port on the switch, it must be added to the static FDB correctly before it can work properly.

config jwac switch_http_port

Purpose	Used to configure the TCP port which the JWAC Switch listens to.
Syntax	**config jwac switch_http_port <tcp_port_number 1 – 65535> {[http | https]}**
Description	This command is used to configure the TCP port which the JWAC Switch listens to. This port number is used in the second stage of the authentication. PC user will have to authenticate to the switch by inputting the user name and password.
Parameters	*<tcp_port_number 1–65535>* – A TCP port which the Switch listens to and uses for the authenticating process. *http* – To specify the JWAC runs HTTP protocol on this TCP port *https* – To specify the JWAC runs HTTPS protocol on this TCP port
Restrictions	The HTTP cannot runs at TCP port 443, and the HTTPS cannot runs at TCP port 80. Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the JWAC switch HTTP port:

```
DGS-3426:5#config jwac switch_http_port 8888 http
Command: config jwac switch_http_port 8888 http

Success.

DGS-3426:5#
```

config jwac ports

Purpose	Used to configure the JWAC port state.
Syntax	**config jwac ports [<portlist> | all] {state [enable | disable] | max_authenticating_host <value 0 – 50> | aging_time [infinite | <min 1 – 1440>] | idle_time [infinite | <min 1 – 1440>] | block_time [<sec 0 – 300>] | auth_mode [host_based | port_based] }(1)**
Description	This command is used to configure the JWAC port state. The max authenticating host default value is 50. The default aging time is 1440 minutes. The default idle time is infinite. The default block time is 60 seconds. The default mode is host-based.
Parameters	*<portlist>* – A port range to set the JWAC state. *all* – All the Switch ports' JWAC state is to be configured. *state* – To specify the port state of JWAC *max_authenticating_host* – Max number of host process authentication on each port at the same time. The max authenticating hosts depends on a specific project. *aging_time* – A time period during which an authenticated host will keep the authenticated state. "infinite" indicates never to age out the authenticated host on the port *idle_time* – If there is no traffic during idle_time, the host will be moved back to the unauthenticated state "infinite" indicates never to check the idle state of the authenticated host on the port. *block_time* – If a host fail to pass the authentication, it will be blocked for a period specified by block_time. *auth_mode* – The port authentication mode can be either host based or port based.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure JWAC ports:

```
DGS-3426:5#config jwac port 1 – 9 state enable
Command: config jwac port 1 – 9 state enable

Success.

DGS-3426:5#
```

config jwac radius_protocol

Purpose	Used to configure radius protocol used by JWAC.
Syntax	**config jwac radius_protocol [local | pap | chap | ms_chap | ms_chapv2 | eap_md5]**
Description	This command is used to specify the RADIUS protocol used by JWAC to complete RADIUS authentication.
Parameters	*local* – JWAC Switch uses local user DB to complete the authentication *pap* – JWAC Switch uses PAP to communicate with RADIUS Server *chap* – JWAC Switch uses CHAP to communicate with RADIUS Server *ms_chap* – JWAC Switch uses MS－CHAP to communicate with RADIUS Server *ms_chapv2* – JWAC Switch uses MS－CHAPv2 to communicate with RADIUS Server *eap_md5* － JWAC Switch uses EAP MD5 to communicate with RADIUS Server
Restrictions	JWAC shares other RADIUS' configuration with 802.1X. When using this command to set the RADIUS protocol, ensure that the RADIUS server added by the **config radius** command supports the protocol. Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the JWAC RADIUS protocol:

```
DGS-3426:5#config jwac radius_protocol ms_chapv2
Command: config jwac radius_protocol ms_chapv2

Success.

DGS-3426:5#
```

create jwac user

Purpose	Used to create JWAC user into local DB.
Syntax	**create jwac user <username 15> {vlan <vlanid 1－4094>}**
Description	This command is used to create JWAC users in the local DB. When “local” is chosen during configuring JWAC RADIUS protocol, the local DB will be used.
Parameters	<*username 15*> – The user name to be created. The maximum length of the username is 15 characters. <*vlanid 1-4094*> –Target VLAN ID for authenticated host which uses this user account to pass authentication.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create a JWAC user:

```
DGS-3426:5#create jwac user 112233
Command: create jwac user 112233

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

DGS-3426:5#
```

config jwac user

Purpose	Used to update local user DB.
Syntax	**config jwac user <username 15> {vlan <vlanid 1 – 4094>}**
Description	This command is used to update the local user DB. Only the created user can be configured.
Parameters	*<username 15>* – The user name to be created. The max length of the username is 15 characters. *<vlanid 1-4094>* –Target VLAN ID for authenticated host which uses this user account to pass authentication.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure a JWAC user:

```
DGS-3426:5# config jwac user 112233
Command: config jwac user 112233

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

DGS-3426:5#
```

delete jwac user

Purpose	Used to delete JWAC user into local DB.
Syntax	**delete jwac [user <username 15> | all_users]**
Description	This command is used to delete JWAC users from the local DB.
Parameters	*user* – To specify the user name to be deleted *all_user* – All user accouts in local DB will be deleted.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete a JWAC user:

```
DGS-3426:5# delete jwac user 112233
Command: delete jwac user 112233

Success.

DGS-3426:5#
```

show jwac user

Purpose	Used to display a JWAC user in the local DB.
Syntax	**show jwac user**
Description	This command is used to display JWAC users in the local DB.
Parameters	None.
Restrictions	None.

Example usage:

To display a JWAC user:

```
DGS-3426:5#show jwac user
Command: show jwac user

Current Accounts:
 Username        Password        VID
 --------------  --------------  ------
1                  1            1

Total Entries : 1

DGS-3426:5#
```

clear jwac auth_state

Purpose	Used to delete host on JWAC enabled ports
Syntax	**clear jwac auth_state [ports [all | <portlist>] {authenticated | authenticating | blocked} | mac_addr <macaddr>]**
Description	This command is used to delete JWAC host.
Parameters	*ports* – To specify the port range to delete host on them *authenticated* – To specify the state of host to delete *authenticating* – To specify the state of host to delete *blocked* – To specify the state of host to delete *<macaddr>* – To delete a specified host with this MAC
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete a JWAC host:

```
DGS-3426:5# clear jwac auth_state ports all blocked
Command: clear jwac auth_state ports all blocked

Success.

DGS-3426:5#
```

show jwac

Purpose	Used to display the JWAC configurations.
Syntax	**show jwac**
Description	This command is used to show all the configurations of JWAC.
Parameters	None.
Restrictions	None.

Example usage:

To display the JWAC configuration:

```
DGS-3426:5# show jwac
Command: show jwac

 State                   : Enabled
 Enabled Ports           : 1:1,1:11,1:23,1:25,1:35
 Virtual IP              : 1.1.1.1
 Switch HTTP Port        : 21212 (HTTP)
 UDP Filtering           : Enabled
 Forcible Logout         : Enabled
 Redirect State          : Enabled
 Redirect Delay Time     : 3 Seconds
 Redirect Destination    : Quarantine Server
 Quarantine Server       : http://172.18.212.147/pcinventory
 Q-Server Monitor        : Enabled (Running)
 Q-Svr Error Timeout     : 5 Seconds
 Radius Auth-Protocol    : PAP
 Authentication Failover : Enabled
 RADIUS Authorization    : Disabled
 Local Authorization     : Disabled

DGS-3426:5#
```

show jwac auth_state ports	
Purpose	Used to display JWAC client host information.
Syntax	**show jwac auth_state ports {<portlist>}**
Description	This command is used to display the information for JWAC client hosts. If port 1 is in host-based mode: (1) mac 00-00-00-00-00-01 is authenticated without VLAN assigned (may be the specified target VLAN does not exist or the target VLAN has not been specified), the ID of RX VLAN will be displayed (RX VLAN ID is 4004 in this example). (2) mac 00-00-00-00-00-02 is authenticated with target VLAN assigned, the ID of target VLAN will be displayed (target VLAN ID is 1234 in this example) (3) mac 00-00-00-00-00-03 failed to pass authentication, the VID field will be shown as "-" indicating that packets with SA 00-00-00-00-00-03 will be droped no matter which VLAN these packets are from. (4) mac 00-00-00-00-00-04 attempts to start authentication, the VID field will be shown as "-" until authentication completed. If port 2 is in port-based mode: (1) mac 00-00-00-00-00-10 is the mac which made port 2 pass authentication, mac address with "(P)" in the end indicats that this authentication is from a port in port-based mode. If port 3 is in port-based mode: (1) mac 00-00-00-00-00-20 attempts to start authentication, mac address with "(P)" in the end indicats the port-based mode authentication. (2) mac 00-00-00-00-00-21 failed to pass authentication, mac address with "(P)" in the end indicats the port-based mode authentication. **NOTE :** In port-based mode, the VLAN ID field is displayed in the same way as host-based mode
Parameters	*port* – A port range to show the information of client host.
Restrictions	None.

Example usage:

To display a JWAC host:

```
DGS-3426:5#show jwac auth_state ports 1-3
Command: show jwac auth_state ports 1-3

Port MAC Address           State               VID       Priority    Aging Time/
Idle Time
                                                                      Block Time
---- ----------------- ------------- ------- ---------- ------------- -------
-
1     00-00-00-00-00-01     Authenticated    4004         3             Infinite
40
1     00-00-00-00-00-02     Authenticated    1234         -             Infinite
50
1      00-00-00-00-00-03     Blocked          -              -                60
-
1      00-00-00-00-00-04    Authenticating    -              -                10
-
2      00-00-00-00-00-10(P)  Authenticated    1234         2               1440
20
3      00-00-00-00-00-20(P)  Authenticating   -             -               20
-
3     00-00-00-00-00-21(P)  Blocked             -             -              200
-

Total Authenticating Hosts :2
Total Authenticated Hosts  :3
Total Blocked Hosts        :2

DGS-3426:5#
```

show jwac ports

Purpose	Used to display JWAC port configuration.
Syntax	**show jwac ports {<portlist>}**
	This command is used to display JWAC port configuration.
Parameters	*<portlist>* – To specify a port range to show the configuration of JWAC.
Restrictions	None.

Example usage:

To display JWAC ports:

```
DGS-3426:5#show jwac ports
Command: show jwac ports

 Port   State     Aging Time  Idle Time  Block Time  Auth Mode   Max
                  (Minutes)   (Minutes)  (Seconds)               Hosts
 -----  --------  ----------  ---------  ----------  ----------  -----
 1      Disabled  1440        Infinite   60          Host_based  50
 2      Disabled  1440        Infinite   60          Host_based  50
 3      Disabled  1440        Infinite   60          Host_based  50

DGS-3426:5#
```

config jwac authentication_page element

Purpose	Used to customize the authentication page.
Syntax	**config jwac authentication_page element [japanese|english] [default|page_title <desc 128> |login_window_title <desc 32>|user_name_title <desc 16>|password_title <desc 16>| logout_window_title <desc 32>]**
Description	This command is used by administrator to customize the JWAC authentication page.
Parameters	*japanese* – Specifies that the page will change to Japanese. *english* – Specifies that the page will change to English. *default* – Specifies to reset the page element back to default. *page_title* – Specifies the title of the authentication page. *login_windown_title* – The login window title of the authentication page. *user_name_title* – Specifies the user name title of the authentication page. *password_title* – Specifies the password title of the authentication page. *logout_window_title* – The logout window title mapping of the authentication page.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the authentication page:

```
DGS-3426:5#config jwac authentication_page element japanese default
Command: config jwac authentication_page element japanese default

Success.

DGS-3426:5#
```

config jwac auth_failover

Purpose	Used to enable or disable JWAC authentication failover.
Syntax	**config jwac auth_failover [enable | disable]**
Description	This command is used by administrators to enable or disable JWAC authentication failover. When the authentication failover is disabled and RADIUS servers are unreachable, the authentication will fail. When the authentication failover is enabled and RADIUS servers authentication are unreachable, the local database will be used to do the authentication.By default, the state is disabled.
Parameters	*enable* – Enable JWAC authentication failover. *disable* – Disable JWAC authentication failover.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable JWAC authentication failover:

```
DGS-3426:5#config jwac auth_failover enable
Command: config jwac auth_failover enable

Success.

DGS-3426:5#
```

config jwac authorization network

Purpose	Used to enable or disable the accepting of an authorized configuration.
Syntax	**config jwac authorization network {radius [enable| disable]| local[enable| disable]} (1)**
Description	This command is used by administrators to configure an authorization network for JWAC. When the authorization is enabled for JWAC's RADIUS, the authorized data assigned by the RADUIS server will be accepted if the global authorization network is enabled. When the authorization is enabled for JWAC's local, the authorized data assigned by the local database will be accepted.
Parameters	*radius* – If specified to enable, the authorized data assigned by the RADUIS server will be accepted if the global authorization network is enabled.The default state is enabled. *local* – If specified to enable, the authorized data assigned by the local database will be accepted if the global authorization network is enabled.The default state is enabled.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable the accepting of an authorized configuration:

```
DGS-3426:5#config jwac authorization network radius enable
Command: config jwac authorization network radius enable

Success.

DGS-3426:5#
```

config jwac authenticate_page

Purpose	Used to choose the authenticate page.
Syntax	**config jwac authenticate_page [japanese| english]**
Description	This command is used by administrators to decide which authenticate page to be used.
Parameters	*japanese* – Choose the Japanese page *english* – Choose the English page. The default page is English.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To choose the Japanese authenticate page:

```
DGS-3426:5#config jwac authenticate_page japanese
Command: config jwac authenticate_page japanese

Success.

DGS-3426:5#
```

show jwac authenticate _page element

Purpose	Used to show the element mapping of the customize authenticate page.
Syntax	**show jwac authenticate_page element**
Description	This command is used to disaplay the elements of the customize authenticate page.
Parameters	None
Restrictions	None

Example usage:

To display an element of the authenticate page:

```
DGS-3426:5#show jwac authenticate_page element
Command: show jwac authenticate_page element

 Current Page : Japanese Version

English page element
------------------------------------------------------------
Page Title              :
Login Window Title      : Authentication Login
User Name Title         : User Name
Password Title          : Password
Login Out Window Title  : Logout from the network

Japanese page element

------------------------------------------------------------
Page Title                           :
Login Windown Title                : 社内LAN 認証ログイン
User Name Title                     : ユーザID
Password Title                      : パスワード
Login Out Windown Title           : 社内LAN 認証ログアウト

DGS-3426:5#
```

43

CABLE DIAGNOSTICS COMMANDS

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

Command	Parameters
cable_diag ports	[<portlist>|all]

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

cable_diag ports	
Purpose	This command is used to diagnose the copper cable. If there is an error in the cable, it can determine the type of error and the position where the error has occurred.
Syntax	**cable_diag ports [<portlist>|all]**
Description	When a port is in link-up state, the diagnostics feature will obtain the distance of the cable. When the status is in link–up state, the cable will not have any problem. This diagnostics feature is for copper cable--ports with fiber cables will be not be included. If the link is up, only cable length will be displayed; no abnormal result will be shown. If the link is down, the reason may be that the partner was powered off or that the port is disabled, the abnormal results won't be shown but the cable length will be indicated. If the link is down and there is some error in the cable, the abnormal results will be shown, but the cable length item won't be shown. Please note that the port to be diagnosed will link down for a while during the test, and the traffic will be displayed intermittently during the test.
Parameters	*portlist* – Specifies a range of ports to be displayed. (UnitID:port number). *all* – Indicates that all ports will be displayed.
Restrictions	None.

Example usage:

To display the cable diagnostics function for the Switch.

```
DGS-3426:5#cable_diag ports 1-7
Command: cable_diag ports 1:1-1:7

Perform Cable Diagnostics ...

 Port   Type   Link Status    Test Result        Cable Length(M)
 ------------------------------------------------------------------
 1:1    GE     Link down      No Cable
 1:2    GE     Link down      No Cable
 1:3    GE     Link down      No Cable
 1:4    GE     Link down      No Cable
 1:5    GE     Link down      No Cable
 1:6    GE     Link down      No Cable
 1:7    GE     Link up        OK                          4

DGS-3426:5#
```

44

MAC-BASED VLAN COMMANDS

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

Command	Parameters
create mac_based_vlan mac_address	<macaddr> vlan <vlan_name 32>
delete mac_based_vlan	{mac_address <macaddr> vlan <vlan_name 32>}
show mac_based_vlan	{mac_address <macaddr> | vlan <vlan_name 32>}

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

create mac_based_vlan	
Purpose	Used to create a static MAC–based VLAN entry.
Syntax	**create mac_based_vlan mac_address <macaddr> vlan <vlan_name 32>**
Description	This command is used to create a static MAC-based VLAN entry.There is a global limitation of the maximum entries supported for the static MAC-based entry.
Parameters	*mac_address* – The MAC addess to be created. *vlan* – The VLAN to be associated with the MAC address.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create a static MAC–based VLAN entry .

```
DGS-3426:5#create mac_based_vlan mac_address 00-00-00-00-00-01 vlan default
Command: create mac_based_vlan mac_address 00-00-00-00-00-01 vlan default
Success.

DGS-3426:5#
```

delete mac_based_vlan	
Purpose	Used to delete the static MAC–based VLAN entry.
Syntax	**delete mac_based_vlan {mac_address <macaddr> vlan <vlan_name 32>}**
Description	This command is used to delete a database entry. If the MAC address and VLAN are not specified, all static MAC-based VLAN entries will be removed.
Parameters	*mac_address* – The MAC address to be deleted. *vlan* – The VLAN to be associated with the MAC address.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete a static MAC–based VLAN entry.

```
DGS-3426:5#delete mac_based_vlan mac_address 00-00-00-00-00-01 vlan default
Command: delete mac_based_vlan mac mac_address 00-00-00-00-00-01 vlan default
Success.

DGS-3426:5#
```

show mac_based_vlan

Purpose	Used to display the static MAC–based VLAN entries.
Syntax	**show mac_based_vlan {mac_address <macaddr> | vlan <vlan_name 32>}**
Description	This command is used to display static MAC-based VLAN entries.
Parameters	*mac_address* – Specifies the MAC address of the entry you want to display. *vlan* – Specifies the VLAN to be associated with the MAC address.
Restrictions	None.

Example usage:

To display a static MAC–based VLAN entry:

```
DGS-3426:5# show mac_based_vlan

    MAC Address       VLAN    Status     Type
--------------------  ------  --------   --------
00–80–e0–14–a7–57      200     Active     Static
00–80–c2–33–c3–45      200     Inactive   Static
00–80–c2–33–c3–45      300     Active     MAC based access control
00–a2–44–17–32–98      400     Active     802.1x
00–a2–44–17–32–90      500     Active     WAC
00–a2–44–17–32–92      600     Active     JWAC

Total Entries : 4

DGS-3426:5#
```

45

LOOP-BACK DETECTION (LBD) GLOBAL COMMANDS

The Loop-back Detection (LBD) Global commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameters
config loopdetect	{recover_timer [0 | <value 60–1000000>] | interval <1 – 32767> | mode [port–based | vlan–based]} (1)
config loopdetect ports	[<portlist>| all] state [enable | disable]
enable loopdetect	
disable loopdetect	
show loopdetect	
show loopdetect ports	[all | <portlist>]
config loopdetect trap	[none | loop_detected | loop_cleared | both]

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

config loopdetect

Purpose	Used to configure the loop–back detection function on the switch.
Syntax	**config loopdetect {recover_timer [0 | <value 60–1000000>] | interval <1–32767> | mode [port–based | vlan–based]} (1)**
Description	This command is used to set up the loop-back detection function (LBD) for the entire switch.
Parameters	*recover_timer* – The time interval (in seconds) used by the Auto-Recovery mechanism to decide how long to check if the loop status is gone. The valid range is *60* to *1000000*. Zero is a special value which specifies the disabled auto–recovery mechanism, hence, users need to recover the disabled port manually. The default value of the recover timer is *60*. *interval* – The time interval (in seconds) at which the device transmits all the CTP(Configuration Test Protocol) packets to detect the loop – back event. The default setting is *10*. The valid range is *1* to *32767*. *mode* – Choose the loop detection operation mode. In the port-based mode, the port will be shutdown (disabled) when detecting loop; in VLAN-based mode, the port can’t process packets of the VLAN that detecting the loop.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To set the recover time to 0, the interval to 20, and the mode VLAN-based:

```
DGS-3426:5#config loopdetect  recover_timer 0 interval 20 vlan–based
Command: config loopdetect  recover_timer 0 interval 20 vlan–based

Success.

DGS-3426:5#
```

config loopdetect ports

Purpose	Used to configure loop – back detection function for the port on the switch.
Syntax	**config loopdetect ports [<portlist>| all] state [enable | disable]**
Description	This command is used to enable the loop – back detection function on specific ports.
Parameters	*portlist* – Specifies a range of ports to be configured. To set all ports in the system, you may use “all” parameters. *state* – Allows loop–detect to be enabled or disabled for the ports specified in the port list. The default is disabled.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To set state enable:

```
DGS-3426:5#config loopdetect ports 1:1-1:5 state enable
Command: config loopdetect ports 1:1-1:5 state enable

Success.

DGS-3426:5#
```

enable loopdetect

Purpose	Used to globally enable loop-detect function on the switch.
Syntax	**enable loopdetect**
Description	This command allows the loop-detect function to be globally enabled on the switch. The default value is disabled.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable loop-detect:

```
DGS-3426:5# enable loopdetect
Command: enable loopdetect

Success.

DGS-3426:5#
```

disable loopdetect

Purpose	Used to globally disable loop-detect function on the switch.
Syntax	**disable loopdetect**
Description	The disable loop-detect command allows the loop-detection function to be globally disabled on the switch. The default value is disabled.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable loopdetect:

```
DGS-3426:5#disable loopdetect
Command: disable loopdetect

Success.

DGS-3426:5#
```

show loopdetect

Purpose	Used to display the switch’s current loop-detect configuration.
Syntax	**show loopdetect**
Description	The show loop-detect command displays the switch’s current loop-detect configuration.
Parameters	None.
Restrictions	None.

Example usage:

To display loop-detect:

```
DGS-3426:5# show loopdetect
Command: show loopdetect
LBD Global Settings
---------------------------------------
LBD Status        : Enabled
LBD Interval      : 20
LBD Recover Time  : 60

DGS-3426:5#
```

show loopdetect ports

Purpose	Used to display the switch’s current per–port loop-detect configuration.
Syntax	**show loopdetect ports [all | <portlist>]**
Description	The show loop-detect ports command displays the switch’s current per-port loop-detect configuration and status.
Parameters	*portlist* – Specifies a range of ports to be displayed. (UnitID:port number). *all* – System will display all ports loopdetect information.
Restrictions	None.

Example usage:

To display loop-detect state of port 1–8 in port–based mode:

```
DGS-3426:5# show loopdetect  ports 1-8
Command: show loopdetect  ports 1-8

Port   Loopdetect State    Loop Status
------ ------------------ ----------
1      Enabled            Normal
2      Enabled            Normal
3      Enabled            Normal
4      Enabled            Normal
5      Enabled            Loop!
6      Enabled            Normal
7      Enabled            Loop!
8      Enabled            Normal

DGS-3426:5#
```

To display loop-detect state of port 1–8 in VLAN–based mode:

```
DGS-3426:5#show loopdetect  ports 1-8
Command: show loopdetect  ports 1-8

Port   Loopdetect State    Loop VLAN
------ ------------------ ----------
1      Enabled            None
2      Enabled            None
3      Enabled            None
4      Enabled            None
5      Enabled            2–8,9–20,300,500,600,700,
                          900,1000,2000
6      Enabled            None
7      Enabled            2
8      Enabled            None

DGS-3426:5#
```

config loopdetect trap

Purpose	Used to configure the trap mode.
Syntax	**config loopdetect trap [none | loop_detected | loop_cleared | both]**
Description	This command is used to configure the trap mode. A ttrap will be sent when the loop condition is detected. Similiarly the trap is sent when the loop condition is cleared.
Parameters	*none* – Trap will not be sent for both cases. *loop_detected* – Trap is sent when the loop condition is detected *loop_cleared* – Trap is sent when the loop condition is cleared. *both* – Trap will be sent for both cases.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the loop-detect trap on the Switch:

```
DGS-3426P:5#config loopdetect trap loop_detected
Command: config loopdetect trap loop_detected

Success.

DGS–3426:5#
```

46

SERIAL NUMBER COMMANDS

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

Command	Parameters
show switch	
show stack_device	

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

show switch

Purpose	Display switch information.
Syntax	**show switch**
Description	The command is used to display switch information.
Parameters	None.
Restrictions	None.

Example usage:

To display switch information, (serial number encoded):

```
DGS–3426:5#show switch
Command: show switch

Device Type       : DGS–3426 Gigabit Ethernet Switch
MAC Address       : 00–01–02–03–04–05
IP Address        : 172.18.211.246 (Manual)
VLAN Name         : default
Subnet Mask       : 255.255.255.0
Default Gateway   : 0.0.0.0
Boot PROM Version : Build 1.00–B13
Firmware Version  : Build 2.60.B26
Hardware Version  : A2
Serial Number     : P1X0188000123
System Name       :
System Location   :
System Contact    :
Spanning Tree     : Disabled
GVRP              : Disabled
IGMP Snooping     : Disabled
MLD Snooping      : Disabled
TELNET            : Enabled (TCP 23)
WEB               : Enabled (TCP 80)
SNMP              : Disabled
RMON              : Disabled
SSL Status        : Disabled
SSH Status        : Disabled
802.1x            : Disabled
Jumbo Frame       : Off
```

```
Clipaging          : Enabled
MAC Notification   : Disabled
Port Mirror        : Disabled
SNTP               : Disabled
HOL Prevention State : Enabled
Syslog Global State  : Disabled
Single IP Management : Disabled
Dual Image           : Supported
Password Encryption Status : Disabled

DGS-3426:5#
```

To display switch information, (serial number not encoded):

```
DGS-3426:5#show switch
Command: show switch

Device Type       : DGS-3426 Gigabit Ethernet Switch
MAC Address       : 00-01-02-03-04-05
IP Address        : 172.18.211.246 (Manual)
VLAN Name         : default
Subnet Mask       : 255.255.255.0
Default Gateway   : 0.0.0.0
Boot PROM Version : Build 1.00-B13
Firmware Version  : Build 2.60.B26
Hardware Version  : A2
System Name       :
System Location   :
System Contact    :
Spanning Tree     : Disabled
GVRP              : Disabled
IGMP Snooping     : Disabled
MLD Snooping      : Disabled
TELNET            : Enabled (TCP 23)
WEB               : Enabled (TCP 80)
SNMP              : Disabled
RMON              : Disabled
SSL Status        : Disabled
SSH Status        : Disabled
802.1x            : Disabled
Jumbo Frame       : Off
Clipaging         : Enabled
MAC Notification  : Disabled
Port Mirror       : Disabled
SNTP              : Disabled
HOL Prevention State : Enabled
Syslog Global State  : Disabled
Single IP Management : Disabled
Dual Image           : Supported
Password Encryption Status : Disabled

DGS-3426:5#
```

show stack_device

Purpose	Used to display the information for devices in the stack.
Syntax	**show stack_device**
Description	This command is used to display stack device information.
Parameters	None.
Restrictions	None.

Example usage:

To display stack information:

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

Box ID  Box Type      H/W Version  Serial Number
------  ------------  -----------  --------------------
1       DGS-3426      1A1G         123456879

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

47

802.1Q VLAN COMMANDS

The 802.1Q VLAN Function 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 1–4094> { type 1q_vlan advertisement }
delete vlan	<vlan_name>
config vlan	< vlan_name > { [add [tagged | untagged | forbidden] | delete] <portlist> | advertisement [enable | disable]}
config gvrp	config gvrp [<portlist> | all] {state [enable | disable]|ingress_checking [enable | disable] | acceptable_frame[tagged_only | admit_all] pvid <vlanid 1–4094> }
enable gvrp	
disable gvrp	
show vlan	{[<vlan_name 32> | vlanid <vlanid_list> | ports <portlist>]}
show gvrp	{<portlist>}

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 1–4094> { type 1q_vlan advertisement }**
Description	This command is used to createsa VLAN on the Switch. The VLAN ID must be always specified for creating a VLAN. The second command allows the user to create a number of VLANs at a time. A unique VLAN name (e.g. VLAN10) will be automatically assigned by the system. However, the user can use config vlan command to rename the VLAN, The automatic assignment of VLAN name is based on the following rule: “VLAN”+ID. For example, for VLAN ID 100, the VLAN name will be VLAN100. If this VLAN name is conflict with the name of an existing VLAN, then it will be renamed based on the following rule: “VLAN”+ID+”ALT”+ collision count. For example, if this conflict is the second collision, then the name will be VLAN100ALT2.
Parameters	*vlan_name* – The name of the VLAN to be created. *tag* – The VLAN ID of the VLAN to be created. The range is 1 – 4094. *Advertisement* – Specifies the VLAN as being able to be advertised out.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create a VLAN with name “v2” and VLAN ID 2:

```
DGS-3426:5# create vlan v2 tag 2 type 1q_vlan advertisement
Command: create vlan v2 tag 2 type 1q_vlan advertisement

Success.

DGS-3426:5#
```

delete vlan

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

Example usage:

To remove a VLAN v1:

```
DGS-3426:5# delete vlan v1
Command: delete vlan v1

Success.

DGS-3426:5#
```

config vlan add ports

Purpose	Used to add additional ports to a previously configured VLAN.
Syntax	**config vlan <vlan_name> { [add [tagged | untagged | forbidden] | delete] <portlist> | advertisement [enable | disable]}**
Description	This command is used to add ports to the port list of a previously configured VLAN. You can specify the additional ports as tagged, untagged, or forbidden. The default is to assign the ports as untagged. If based on VLAN ID to configure VLAN, multiple VLANs can be configured at a time. During configuration of multiple VLANs, error message will be returned if the configurations are conflict.
Parameters	*vlan_name* – The name of the VLAN you want to add ports to. *tagged* – Specifies the additional ports as tagged. *untagged* – Specifies the additional ports as untagged. *forbidden* – Specifies the additional ports as forbidden. *portlist* – A range of ports to add to the VLAN. *advertisement* – Specifies whether the VLAN is able to join a GVRP or not.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure VLAN add ports:

```
DGS-3426:5#config vlan v1 add tagged 2:4-2:8
Command: config vlan v1 add tagged 2:4-2:8

Success.

DGS-3426:5#
```

config vlan delete ports

Purpose	Used to delete one or more ports from a previously configured VLAN.
Syntax	**config vlan <vlan_name> delete <portlist>**
Description	This command is used to delete one or more ports from a previously configured VLAN. If based on VLAN ID to configure VLAN, multiple VLANs can be configured at a time.
Parameters	*vlan_name* – The name of the VLAN you want to delete ports from. *portlist* – Specifies a range of ports to be configured.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete configured VLAN ports:

```
DGS-3426:5# config vlan v1 delete 2:4-2:8
Command: config vlan v1 delete 2:4-2:8

Success.

DGS-3426:5#
```

config vlan advertisement

Purpose	Used to enable or disable VLAN advertisement.
Syntax	**config vlan <vlan_name> advertisement [enable | disable]**
Description	This command is used to enable or disable VLAN advertisement.
Parameters	*vlan_name* – The name of the VLAN on which you want to configure. *advertisement* – Join GVRP or not. If not, the VLAN can't join dynamically.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure VLAN advertisement:

```
DGS-3426:5# config vlan default advertisement enable
Command: config vlan default advertisement enable

Success.

DGS-3426:5#
```

enable gvrp

Purpose	Used to enable Generic VLAN Registration Protocol (GVRP).
Syntax	**enable gvrp**
Description	This command is used to enable the Generic VLAN Registration Protocol (GVRP). The default setting is disabled.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable the Generic VLAN Registration Protocol:

```
DGS-3426:5#enable gvrp
Command: enable gvrp

Success.

DGS-3426:5#
```

disable gvrp

Purpose	Used to disable the Generic VLAN Registration Protocol (GVRP).
Syntax	**disable gvrp**
Description	This command is used to disable the Generic VLAN Registration Protocol (GVRP).
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable Generic VLAN Registration Protocol:

```
DGS-3426:5# disable gvrp
Command: disable gvrp

Success.

DGS-3426:5#
```

show vlan

Purpose	Used to show VLAN information, including parameter settings and operational values.
Syntax	**show vlan { [<vlan_name 32> | vlanid <vlanid_list> | ports <portlist>]}**
Description	This command is used to display summary information about each VLAN, which includes: VLANID VLAN Name Tagged / untagged / Forbidden/－ status for each port Member / Non–member/－ status for each port
Parameters	*vlan_name* – The name of the VLAN to be displayed. *vlanid* – The ID of the VLAN to be displayed. *portlist* – The list of ports for which the VLAN information will be displayed.
Restrictions	None.

Example usage:

To display VLAN information:

```
DGS-3426:5#show vlan
Command: show vlan

VID             : 1          VLAN Name       : default
VLAN TYPE       : Static     Advertisement   : Enabled
Member Ports    : 1:1-1:26,2:1-2:26
Static Ports    : 1:1-1:26,2:1-2:26
Current Tagged Ports:
Current Untagged Ports  : 1:1-1:25,2:1-2:25
Static Tagged Ports:
Static Untagged Ports   : 1:1-1:26,2:1-2:26
Forbidden Ports :

VID             : 2          VLAN Name       : v1
VLAN TYPE       : Static     Advertisement   : Disabled
Member Ports    : 1:26,2:26
Static Ports  :
Current Tagged Ports:
Current Untagged Ports  :
Static Tagged Ports:
Static Untagged Ports   :
Forbidden Ports         :

Total Entries : 2

DGS-3426:5#
```

show gvrp

Purpose	Used to display the GVRP status for a port list on the Switch.
Syntax	**show gvrp {<portlist>}**
Description	This command is used to display the GVRP status for a port list on the Switch.
Parameters	*portlist* – Specifies a range of ports to be displayed. (UnitID:port number). If no parameter specified, system will display all port GVRP information.
Restrictions	None.

Example usage:

To display GVRP status settings:

```
DGS-3426:5# show gvrp
Command: show gvrp

lobal GVRP : Disabled

Port     PVID  GVRP      Ingress Checking  Acceptable Frame Type
-------  ----  --------  ----------------  -------------------------
 1:1     1     Disabled  Enabled           All Frames
 1:2     1     Disabled  Enabled           All Frames
 1:3     1     Disabled  Enabled           All Frames
 1:4     1     Disabled  Enabled           All Frames
 1:5     1     Disabled  Enabled           All Frames
 1:6     1     Disabled  Enabled           All Frames
 1:7     1     Disabled  Enabled           All Frames
 1:8     1     Disabled  Enabled           All Frames
 1:9     1     Disabled  Enabled           All Frames
 1:10    1     Disabled  Enabled           All Frames
 1:11    1     Disabled  Enabled           All Frames
 1:12    1     Disabled  Enabled           All Frames
 1:13    1     Disabled  Enabled           All Frames
 1:14    1     Disabled  Enabled           All Frames
 1:15    1     Disabled  Enabled           All Frames
 1:16    1     Disabled  Enabled           All Frames
 1:17    1     Disabled  Enabled           All Frames
 1:18    1     Disabled  Enabled           All Frames

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

48

MAC-BASED ACCESS CONTROL (MAC) COMMANDS

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

Command	Parameters
enable mac_based_access_control	
disable mac_based_access_control	
config mac_based_access_control password	<passwd 16>
config mac_based_access_control method	[local | radius]
config mac_based_access_control guest_vlan ports	<portlist>
config mac_based_access_control ports	[<portlist> | all] {state [enable | disable] | mode [port_based | host_based] | aging_time [infinite | <min 1–1440>] | block_time [infinite|<sec 1-300>] | max_users [no_limit |<value 1-4000>]} (1)
create mac_based_access_control	[guest_vlan <vlan_name 32>| guest_vlanid <vlanid 1–4094>]
delete mac_based_access_control	[guest_vlan <vlan_name 32>|guest_vlanid <vlanid 1–4094>]
clear mac_based_access_control auth_state	[ports [all | portlist] | mac_addr <macaddr>]
create mac_based_access_control_local mac	<macaddr> [vlan <vlan_name 32>|vlanid <vlanid 1–4094>]
config mac_based_access_control_local mac	<macaddr> [vlan <vlan_name 32>|vlanid <vlanid 1–4094> | clear_vlan]
delete mac_based_access_control_local	[mac <macaddr> | vlan <vlan_name 32>|vlanid <vlanid 1–4094>]
show mac_based_access_control	{ports {<portlist> }}
show mac_based_access_control_local	{[mac<macaddr> | [vlan <vlan_name 32>|vlanid <vlanid 1–4094>]]}
show mac_based_access_control auth_state	ports <portlist>
config mac_based_access_control auth_failover	[enable | disable]
config mac_based_access_control authorization network	{radius [enable | disable] | local [enable | disable]} (1)
config mac_based_access_control max_users	[<value 1-4000> | no_limit]

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

enable mac_based_access_control

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

Example usage:

To enable MAC-based access control:

```
DGS-3426:5# enable mac_based_access_control
Command: enable mac_based_access_control

Success.

DGS-3426:5#
```

disable mac_based_access_control

Purpose	Used to disable MAC-based access control.
Syntax	**disable mac_based_access_control**
Description	This command is used to disable the MAC-based access control function.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable MAC-based access control:

```
DGS-3426:5#disable mac_based_access_control
Command: disable mac_based_access_control

Success.

DGS-3426:5#
```

config mac_based_access_control password

Purpose	Used to configure the MAC-based access control password.
Syntax	**config mac_based_access_control password <passwd 16>**
Description	This command is used to set a password that will be used for authentication via a RADIUS server.
Parameters	*<passwd 16>* – In RADIUS mode, the Switch communicates with a RADIUS server using the password. The maximum length of the key is 16.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the MAC-based access control password:

```
DGS-3426:5# config mac_based_access_control password switch
Command: config mac_based_access_control password switch

Success.

DGS-3426:5#
```

config mac_based_access_control method

Purpose	Used to configure the MAC-based access control authenticating method.
Syntax	**config mac_based_access_control method [local | radius]**
Description	This command is used to specify to authenticate via local database or via RADIUS server.
Parameters	*local* – Specify to authenticate via local database. *radius* – Specify to authenticate via RADIUS server.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the MAC-based access control authenticating method:

```
DGS-3426:5#config mac_based_access_control method local
Command: config mac_based_access_control method local

Success.

DGS-3426:5#
```

config mac_based_access_control guest_vlan ports

Purpose	Used to configure the MAC-based access control guest VLAN membership
Syntax	**config mac_based_access_control guest_vlan ports <portlist>**
Description	This command is used to put the specified port in guest VLAN mode. For those ports not contained in the portlist, they are in non－guest VLAN mode.For detailed information for operation of guest VLAN mode, please see the description for the **config mac_based_access_control** command.
Parameters	*<portlist>* – When the guest VLAN is configured for a port successfully, the port will make the VLAN assignment based on the assigned VLAN and remove it from the guest VLAN. If the user authentication fails, the user will stay in the guest VLAN mode.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure a MAC-based access control guest VLAN:

```
DGS-3426:5# config mac_based_access_control guest_vlan ports 1－8
Command: config mac_based_access_control guest_vlan ports 1－8

Success.

DGS-3426:5#
```

config mac_based_access_control ports	
Purpose	Used to configure the parameters of MAC–based access control.
Syntax	**config mac_based_access_control ports [<portlist> | all] {state [enable | disable] | mode [port_based | host_based] | aging_time [infinite | <min 1–1440>] | block_time [infinite|<sec 1-300>] | max_users [no_limit | <value 1 - 4000>]} (1)**
Description	This command is used to configure the MAC-based access control setting. When the MAC-based access control function is enabled for a port, and the guest VLAN function for this port is disabled, the user attached to this port will not be forwarded unless the user passes authentication. The user that does not pass authentication will not be serviced by the switch. If the user passes authentication, the user will be able to forward traffic operated under the assigned VLAN configuration. When the MAC-based access control function is enabled for a port, and the guest VLAN function for this port is enabled, it will move from the original VLAN member port, and become the member port of the guest_vlan, before the authentication process starts. After the authentication, if a valid VLAN is assigned by the RADIUS server, then this port will be removed from the guest VLAN and become the member port of the assigned VLAN. For guest VLAN mode, there are two situations that need to be considered. If the product doesn't support MAC-based VLAN classifications when the port has been moved to the authorized VLAN, the subsequent users will not be authenticated again. They will operate in the current authorized VLAN. In the case where it doesn't support MAC–based VLAN classification, the guest VLAN and host–based mode can't be enabled at the same time. If the product supports the MAC–based VLAN classification, then each user will be authorized individually and capable of getting its own VLAN. For guest VLAN mode, if the MAC address is authorized, but no VLAN information is assigned from the RADIUS server or the VLAN assigned by RADIUS server is invalid (e.g. the assigned VLAN is not existent), this port/MAC will be removed from the member port of the guest VLAN and become a member port of the original VLAN
Parameters	*ports* – A range of ports enable or disable the MAC-based access control function. *state* – Specify whether MAC access control function is enabled or disabled. *mode* – Either port-based or host-based. *port_based*: means that all users connected to a port share the first authentication result. *host_based*: means that each user can have its own authentication result. If the Switch doesn't support MAC–based VLANs, then the Switch will not allow the option *host_based* for ports that are in guest vlan mode. *aging_time* – A time period during which an authenticated host will be kept in authenticated state. When the aging time is time–out, the host will be moved back to unauthenticated state. *block_time* – If a host fails to pass the authentication, the next authentication will not started within block_time unless the user clear the entry state manually. *max_user* – max number of authenticated clients on per port.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure port state:

```
DGS-3426:5#config mac_based_access_control ports 1–8 state enable
Command: config mac_based_access_control ports 1–8 state enable

Success.

DGS-3426:5#
```

To configure port mode:

```
DGS-3426:5#config mac_based_access_control ports 1–8 mode port_based
Command: config mac_based_access_control ports 1–8 mode port_based
Success.

DGS-3426:5#
```

create mac_based_access_control

Purpose	Used to create a guest VLAN.
Syntax	**create mac_based_access_control [guest_vlan <vlan_name 32>|guest_vlanid <vlanid 1–4094>]**
Description	This command is used to create a guest VLAN.
Parameters	*guest_vlan* – If the MAC address is authenticated failure, the port will be assigned to this vlan. *guest_vlanid* – If the MAC address is authenticated failure, the port will be assigned to this vlan.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create a MAC-based access control guest VLAN:

```
DGS-3426:5# create mac_based_access_control guest_vlan default
Command: create mac_based_access_control guest_vlan default
Success.

DGS-3426:5#
```

delete mac_based_access_control

Purpose	Used to delete a guest VLAN.
Syntax	**delete mac_based_access_control [guest_vlan <vlan_name 32>| guest_vlanid <vlanid 1–4094>]**
Description	This command is used to de–assign the guest VLAN. When the guest VLAN is de–assigned, the guest VLAN function is disabled.
Parameters	*guest_vlan* – Specifies the name of the guest VLAN. *guest_vlanid* – Specifies the VLAN ID of the guest VLAN.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete a guest VLAN:

```
DGS-3426:5# delete mac_based_access_control guest_vlan default
Command: delete mac_based_access_control guest_vlan default

Success.

DGS-3426:5#
```

clear mac_based_access_control auth_state

Purpose	Used to reset the current state of a user. The re – authentication will be started after the user traffic is received again.
Syntax	**clear mac_based_access_control auth_state [ports [all | portlist] | mac_addr <macaddr>]**
Description	This command is used to clear the authentication state of a user (or port). The port (or the user) will return to un – authenticated state. All the timer associated with the port (or the user) will be reset.
Parameters	*ports* – To specify the port range to delete MAC on them *<macaddr>* – To delete a specified host with this MAC
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To clear the MAC authentication state on MAC-enabled ports:

```
DGS-3426:5#clear mac_based_access_control auth_state ports all
Command: clear mac_based_access_control auth_state ports all

Success.

DGS-3426:5#
```

create mac_based_access_control_local mac

Purpose	Used to create the local database entry for MAC-based access control.
Syntax	**create mac_based_access_control_local mac <macaddr> [vlan <vlan_name 32>| vlanid <vlanid 1–4094>]**
Description	This command is used to create a database entry.
Parameters	*mac* – The MAC address that access accept by local mode *vlan* – If the MAC address is authorized, the port will be assigned to this VLAN. *vlanid* – If the MAC address is authorized, the port will be assigned to this VLAN.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create a local database entry:

```
DGS-3426:5# create mac_based_access_control_local mac 00-00-00-00-00-01 vlan
default
Command: create mac_based_access_control_local mac 00-00-00-00-00-01 vlan
default

Success.

DGS-3426:5#
```

config mac_based_access_control_local mac

Purpose	Used to configure the local database entry.
Syntax	**config mac_based_access_control_local mac <macaddr> [vlan <vlan_name 32>| vlanid <vlanid 1–4094>]**
Description	This command is used to modify a database entry.
Parameters	*mac* – The MAC address that access accept by local mode *vlan* – If the MAC address is authorized, the port will be assigned to this VLAN. *vlanid* – If the MAC address is authorized, the port will be assigned to this VLAN.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure a local database entry:

```
DGS-3426:5#config mac_based_access_control_local mac 00-00-00-00-00-01 vlan
default
Command: config mac_based_access_control_local mac 00-00-00-00-00-01 vlan
default

Success.

DGS-3426:5#
```

delete mac_based_access_control_local

Purpose	Used to delete the local database entry.
Syntax	**delete mac_based_access_control_local [mac <macaddr> | [vlan <vlan_name 32>|vlanid <vlanid 1–4094>]]**
Description	This command is used to delete a database entry.
Parameters	*mac* – Deletes the database by this MAC address. *vlan* – Deletes the database by this VLAN name. *vlanid* – Deletes the database by this VLAN ID.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete the local database entry by MAC address:

```
DGS-3426:5#delete mac_based_access_control_local mac 00-00-00-00-00-01
Command: delete mac_based_access_control_local mac 00-00-00-00-00-01

Success.

DGS-3426:5#
```

To delete the local database entry by VLAN name:

```
DGS-3426:5#delete mac_based_access_control_local vlan default
Command: delete mac_based_access_control_local vlan default

Success.

DGS-3426:5#
```

show mac_based_access_control

Purpose	Used to display the MAC-based access control global and port settings.
Syntax	**show mac_based_access_control {ports {<portlist> }}**
Description	This command is used to display the MAC-based access control global and port settings.
Parameters	*ports* – Display the MAC-based access control port state.
Restrictions	None.

Example usage:

To display MAC-based access control settings:

```
DGS-3426:5#show mac_based_access_control ports 1-7
Command: show mac_based_access_control ports 1:1-1:7


Port    State     Aging Time   Block Time  Auth Mode    Max User
                    (mins)      (secs)
-----  --------   ----------   ---------   ----------   --------
1:1    Disabled   1440         300         Host_based   128
1:2    Disabled   1440         300         Host_based   128
1:3    Disabled   1440         300         Host_based   128
1:4    Disabled   1440         300         Host_based   128
1:5    Enabled    1440         300         Host_based   128
1:6    Enabled    1440         300         Host_based   128
1:7    Enabled    1440         300         Host_based   128

DGS-3426:5#
```

To display MAC-based access control:

```
DGS-3426:5#show mac_based_access_control
Command: show mac_based_access_control

MAC Based Access Control
------------------------------------
State                  : Disabled
Method                 : RADIUS
Authentication Failover: Disabled
Password               : default
Max User               : No Limit
Guest VLAN             : default
Guest VLAN Member Ports: 1-8
RADIUS Authorization   : Enabled
Local Authorization    : Enabled

DGS-3426:5#
```

show mac_based_access_control_local

Purpose	Used to display a MAC-based access control local database.
Syntax	**show mac_based_access_control_local {[mac<macaddr> | [vlan <vlan_name 32>|vlanid <vlanid 1–4094>]]}**
Description	This command is used to display the MAC-based access control local database.
Parameters	*mac* – Display a MAC-based access control local database by this MAC address *vlan* – Display a MAC-based access control local database by this VLAN name. *vlanid* – Display a MAC-based access control local database by this VLAN ID.
Restrictions	None.

Example usage:

To display a MAC-based access control local:

```
DGS-3426:5# show mac_based_access_control_local
Command: show mac_based_access_control_local

MAC Address        VID
-----------------  - - - - -
00-00-00-00-00-01  1
00-00-00-00-00-02  123
00-00-00-00-00-03  123
00-00-00-00-00-04  1

Total Entries:4

DGS-3426:5#
```

To display MAC-based access control local by MAC address:

```
DGS-3426:5#show mac_based_access_control_local mac 00-00-00-00-00-01
Command:    show    mac_based_access_control_local    mac    00-00-00-00-00-01

MAC Address        VID
-----------------  - - - - -
00-00-00-00-00-01  1

Total Entries:1


DGS-3426:5#
```

To display MAC- based access control local by VLAN:

```
DGS-3426:5#show mac_based_access_control_local vlan default
Command: show mac_based_access_control_local vlan default

MAC Address        VID
-----------------  - - - - -
00-00-00-00-00-01     1
00-00-00-00-00-04     1

Total Entries:2

DGS-3426:5#
```

show mac_based_access_control auth_state

Purpose	Used to display the MAC-based access control authenticated state.
Syntax	**show mac_based_access_control auth_state ports <portlist>**
Description	This command is used to display the MAC-based access control authenticated state.
Parameters	*ports* – Display MAC-based access control port state
Restrictions	None.

Example usage:

To display the MAC-based access control authentication state:

```
DGS-3426:5#show mac_based_access_control auth_state ports 1-7
Command: show mac_based_access_control auth_state ports 1:1-1:7

Port MAC Address          State         VID  Priority Aging Time/
                                                      Block Time
---- -------------------- ------------- ---- -------- -----------

Total Authenticating Hosts  : 0
Total Authenticated Hosts   : 0
Total Blocked Hosts         : 0


DGS-3426:5#
```

config mac_based_access_control auth_failover

Purpose	Used to configure the MAC-based access control authentication failover function.
Syntax	**config mac_based_access_control auth_failover [enable | disable]**
Description	When the authentication failover is disabled and if the RADUIUS servers are unreachable, the authentication will fail. When the authentication failover is enabled, and if the RADIUS servers authentication is unreachable, the local database will be used to do the authentication. The state is disabled, by default.
Parameters	*enable* – Enables the protocol authentication failover. *disable* – Disables the protocol authentication failover.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the MAC-based access control authentication failover:

```
DGS-3426:5#config mac_based_access_control auth_failover enable
Command: config mac_based_access_control auth_failover enable

Success.

DGS-3426:5#
```

config mac_based_access_control authorization network

Purpose	This function will enable the accepting of an authorized configuration.
Syntax	**config mac_based_access_control authorization network {radius [enable | disable]| local [enable | disable]} (1)**
Description	This command is used to enable or disable the accepting of an authorized configuration. When the authorization is enabled for MAC-based access control's RADIUS, the authorized data assigned by the RADIUS server will be accepted if the global authorization network is enabled. When the authorization is enabled for MAC-based access controls local, the authorized data assigned by the local database will be accepted.
Parameters	*radius* – If specified to enable, the authorized data assigned by the RADUIS server will be accepted if the global authorization network is enabled. The default state is enabled. *local* – If specified to enable, the authorized data assigned by the local database will be accepted if the global authorization network is enabled. The default state is enabled.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the MAC-based access control authorized network:

```
DGS-3426:5#config mac_based_access_control authorization network local disable
Command: config mac_based_access_control authorization network local disable

Success.

DGS-3426:5#
```

config mac_based_access_control max_users

Purpose	Used to configure the maximum number of authorized clients.
Syntax	**config mac_based_access_control max_users [<value 1-4000> | no_limit]**
Description	This command is used to configure the maximum number of authorized clients. The setting is a global limitation on the maximum number of users that can be learned via MAC-Based access control. In addition to the global limitation, the per port maximum number of users is also limited. It is specified by configure MAC-based access control ports maximum users.
Parameters	*value 1-4000* – Specifies to set the maximum number of authorized clients on the whole device. *no_limit* – Specifies to not limit the system's maximum number of users. The default is *128*.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the MAC-based access control maximum number of users:

```
DGS–3426:5#config mac_based_access_control max_users 126
Command: config mac_based_access_control max_users 126

Success.

DGS–3426:5#
```

49

Q-IN-Q COMMANDS

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

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

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

enable qinq

Purpose	Used to enable Q-in-Q mode.
Syntax	**enable qinq**
Description	This command is used to enable the Q-in-Q mode. When enable Q-in-Q, all network port roles will be NNI port and their outer TPID will be set to 88a8. All existed static VLAN will run as SP-VLAN. All dynamically learned L2 address will be cleared. All dynamically registered VLAN entries will be cleared, GVRP will be disabled. If you need to run GVRP on the switch, you shall enable GVRP manually. In Q-in-Q mode, SP-VLAN GVRP Address (01-80-C2-00-00-0D) will be used by GVRP protocol. The default setting of Q-in-Q is disabled
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable Q-in-Q:

```
DGS-3426:5#enable qinq
Command: enable qinq

Success.

DGS-3426:5#
```

disable qinq

Purpose	Used to disable the Q-in-Q mode.
Syntax	**disable qinq**
Description	This command is used to disable the Q-in-Q mode. All dynamically learned L2 address will be cleared. All dynamically registered VLAN entries will be cleared. GVRP will disable. If you need to run GVRP on the switch, you shall enable GVRP manually. All existed SP-VLAN will run as static 1Q VLAN.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable Q-in-Q:

```
DGS-3426:5#disable qinq
Command: disable qinq

Success.

DGS-3426:5#
```

show qinq

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

Example usage:

To display global Q-in-Q status:

```
DGS-3426:5#show qinq
Commands: show qinq

 QinQ Status: Enabled

DGS-3426:5#
```

config qinq ports

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

Example usage:

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

```
DGS-3426:5#config qinq ports 1-4 role nni tpid 0x88a8
Command: config qinq ports 1-4 role nni tpid 0x88a8

Success.

DGS-3426:5#
```

show qinq port

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

Example usage

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

```
DGS–3426:4#show qinq port 1:1-1:4
Commands: show qinq ports 1:1-1:4

Port   Role      Miss Drop   TPID
-----  ------    ---------  ------
1:1    UNI       Enabled    0x88A8
1:2    UNI       Enabled    0x88A8
1:3    UNI       Enabled    0x88A8
1:4    NNI       Disabled   0x88A8

DGS–3426:
```

create vlan_translation ports

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

Example usage

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

```
DGS–3426:5#create vlan_translation ports 1-4 cvid 10 add svid 100 priority 4
Command: create vlan_translation ports 1-4 cvid 10 add svid 100 priority 4

Success.

DGS–3426:5#
```

delete vlan_translation ports

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

Example usage

To delete a VLAN translation rule on ports 1-4:

```
DGS-3426:5#delete vlan_translation ports 1-4
Command: delete vlan_translation ports 1-4

Success.

DGS-3426:5#
```

show vlan_translation

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

Example usage

To show VLAN translation rules in the system:

```
DGS-3426:5#show vlan_translation
Commands: show vlan_translation
Port       CVID      SPVID     Action     Priority
------     -----      -----    ------     ------
1          10         100       Add         4
1          20         100       Add         5
1          30         200       Add         6
2          10         100       Add         7
2          20         100       Add         1

Total Entries: 5

DGS-3426:5#
```

50

LLDP COMMANDS

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

Command	Parameters
enable lldp	
disable lldp	
config lldp	message_tx_interval <sec 5-32768>
config lldp	message_tx_hold_multiplier <2–10>
config lldp	tx_delay <sec 1-8192>
config lldp	reinit_delay <sec 1-10>
config lldp	notification_interval <sec 5-3600>
config lldp ports	[<portlist> | all] notification [enable | disable]
config lldp ports	[<portlist> | all] admin_status [tx_only | rx_only | tx_and_rx | disable]
config lldp ports	[<portlist> | all] mgt_addr [ipv4 <ipaddr> | ipv6 <ipv6addr>] [enable | disable]
config lldp ports	[<portlist> | all] basic_tlvs [all | {port_description | system_name | system_description | system_capabilities} (1)] [enable | disable]
config lldp ports	[<portlist> | all] dot1_tlv_pvid [enable | disable]
config lldp ports	[<portlist> | all] dot1_tlv_protocol_vid [vlan [all | <vlan_name 32>] | vlanid <vlanid_list>] [enable | disable]
config lldp ports	[<portlist> | all] dot1_tlv_vlan_name [vlan [all | <vlan_name 32>] | vlanid <vlanid_list>] [enable | disable]
config lldp ports	[<portlist>|all] dot1_tlv_ protocol_identity[all | { eapol | lacp | gvrp | stp }(1)] [enable | disable]
config lldp ports	dot3_tlvs [all | {mac_phy_configuration_status | link_aggregation | power_via_mdi | 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**
Description	This command is used as a global control for the LLDP function. When this function is enabled, the switch can start to transmit LLDP packets and receive and process the LLDP packets. The specific function of each port will depend on the per port LLDP setting. For the advertisement of LLDP packets, the switch announces the information to its neighbor through ports. For the receiving of LLDP packets, the switch will learn the information from the LLDP packets advertised from the neighbor in the neighbor table. The default state for LLDP is disabled.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable LLDP:

```
DGS-3426:5#enable lldp
Command: enable lldp

Success.

DGS-3426:5#
```

disable lldp

Purpose	Used to disable LLDP operation on the Switch.
Syntax	**disable lldp**
Description	This command is used to stop the sending and receiving of LLDP advertisement packets on the Switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable LLDP:

```
DGS-3426:5#disable lldp
Command: disable lldp

Success.

DGS-3426:5#
```

config lldp message_tx_interval

Purpose	Used to change the packet transmission interval.
Syntax	**config lldp message_tx_interval <sec 5–32768>**
Description	This command is used as an interval to control how often active ports retransmit advertisements to their neighbors.
Parameters	*message_tx_interval* – Changes the interval between consecutive transmissions of LLDP advertisements on any given port. The range is from *5* seconds to *32768* seconds. The default setting is *30* seconds.
Restrictions	Only Administrator and Operator-level users can issue this command.

Usage Example:

To show the packet transmission interval:

```
DGS-3426:5#config lldp message_tx_interval 30
Command: config lldp message_tx_interval 30

Success.

DGS-3426:5#
```

config lldp message_tx_hold_multiplier

Purpose	Used to configure the message hold multiplier.
Syntax	**config lldp message_tx_hold_multiplier <2-10>**
Description	This command is used as a multiplier on the msgTxInterval to compute the TTL value of txTTL in an LLDPDU. TheTTL will be carried in the LLDPDU packet. The lifetime will be the minimum of 65535 and (message_tx_interval * message_tx_hold_multiplier). At the partner switch, when the tme-to-Live for a given advertisement expires, the advertised data is deleted from the neighbor switch's MIB.
Parameters	*message_hold_multiplier* – The range is from *2* to *10*. The default setting is *4*.
Restrictions	Only Administrator and Operator-level users can issue this command.

Usage Example:

To change the multiplier value:

```
DGS-3426:5#config lldp message_tx_hold_multiplier 3
Command: config lldp message_tx_ hold_multiplier 3

Success.

DGS-3426:5#
```

config lldp tx_delay

Purpose	Used to change the minimum time (delay-interval) any LLDP port will delay advertising successive LLDP advertisements due to a change in LLDP MIB content. The tx_delay defines the minimum interval between sending of LLDP messages due to constantly change of MIB content.
Syntax	**config lldp tx_delay <sec 1–8192>**
Description	This command is used as an LLDP message_tx_interval (transmit interval) which must be greater than or equal to (4 x tx_delay interval).
Parameters	*tx_delay* – The range is from *1* second to *8192* seconds. The default setting is *2* seconds. NOTE: txDelay should be less than or equal to 0.25 * msgTxInterval.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the delay interval:

```
DGS-3426:5#config lldp tx_delay 8
Command: config lldp tx_delay 8

Success.

DGS-3426:5#
```

config lldp reinit_delay

Purpose	Change the minimum time of the reinitialization delay interval.
Syntax	**config lldp reinit_delay <sec 1-10>**
Description	An re-enabled LLDP port will wait for reinit_delay after last disable command before reinitializing.
Parameters	*reinit_delay* – The range is from *1* second to *10* seconds. The default setting is *2* seconds.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To changes the re-initialization delay interval to five seconds:

```
DGS-3426:5#config lldp reinit_delay 5
Command: config lldp reinit_delay 5

Success.

DGS-3426:5#
```

config lldp notification _interval

Purpose	Used to configure the timer of the notification interval for sending notification to configured SNMP trap receiver(s).
Syntax	**config lldp notification_interval <sec 5–3600>**
Description	This command is used to globally change the interval between successive LLDP change notifications generated by the Switch.
Parameters	*notification_interval* – The range is from *5* seconds to *3600* seconds. The default setting is *5* seconds.
Restrictions	Only Administrator and Operator-level users can issue this command.

Usage Example:

To change the notification interval to 10 seconds:

```
DGS-3426:5#config lldp notification_interval 10
Command: config lldp notification_interval 10

Success.

DGS-3426:5#
```

config lldp ports notification

Purpose	Used to configure each port for sending notification to configured SNMP trap receiver(s).
Syntax	**config lldp ports [<portlist> | all] notification [enable | disable]**
Description	This command is used to enable or disable each port for sending changes notification to configured SNMP trap receiver(s) if an LLDP data change is detected in an advertisement received on the port from an LLDP neighbor. The definition of change includes new available information, information timeout, information update. And the changed type includes any data update /insert/remove.
Parameters	*<portlist>* – Use this parameter to define ports to be configured. *all* – Use this parameter to set all ports in the system. *notification* – Enables or disables the SNMP trap notification of LLDP data changes detected on advertisements received from neighbor devices. The default notification state is disabled.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To change the SNMP notification state of ports 1 to 5 to enable:

```
DGS-3426:5#config lldp ports 1-5 notification enable
Command: config lldp ports 1-5 notification enable

Success.

DGS-3426:5#
```

config lldp ports admin_status

Purpose	Used to configure per-port transmit and receive modes.
Syntax	**config lldp ports [<portlist> | all] admin_status [tx_only | rx_only | tx_and_rx | disable]**
Description	This command is used to control which ports participate in LLDP traffic and whether the participating ports allow LLDP traffic in only one direction or in both directions.
Parameters	*<portlist>* – Use this parameter to define ports to be configured. *all* – Use this parameter to set all ports in the system. *admin_status* – *tx_only*: Configure the specified port(s) to transmit LLDP packets, but block inbound LLDP packets from neighbor devices; *rx_only*: Configure the specified port(s) to receive LLDP packets from neighbors, but block outbound packets to neighbors; *tx_and_rx*: Configure the specified port(s) to both transmit and receive LLDP packets; *disable*: Disable LLDP packet transmit and receive on the specified port(s). The default per port state is *tx_and_rx*.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure ports 1 to 5 to transmit and receive:

```
DGS-3426:5#config lldp ports 1-5 admin_status rx_and_tx
Command: config lldp ports 1-5 admin_status rx_and_tx

Success.

DGS-3426:5#
```

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 is used to specify whether the system's IP address needs to be advertised from the specified port. For layer 3 devices, each managed address can be individually specified. The management addresses that are added in the list will be advertised in the LLDP from the specified interface associated with each management address. The interface for that management address will be also advertised in the if-index Form
Parameters	*<portlist>* – Use this parameter to define ports to be configured. *all* – Use this parameter to set all ports in the system. *ipv4* – The IP address of IPv4. *Ipv6* – The IP address of IPv6.
Restrictions	Only Administrator and Operator-level users can issue this command.

Usage Example:

To enable ports 1 to 2 to manage address entry:

```
DGS-3426:5#config lldp ports 1-2 mgt_addr ipv4 192.168.254.10 enable
Command: config config lldp ports 1-2 mgt_addr ipv4 192.168.254.10 enable

Success.

DGS-3426:5#
```

config lldp ports basic_tlvs

Purpose	Used to configure an individual port or group of ports to exclude one or more optional TLV data types from outbound LLDP advertisements.
Syntax	**config lldp ports [<portlist> | all] basic_tlvs [all | {port_description | system_name | system_description | system_capabilities}] [enable | disable]**
Description	An active LLDP port on the switch always includes the mandatory data in its outbound advertisements. And there are four optional data that can be configured for an individual port or group of ports to exclude one or more of these data types from outbound LLDP advertisements. The mandatory data type include four basic types of information (end of LLDPDU TLV, chassis ID TLV, port ID TLV, and Time to Live TLV). The mandatory type cannot be disabled. There are also four data types which can be optionally selected. They are *port_description*, *system_name*, *system_description*, and *system_capability*.
Parameters	*<portlist>* – Use this parameter to define ports to be configured. *all* – Use this parameter to set all ports in the system. *port_description* – This TLV optional data type indicates that LLDP agent should transmit 'Port Description TLV on the port. The default state is disabled. *system_name* – This TLV optional data type indicates that LLDP agent should transmit 'System Name TLV'. The default state is disabled. *system_description* – This TLV optional data type indicates that LLDP agent should transmit 'System Description TLV'. The default state is disabled. *system_capabilities* – This TLV optional data type indicates that LLDP agent should transmit 'System Capabilities TLV'. The system capability will indicate whether the device provides repeater, bridge, or router function, and whether the provided functions are currently enabled. The default state is disabled.
Restrictions	Only Administrator and Operator-level users can issue this command.

Usage Example:

To configure exclude the system name TLV from the outbound LLDP advertisements for all ports:

```
DGS-3426:5#config lldp ports all basic_tlvs system_name enable
Command: config lldp ports all basic_tlvs system_name enable

Success.

DGS-3426:5#
```

config lldp dot1_tlv_pvid

Purpose	Used to configure an individual port or group of ports to exclude one or more of IEEE 802.1 Organizationally port VLAN ID TLV data types from outbound LLDP advertisements.
Syntax	**config lldp ports [<portlist> | all] dot1_tlv_pvid [enable | disable]**
Description	This TLV optional data type determines whether the IEEE 802.1 organizationally defined port VLAN TLV transmission is allowed on a given LLDP transmission capable port.
Parameters	*<portlist>* – Use this parameter to define ports to be configured. *all* – Use this parameter to set all ports in the system. *dot1_tlv_pvid* – This TLV optional data type determines whether the IEEE 802.1 organizationally defined port VLAN ID TLV transmission is allowed on a given LLDP transmission capable port. The default state is disabled.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure exclude the VLAN nameTLV from the outbound LLDP advertisements for all ports:

```
DGS-3426:5#config lldp ports all dot1_tlv_pvid enable
Command: config lldp ports all dot1_tlv_pvid enable

Success.

DGS-3426:5#
```

config lldp dot1_tlv_protocol_vid

Purpose	Used to configure an individual port or group of ports to exclude one or more of IEEE 802.1 Organizationally port and protocol VLAN ID TLV data types from outbound LLDP advertisements.
Syntax	**config lldp ports [<portlist> | all] dot1_tlv_protocol_vid [vlan [all | <vlan_name 32>] | vlanid <vlanid_list>] [enable | disable]**
Description	This 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	*<portlist>* – Use this parameter to define ports to be configured. *all* – Use this parameter to set all ports in the system. *dot1_tlv_protocol_vid* – This TLV optional data type determines whether the IEEE 802.1 organizationally defined port and protocol VLAN ID TLV transmission is allowed on a given LLDP transmission capable port. The default state is disabled.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure exclude the port and protocol VLAN ID TLV from the outbound LLDP advertisements for all ports:

```
DGS-3426:5#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-3426:5#
```

config lldp dot1_tlv_vlan_name

Purpose	Used to configure an individual port or group of ports to exclude one or more of IEEE 802.1 Organizationally VLAN name TLV data types from outbound LLDP advertisements.
Syntax	**config lldp ports [<portlist> | all] dot1_tlv_vlan_name [vlan [all | <vlan_name 32>] | vlanid <vlanid_list>] [enable | disable]**
Description	This 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	*<portlist>* – Use this parameter to define ports to be configured. *all* – Use this parameter to set all ports in the system. *dot1_tlv_vlan_name* – This TLV optional data type indicates whether the corresponding Local System’s VLAN name instance will be transmitted on the port. If a port is associated with multiple VLANs, those enabled VLAN IDs will be advertised. The default state is disabled.
Restrictions	Only Administrator and Operator-level users can issue this command.

Usage Example:

To configure exclude the VLAN name TLV from the outbound LLDP advertisements for all ports:

```
DGS-3426:5#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-3426:5#
```

config lldp dot1_tlv_protocol_identity

Purpose	Used to configure an individual port or group of ports to exclude one or more of IEEE 802.1 Organizationally protocol identity TLV data types from outbound LLDP advertisements.
Syntax	**config lldp ports [<portlist> | all] dot1_tlv_ protocol_identity [all | {eapol | lacp | gvrp | stp } (1)] [enable | disable]**
Description	This 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	*<portlist>* – Use this parameter to define ports to be configured. *all* – Use this parameter to set all ports in the system. *dot1_tlv_protocol_identity* – This TLV optional data type indicates whether the corresponding Local System's Protocol Identity instance will be transmitted on the port. The Protocol Identity TLV provides a way for stations to advertise protocols that are important to the operation of the network. Such as Spanning Tree Protocol, the Link Aggregation Control Protocol, and numerous vendor proprietary variations are responsible for maintaining the topology and connectivity of the network. If EAPOL,

config lldp dot1_tlv_protocol_identity

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

Example usage:

To configure exclude the protocol identity TLV from the outbound LLDP advertisements for all ports:

```
DGS-3426:5#config lldp ports all dot1_tlv_protocol_identity all enable
Command: config lldp ports all dot1_tlv_protocol_identity all enable

Success.

DGS-3426:5#
```

config lldp dot3_tlvs

Purpose	Used to configure an individual port or group of ports to exclude one or more of IEEE 802.3 Organizationally Specific TLV data types from outbound LLDP advertisements.
Syntax	**config lldp ports [<portlist> | all] dot3_tlvs [all | {mac_phy_configuration_status | link_aggregation | power_via_mdi | maximum_frame_size}] [enable | disable]**
Description	Each Specific TLV in this extension can be enabled individually.
Parameters	*<portlist>* – Use this parameter to define ports to be configured. *all* – Use this parameter to set all ports in the system. *mac_phy_configuration_status* – This TLV optional data type indicates that LLDP agent should transmit 'MAC/PHY configuration/status TLV'. This type indicates it is possible for two ends of an IEEE 802.3 link to be configured with different and/or speed settings and still establish some limited network connectivity. More precisely, the information includes whether the port support the auto-negotiation function, whether the function is enabled, the auto-negotiated advertised capability, and the operational MAU type. The default state is disabled. *link_aggregation* – This TLV optional data type indicates that LLDP agent should transmit 'Link Aggregation TLV'. This type indicates the current link aggregation status of IEEE 802.3 MACs. More precisely, the information should include whether the port is capable of doing link aggregation, whether the port is aggregated in a aggregated link, and the aggregated port ID. The default state is disabled. *power_via_mdi* – This TLV optional data type indicates that the LLDP agent should transmit 'Power via MDI TLV'. Three IEEE 802.3 PMD implementations (10BASE-T, 100BASE-TX, and 1000BASE-T) allow power to be supplied over the link for connected non-powered systems. The Power Via MDI TLV allows network management to advertise and discover the MDI power support capabilities of the sending IEEE 802.3 LAN station. The default state is disabled. Note: Not supported in the current release. *maximum_frame_size* – This TLV optional data type indicates that LLDP agent should transmit 'Maximum-frame-size TLV. The default state is disabled.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure exclude the MAC/PHY configuration/status TLV from the outbound LLDP advertisements for all ports:

```
DGS-3426:5#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-3426:5#
```

config lldp forward_message

Purpose	Used to configure the forwarding of LLDPDU packets when LLDP is disabled.
Syntax	**config lldp forward_message [enable | disable]**
Description	When LLDP is disabled and LLDP forward_message is enabled, the received LLDPDU packets will be forwarded. The default state is disabled.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Usage Example:

To configure LLDP forward_message:

```
DGS-3426:5#config lldp forward_message enable
Command: config lldp forward_message enable

Success.

DGS-3426:5#
```

show lldp

Purpose	This command displays the switch’s general LLDP configuration status.
Syntax	**show lldp**
Description	This command is used to display the Switch’s general LLDP configuration status.
Parameters	None.
Restrictions	None.

Usage Example:

To display the LLDP system level configuration status:

```
DGS-3426:5#show lldp
Command: show lldp

LLDP System Information
    Chassis ID Subtype         : MAC Address
    Chassis ID                 : 00-80-C2-11-22-00
    System Name                :
    System Description         : Fast 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-3426:5#
```

show lldp mgt_addr

Purpose	Used to display the LLDP management address information.
Syntax	**show lldp mgt_addr {[ipv4 <ipaddr> | ipv6 <ipv6addr>]}**
Description	This command is used to displays the LLDP management address information.
Parameters	*ipv4* – The IP address of IPv4. *Ipv6* – The IP address of IPv6.
Restrictions	None.

Example usage:

To display management address information for port 1:

```
DGS-3426:5#show lldp mgt_addr ipv4 192.168.254.10
Command: show lldp mgt_addr ipv4 192.168.254.10

Address 1
---------------------------------------------------
      Subtype      : IPv4
      Address      : 192.168.254.10
      IF type      : Unknown
      OID          : 1.3.6.1.4.1.171.10.36.1.11
      Advertising Ports : 1-5,7

DGS-3426:5#
```

show lldp ports

Purpose	Display the LLDP per port configuration for advertisement options.
Syntax	**show lldp ports {<portlist>}**
Description	This command is used to display 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-3426:5#show lldp ports 1
Command: show lldp ports 1:1

Port ID                : 1:1
-----------------------------------------------------------------
Admin Status           : TX_and_RX
Notification Status    : Disabled
Advertised TLVs Option :
    Port Description                                     Disabled
    System Name                                          Disabled
    System Description                                   Disabled
    System Capabilities                                  Disabled
    Enabled Management Address
        (None)
    Port VLAN ID                                         Disabled
    Enabled Port_and_Protocol_VLAN_ID
        (None)
    Enabled VLAN Name
        (None)
    Enabled Protocol_Identity
        (None)
    MAC/PHY Configuration/Status                          Disabled
    Power Via MDI                                         Disabled
    Link Aggregation                                      Disabled
    Maximum Frame Size                                    Disabled
 CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

show lldp local_ports

Purpose	Used to display the per-port information currently available for populating outbound LLDP advertisements.
Syntax	**show lldp local_ports {<portlist>} {mode [brief | normal | detailed]}**
Description	This command is used to display the per-port information currently available for populating outbound LLDP advertisements.
Parameters	*<portlist>* – Use this parameter to define ports to be configured. *brief* – Display the information in brief mode. *normal* – Display the information in normal mode. This is the default display mode. *detailed* – Display the information in detailed mode.
Restrictions	None.

Usage Example:

To display outbound LLDP advertisements for port 1-2:

```
DGS-3426:5#show lldp local_ports 1-2
Command: show lldp local_ports 1-2

Port ID : 1
-----------------------------------------------------------
Port ID Subtype                   : Local
Port ID                           : 1/1
Port Description                  : RMON Port  1 on Unit 1
Port PVID                         : 1
Management Address Count          : 1
PPVID Entries Count               : 0
VLAN Name Entries Count           : 1
Protocol Identity Entries Count   : 0
MAC/PHY Configuration/Status      : (See Detail)
Link Aggregation                  : (See Detail)
Maximum Frame Size                : 1536

Port ID : 2
-----------------------------------------------------------
Port ID Subtype                   : Local
Port ID                           : 1/1
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 is used to display the information learned from the neighbor parameters. Due to a memory limitation, only 32 VLAN Name entries and 10 Management Address entries can be received.
Parameters	*<portlist>* – Use this parameter to define ports to be configured. *mode* – Choose from three options: *brief* – Display the information in brief mode. *normal* – Display the information in normal mode. This is the default display mode. *detailed* – Display the information in detailed mode.
Restrictions	None.

Example usage:

To display remote table in brief mode:

```
DGS-3426:5#show lldp remote_ports 1-2 mode brief
Command: show lldp remote_ports 1-2 mode brief

Port ID: 1
---------------------------------------------------
Remote Entities Count   : 1
Entity 1
     Chassis ID Subtype     : MAC Address
     Chassis ID             : 00-01-0-2-03-04-01
     Port ID Subtype        : Local
     Port ID                : 1/3
     Port Description       : RMON Port 1 on Unit 3

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

show lldp statistics

Purpose	Used to display the system LLDP statistics information.
Syntax	**show lldp statistics**
Description	This command is used to display an overview of neighbor detection activity on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display global statistics information:

```
DGS-3426:5#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-3426:5#
```

show lldp statistics ports

Purpose	Used to display the ports LLDP statistics information.
Syntax	**show lldp statistics ports {<portlist>}**
Description	This command is used to display per-port LLDP statistics.
Parameters	*<portlist>* – Use this parameter to define ports to be configured. When portlist is not specified, information for all ports will be displayed.
Restrictions	None.

Usage Example:

To display statistics information of port 1:

```
DGS-3426:5#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-3426:5#
```

51

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 | infinite] collectoraddress <ipaddr> | collectorport <udp_port_number 1-65535> | maxdatagramsize <value 300-1400>}
config sflow analyzer_server	<value 1-4> {timeout [<sec 1-2000000 | infinite] collectoraddress <ipaddr> | collectorPort <udp_port_number 1-65535> | maxdatagramsize <value 300-1400>} (1)
delete sflow analyzer_server	<value 1-4>
show sflow analyzer_server	
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>} (1)
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 and Operator-level users can issue this command.

Example usage:

To enable the sFlow function:

```
DGS-3426:5#enable sflow
Command:enable sflow

Success.

DGS-3426:5#
```

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 and Operator-level users can issue this command.

Example usage:

To disable the sFlow:

```
DGS-3426:5#disable sflow
Command:disable sflow

Success.

DGS-3426:5#
```

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 1-2000000 | infinite] 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 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	*<value 1-4>* – Enter a value from *1* to *4* to identify the sFlow server being created here. *owner <name 16>* – Enter the owner of the entry made here. The user that added this sFlow analyzer configures this name.

create 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. If it is specified as infinite, the server will never timeout. *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* and *1400* bytes with a default setting of *1400* bytes.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create the sFlow server:

```
DGS-3426:5#create sflow analyzer_server 1 owner monitor
Command: create sflow analyzer_server 1 owner monitor

Success.

DGS-3426:5#
```

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 | infinite] collectoraddress <ipaddr> | collectorport <udp_port_number 1-65535> | maxdatagramsize <value 300-1400>} (1)**
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	*<value 1-4>* – Enter a value from *1* to *4* to identify the sFlow server being configured here. *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. If specified as infinite, the server will never timeout. *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 and Operator-level users can issue this command.

Example usage:

To configure the sFlow server:

```
DGS-3426:5#config sflow analyzer_server 1 collectoraddress 10.90.90.9
Command: config sflow analyzer_server 1 collectoraddress 10.90.90.9

Success.

DGS-3426:5#
```

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 is used to delete a previously created sFlow analyzer server.
Parameters	*<value 1-4>* – Enter the value identifying the analyzer to be deleted here.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete an sFlow analyzer server:

```
DGS-3426:5#delete sflow analyzer_server 1
Command: delete sflow analyzer_server 1

Success.

DGS-3426:5#
```

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 is used to display the settings for a previously created sFlow analyzer server.
Parameters	None.
Restrictions	None.

Example usage:

To display the sFlow analyzer server settings:

```
DGS-3426:5#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-3426:5#
```

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 is used to configure the settings for the Switch's counter poller. This mechanism will take a poll of the IF counters of the Switch and package them with the other previously mentioned data into a datagram which will be sent to the sFlow Analyzer Server for examination.
Parameters	*<portlist>* – Use this parameter to set the ports that will be mined for sFlow information. *all* – Use this parameter to set all ports to be mined for sFlow information. *analyzer_server_id <value 1-4>* – Enter a value from *1* to *4* to identify the sFlow server where this information will be sent. *interval [disable | <sec 20-120>]* – 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.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create the sFlow counter poller:

```
DGS-3426:5#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-3426:5#
```

config sflow counter_poller ports

Purpose	Used to configure the counter poller for the sFlow function of the switch.
Syntax	**config sflow counter_poller ports [<portlist> | all] {interval [disable | <sec 20-120>]}**
Description	This command is used to configure the settings for the Switch's counter poller. This mechanism will take a poll of the IF counters of the Switch and package them with the other previously mentioned data into a datagram which will be sent to the sFlow Analyzer Server for examination.
Parameters	*<portlist>* – Use this parameter to set the ports that will be mined for sFlow information. *all* – Use this parameter to set all ports to be mined for sFlow information. *interval [disable | <sec 20-120>]* – 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.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the sFlow counter poller settings:

```
DGS-3426:5#config sflow counter_poller ports 1 interval 50
Command: create sflow counter_poller ports 1 interval 50

Success.

DGS-3426:5#
```

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 is used to delete the Switch's counter poller.
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 and Operator-level users can issue this command.

Example usage:

To delete the sFlow counter poller settings:

```
DGS-3426:5#delete sflow counter_poller ports all
Command:delete sflow counter_poller ports all

Success.

DGS-3426:5#
```

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 is used to display the Switch's counter poller.
Parameters	None.
Restrictions	None.

Example usage:

To show the sFlow counter poller settings:

```
DGS-3426:5#show sflow counter_poller
Command:show sflow counter_poller

Port       Analyzer Server ID     Polling Interval (secs)
--------   --------------------   -----------------------
1          1                      20

Total Entries : 1

DGS-3426:5#
```

create sflow flow_sampler ports

Purpose	Used to configure the flow sampler settings for the sFlow function.
Syntax	**create sflow flow_sampler ports [<portlist> | all] analyzer_server_id <value 1-4> {rate <value 0-65535> | maxheadersize <value 18-256>}**
Description	This command is used to 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	*<portlist>* – Use this parameter to set the ports that will be mined for sFlow information. *all* – Use this parameter to set all ports to be mined for sFlow information. *analyzer_server_id <value 1-4>* – Enter a value from *1* to *4* to identify the sFlow server where this information will be sent. *rate <value 0-65535>* – 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. *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 and Operator-level users can issue this command.

Example usage:

To create the sFlow flow sampler:

```
DGS-3426:5#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-3426:5#
```

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>} (1)**
Description	This command is used 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	*<portlist>* – Use this parameter to set the ports that will be mined for sFlow information. *all* – Use this parameter to set all ports to be mined for sFlow information. *rate <value 0-65535>* – 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. *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 and Operator-level users can issue this command.

Example usage:

To configure the sflow flow sampler:

```
DGS-3426:5#config sflow flow_sampler ports 1 rate 20000 maxheadersize 128
Command: config sflow flow_sampler ports 1 rate 20000 maxheadersize 128

Success.

DGS-3426:5#
```

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 is used 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 and Operator-level users can issue this command.

Example usage:

To delete the sFlow flow sampler settings:

```
DGS-3426:5#delete sflow flow sampler ports all
Command: delete sflow flow sampler ports all

Success.

DGS-3426:5#
```

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 is used to display the Switch’s sFlow flow sampler information.
Parameters	None.
Restrictions	None.

Example usage:

To show the sFlow flow sampler settings:

```
DGS-3426:5#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-3426:5#
```

show sflow

Purpose	Used to display the sflow settings configured on the switch
Syntax	**show sflow**
Description	This command is used to display the Switch’s sFlow settings.
Parameters	None.
Restrictions	None.

Example usage:

To show the sFlow settings:

```
DGS-3426:5#show sflow
Command:show sflow

SFlow Version     : 1.00
SFlow Address     : 10.53.13.199
SFlow State       : Enabled

DGS-3426:5#
```

52

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 | IEEE802]}
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>
delete dhcp excluded_address	[begin_address <ipaddr> end_address <ipaddr> | all]

Command	Parameters
show dhcp excluded_address	
show dhcp pool	{ <pool_name 12>}

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 is used to create a DCHP pool for the DHCP server. Once created, this pool may be modified for accepting DHCP clients into this pool.
Parameters	*<pool_name 12>* – Enter an name of up to 12 alphanumeric characters to identify the pool to be created with this command.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create the DHCP pool Floor2:

```
DGS-3426:5#create dhcp pool Floor2
Command:create dhcp pool Floor2

Success.

DGS-3426:5#
```

delete dhcp pool

Purpose	Used to delete a DHCP pool.
Syntax	**delete dhcp pool {<pool_name 12> | all}**
Description	This command is used to delete a DHCP poll that was created with the **create dhcp pool** command.
Parameters	*<pool_name 12>* – Enter an name of up to 12 alphanumeric characters to identify the pool to be deleted with this command. *all* – Enter this command to delete all created DHCP pool.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete the DHCP pool Floor2:

```
DGS-3426:5#delete dhcp pool Floor2
Command:delete dhcp pool Floor2

Success.

DGS-3426:5#
```

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 | IEEE802]}**
Description	This command is used to 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	*<pool_name 12>* – Enter the name of the previously created pool that will contain the manual binding entry. *<ipaddr>* – 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. *hardware_address <macaddr>* – Enter the MAC address of the device to be statically bound to the IP address entered in the previous field. *type* [Ethernet | IEEE802] – This field is used to specify the type of connection for which this manually bound entry will be set. *Ethernet* will denote that the manually bound device is connected directly to the Switch, while the *IEEE802* denotes that the manually bound device is outside the local network of the Switch.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create a manual binding DHCP entry:

```
DGS-3426:5#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-3426:5#
```

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 is used to delete a DHCP manual binding entry created with the **create dhcp pool manual_binding** command.
Parameters	*<pool_name 12>* – Enter the previously created pool name from which to delete a manual binding DHCP entry. *<ipaddr>* – Enter the IP address of the manual binding entry to be deleted. *all* – Enter this command to delete all manual binding entries for the given pool.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete the multicast range Floor2:

```
DGS-3426:5#delete dhcp pool manual_binding Floor2 10.10.10.1
Command: delete dhcp pool manual_binding Floor2 10.10.10.1

Success.

DGS-3426:5#
```

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 is used to 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-3426:5#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-3426:5#
```

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-3426:5#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-3426:5#
```

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 and Operator-level users can issue this command.

Example usage:

To display the DHCP binding information on the Switch:

```
DGS-3426:5#clear dhcp_binding
Command:clear dhcp_binding

Success.

DGS-3426:5#
```

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 is used to 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 and Operator-level users can issue this command.

Example usage:

To configure the number of Ping packets to be used for DHCP:

```
DGS-3426:5#config dhcp ping_packets 2
Command: config dhcp ping_packets 2

Success.

DGS-3426:5#
```

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	*<millisecond 500-2000>* – 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 and Operator-level users can issue this command.

Example usage:

To configure the Ping timeout:

```
DGS-3426:5#config dhcp ping_timeout 500
Command: config dhcp ping_timeout 500

Success.

DGS-3426:5#
```

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	*<pool_name 12>* – Enter the previously created pool name from which the boot file will be set. *<file_name 64>* – Enter the name of the boot file that will be used for DHCP clients.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To set the boot file:

```
DGS-3426:5#config dhcp pool boot_file accounting boot.had
Command: config dhcp pool boot_file accounting boot.had

Success.

DGS-3426:5#
```

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	*<pool_name 12>* – Enter the previously created pool name for which to add a default router. *<ipaddr>* – 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 and Operator-level users can issue this command.

Example usage:

To configure the default router:

```
DGS-3426:5#config dhcp pool default_router accounting 10.245.32.1
Command: config dhcp pool default_router accounting 10.245.32.1

Success.

DGS-3426:5#
```

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	*<pool_name 12>* – Enter the previously created pool name for which to add a DNS address. *<ipaddr>* – Enter the IP address for the DNS server for this pool. Users may specify up to three DNS servers.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the DNS server address foe a DHCP pool:

```
DGS-3426:5#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-3426:5#
```

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 and Operator-level users can issue this command.

Example usage:

To configure the domain name for a DHCP pool:

```
DGS-3426:5#config dhcp pool domain_name accounting d_link.com
Command: config dhcp pool domain_name accounting d_link.com

Success.

DGS-3426:5#
```

config dhcp pool lease

Purpose	Used to configure the lease time of DCHP clients within a DHCP pool.
Syntax	**config dhcp pool lease<pool_name 12> [<day 0-365> <hour 0-23> <minute 0-59> | infinite]**
Description	This command is used to specify the 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. *day 0-365* – Enter the amount of days for the lease. The default setting is one day. *hour 0-23* – Enter the number of hours for the lease. *minute 0-59* – Enter the number of minutes for the lease. *infinite* – Enter this parameter to set the allotted IP address to never be timed out of its lease.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the lease time for the DHCP pool:

```
DGS-3426:5#config dhcp pool lease accounting infinite
Command: config dhcp pool lease accounting infinite

Success.

DGS-3426:5#
```

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	*<pool_name 12>* – Enter the previously created pool name for which to set the Net BIOS name server for DHCP clients. *<ipaddr>* – 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 and Operator-level users can issue this command.

Example usage:

To configure the Net BIOS name server for the DHCP pool:

```
DGS-3426:5#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-3426:5#
```

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 *Broadcast*, *Peer to Peer*, *Mixed* and *Hybrid*.
Parameters	*<pool_name 12>* – Enter the previously created pool name for which to set the Net BIOS node type for DHCP clients. *[broadcast* | *peer_to_peer* | *mixed* | *hybrid]* – Users may choose the node type for the Net BIOS from one of the four listed.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the Net BIOS node type for the DHCP pool:

```
DGS-3426:5#config dhcp pool netbios_node_type accounting hybrid
Command: config dhcp pool netbios_node_type accounting hybrid

Success.

DGS-3426:5#
```

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 is used 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	*<pool_name 12>* – Enter the previously created pool name for which to set the network address. *<network_address>* – 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).
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the network address for the DHCP pool:

```
DGS-3426:5#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-3426:5#
```

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	*<pool_name 12>* – Enter the previously created pool name for which to set the next server. *<ipaddr>* – Enter the IP address of the next server which has the boot file.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the IP address of the next server:

```
DGS-3426:5#config dhcp pool next_server accounting 10.99.88.77
Command: config dhcp pool next_server accounting 10.99.88.77

Success.

DGS-3426:5#
```

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 and Operator-level users can issue this command.

Example usage:

To enable DHCP server:

```
DGS-3426:5#enable dhcp_server
Command: enable dhcp_server

Success.

DGS-3426:5#
```

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 and Operator-level users can issue this command.

Example usage:

To disable the DHCP server:

```
DGS-3426:5#disable dhcp_server
Command: disable dhcp_server

Success.

DGS-3426:5#
```

show dhcp_server

Purpose	Used to display the DHCP server settings.
Syntax	**show dhcp_server**
Description	This command is used to 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-3426:5#show dhcp_server
Command:show dhcp_server

DHCP Server Global State: Disable
Ping Packet Number         : 2
Ping Timeout               : 500 ms

DGS-3426:5#
```

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 is used 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	*begin_address <ipaddr>* – Enter the beginning IP address of the range of IP addresses to be excluded from the DHCP pool. *end_address <ipaddr>* – Enter the ending IP address of the range of IP addresses to be excluded from the DHCP pool.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure IP addresses that will be excluded :

```
DGS-3426:5#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-3426:5#
```

delete dhcp excluded_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> | all]**
Description	This command is used 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	*begin_address <ipaddr>* – Enter the beginning IP address of the range of IP addresses to be deleted from the excluded IP address list, from the DHCP pool. *end_address <ipaddr>* – Enter the ending IP address of the range of IP addresses to be deleted from the excluded IP address list, from the DHCP pool. *all* – Enter this command to delete all excluded IP addresses, from the DHCP pool.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete excluded IP addresses:

```
DGS-3426:5#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-3426:5#
```

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 excluded IP addresses:

```
DGS-3426:5#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-3426:5#
```

show dhcp pool

Purpose	Used to show the DHCP pool information.
Syntax	**show dhcp pool {<pool_name 12>}**
Description	This command is used to display the DHCP pool information. Entering the command without the pool name will display all DHCP pool information on the switch.
Parameters	*<pool_name 12>* – Enter the name of the DHCP pool for which to view DHCP pool information.
Restrictions	None.

Example usage:

To display the DHCP pool information:

```
DGS-3426:5#show dhcp pool Floor2
Command: show dhcp pool Floor2

 Pool Name              :Floor2
 Network Address        :10.0.0.0/8
 Domain Name            :
 DNS Server Address     :0.0.0.0
 NetBIOS Name Server    :0.0.0.0
 NetBIOS Node Type      :Broadcast
 Default Router         :0.0.0.0
 Pool Lease             :1 Days, 0 Hours, 0 Minutes
 Boot File              :
 Next Server            :0.0.0.0

 Total Pool Entry: 1

DGS-3426:5#
```

53

DHCP SERVER SCREENING COMMANDS

The DHCP Server Screening Commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

The DHCP Server Screening commands allow you not only to restrict all DHCP server packets but also to receive any specified DHCP server packets by any specified DHCP client, it is useful when one or more than one DHCP servers are present on the network and both provide DHCP services to different distinct groups of clients. Enabling DHCP server screening for the first time will create both an access profile and access rule per port, following this other access rules can be created. These rules are used to block all DHCP server packets. Similarly, the addition of a permit DHCP entry will create one access profile and one access rule the first time the DHCP client MAC address is the client MAC address, and the source IP address is the same as the DHCP server's IP address (UDP port number 67). These rules are used to permit the DHCP server packets with specific fields, which the user configures.

When the DHCP server screening function is enabled, all DHCP server packets will be filtered from a specific port. Also, you are allowed to create entries for specific port-based server IP address and client MAC address binding entries. Be aware that the DHCP server screening function must be enabled first. Once all settings are complete, all DHCP server packets will be filtered from a specific port except those that meet the server IP address and client MAC address binding.

Command	Parameters
config filter dhcp_server	[add permit server_ip <ipaddr> {client_mac <macaddr>} ports [<portlist>|all] | delete permit server_ip <ipaddr> {client_mac <macaddr>} ports [<portlist>|all] | ports [<portlist>|all] state [enable|disable]]
show filter dhcp_server	
config filter dhcp_server trap_log	[enable | disable]
config filter dhcp_server illegal_server_log_suppress_duration	[1min | 5min | 30min]

Each command is listed in detail in the following sections.

config filter dhcp_server

Purpose	DHCP server packets except those that have been IP/client MAC bound will be filtered. This command is used to configure the state of the function for filtering of DHCP server packet and to add/delete the DHCP server/client binding entry.
Syntax	**config filter dhcp_server [add permit server_ip <ipaddr> {client_mac <macaddr>} ports [<portlist>|all] | delete permit server_ip <ipaddr> {client_mac <macaddr>} ports [<portlist>|all] | ports [<portlist>|all] state [enable|disable]]**
Description	This command has two purposes: to filter all DHCP server packets on the specified port(s) and to allow some DHCP server packets to be forwarded if they are on the pre-defined server IP address/MAC address binding list. Thus the DHCP server can be restricted to service a specified DHCP client. This is useful when there are two or more DHCP servers present on a network.
Parameters	*ipaddr* – The IP address of the DHCP server to be filtered. *macaddr* – The MAC address of the DHCP client. *state* – To Enable/disable the filter DHCP server state. *portlist* – The port list of filter DHCP server.
Restrictions	Only Administrator and Operator-level users can issue this command. Enabling the DHCP filter will create one access profile and create one access rule per port (UDP port 67). Addition of a DHCP filter permit entry will create one access profile and create one access rule (DA = client MAC address, SA = source IP address and UDP port 67).

Example usage:

To add an entry from the DHCP server/client filter list in the switch's database:

```
DGS-3426:5#config filter dhcp_server add permit server_ip 10.1.1.1 client_mac
00-00-00-00-00-01 ports 1:1-1:3
Command: config filter dhcp_server add permit server_ip 10.1.1.1 client_mac 00-
00-00-00-00-01 ports 1:1-1:3


Success.


DGS-3426:5#
```

To configure the DHCP server screening state:

```
DGS-3426:5#config filter dhcp_server ports 1:1-1:3 state enable
Command: config filter dhcp_server ports 1:1-1:3 state enable


Success.


DGS-3426:5#
```

show filter dhcp_server

Purpose	Used to display current DHCP server/client filter list created on the switch.
Syntax	**Show filter dhcp_server**
Description	This command is used to display DHCP server/client filter list created on the switch. The log ceasing unauthorized duration and the log/trap state.
Parameters	None.
Restrictions	None.

Example usage:

To display the DHCP server/client filter list created on the switch the log ceasing unauthorized duration and the log/trap state:

```
DGS-3426:5#show filter dhcp_server
Command: show filter dhcp_server

Filter DHCP Server Trap_Log State: Disabled

 Enabled Ports: 1:1-1:3

Illegal Server Log Suppress Duration:5 minutes
Filter DHCP Server/Client Table
Server IP Address Client MAC Address  Port
----------------- -----------------   -------------------
10.1.1.1          00-00-00-00-00-01   1:1-1:3

Total Entries: 1

DGS-3426:5#
```

config filter dhcp_server trap_log

Purpose	Used to configure the trap and log related to the DHCP server screening.
Syntax	**config filter dhcp_server trap_log [enable | disable]**
Description	This command is used to enable or disable trap/log related to DHCP server filter.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable log and trap for the DHCP server screening event:

```
DGS-3426:5#config filter dhcp_server trap_log disable
Command: config filter dhcp_server trap_log disable

Success.

DGS-3426:5#
```

config filter dhcp_server illegal_server_log_suppress_duration

Purpose	This function is used to configure the illegal server log suppress duration.
Syntax	**config filter dhcp_server illegal_server_log_suppress_duration [1min | 5min | 30min]**
Description	This command Iis used to filter any illegal DHCP server packets. The DHCP server who sends the illegal packets will be logged. This command is used to suppress the logging of DHCP servers who continue to send illegal DHCP packets. The same illegal DHCP server IP address that is detected will be logged only once regardless of how many illegal packets are sent.
Parameters	*illegal _server_log_suppress_duration* – The log can be suppressed by 1 minute, 5 minutes or 30 minutes. The default value is 5 minutes.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the illegal server log suppress duration for 30 minutes:

```
DGS-3426:5#config filter dhcp_server illegal_server_log_suppress_duration 30min
Command: config filter dhcp_server illegal_server_log_suppress_duration 30min


Success.

DGS-3627:5#
```

54

RSPAN COMMANDS

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

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

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

enable rspan

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

Example usage:

To enable RSPAN:

```
DGS-3426:5#enable rspan
Command: enable rspan
Success.

DGS-3426:5#
```

disable rspan

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

Example usage:

To disable RSPAN:

```
DGS-3426:5#disable rspan
Command: disable rspan

Success.

DGS-3426:5#
```

create rspan vlan

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

Example usage:

To create an RSPAN VLAN by VLAN name:

```
DGS-3426:5#create rspan vlan vlan_name v2
Command: create rspan vlan vlan_name v2

Success.

DGS-3426:5#
```

To create an RSPAN VLAN by VLAN ID:

```
DGS-3426:5#create rspan vlan vlan_id 6
Command: create rspan vlan vlan_id 6

Success.

DGS-3426:5#
```

delete rspan vlan

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

Example usage:

To delete an RSPAN VLAN by VLAN name:

```
DGS-3426:5#delete rspan vlan vlan_name v2
Command: delete rspan vlan vlan_name v2

Success.

DGS-3426:5#
```

To delete an RSPAN VLAN by VLAN ID:

```
DGS-3426:5#delete rspan vlan vlan_id 6
Command: delete rspan vlan vlan_id 6

Success.

DGS-3426:5#
```

config rspan vlan source

Purpose	Used by the source switch to configure the source settings for the RSPAN VLAN.
Syntax	**config rspan vlan [vlan_name <vlan_name>| vlan_id <vlanid 1-4094>] source {[add | delete] ports <portlist> [rx | tx | both]}]**
Description	This command is used to configure the source setting for the RSPAN VLAN on the source switch. The output port of the RSPAN mirrored packet will use the same destination port as defined by the mirror command. **Note:** That if RSPAN is enabled, the packets mirrored to the destination port are always added with RSPAN VLAN tag. If the mirror is enabled but RSPAN is disabled, the packets mirrored to the destination port may be in tagged or untagged form. **Note:** That only one RSPAN VLAN can be configured with source settings.
Parameters	*vlan_name* – Specifies the RSPAN VLAN by VLAN name. *vlan_id* – Specifies the RSPAN VLAN by VLAN ID. *source* – When ports are not specified by this command, the source of RSPAN can come from the source specified by the mirror command or the flow-based source specified by ACL. *add* – Add source ports. *delete* – Delete source ports. *ports <portlist>* – Specifies the source portlist to add or delete from the RSPAN souce. *rx* – Only monitors ingress packets. *tx* – Only monitors egress packets. *both* – Monitors both ingress and egress packets.
Restrictions	Only Administrator and Operator-level users can issue this command.

NOTE: If the ACL function has been used to implement per flow RSPAN, the source needs to be set otherwise the per port RSPAN will not work.

Example usage:

To config RSPAN VLAN by VLAN name:

```
DGS-3426:5#config rspan vlan vlan_name vlan2 source add ports 2-5 rx
Command: config rspan vlan vlan_name vlan2 source add ports 1:2-1:5 rx

Success.

DGS-3426:5#
```

To config RSPAN VLAN by VLAN ID:

```
DGS-3426:5#config rspan vlan vlan_id 6 source add ports 2-5 rx
Command: config rspan vlan vlan_id 6 source add ports 1:2-1:5 rx


Success.

DGS-3426:5#
```

To config RSPAN VLAN:

```
DGS-3426:5#config rspan vlan vlan_id 2 source
Command: config rspan vlan vlan_id 2 source

Success.

DGS-3426:5#
```

config rspan vlan redirect

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

Example usage:

To configure RSPAN redirect:

```
DGS-3426:5#config rspan vlan vlan_id 2 redirect add port 1:18
Command: config rspan vlan vlan_id 2 redirect add port 1:18

DGS-3426:5#
```

show rspan

Purpose	Used by display RSPAN configuration.
Syntax	**show rspan {[vlan_name <vlan_name> | vlan_id <vlanid 1-4094>]}**
Description	This command is used to display RSPAN configuration.
Parameters	*vlan_name* – Specifies the RSPAN VLAN by VLAN name. *vlan_id* – Specifies the RSPAN VLAN by VLAN ID.
Restrictions	None.

Example usage:

To display RSPAN:

```
DGS-3426:5#show rspan
Command: show rspan

RSPAN   : Enabled

RSPAN VLAN ID  : 2
--------------------
  Source Port
      RX           : 1:2-1:5
      TX           :
  Redirect Port    : 1:18

Total RSPAN VLAN :1
```

To display RSPAN by VLAN name:

```
DGS-3426:5#show rspan vlan_name vlan2
Command: show rspan vlan_name vlan2

RSPAN   : Enabled

RSPAN VLAN ID  : 2
--------------------
  Source Port
      RX           : 1:2-1:5
      TX           :
  Redirect Port    : 1:18

Total RSPAN VLAN :1
```

55

ACL FLOW METERING COMMANDS

ACL Flow Metering is used to configure per-flow Bandwidth Control. 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 1-6> 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 1-6> {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	**<value 1-6> 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	*profile_id <value 1-6>* – Enter the pre-configured Profile ID for which to configure the ACL Flow Metering parameters. *access_id <value 1-128>* – Enter the pre-configured Access ID for which to configure the ACL Flow Metering parameters. *tr_tcm* – 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. • *cir <value 1-156249>* – The Committed Information Rate can be set between *1* and *156249*. IP flow rates at or below this level will be considered *green*. IP flow rates that exceed this rate but not the PIR rate are considered *yellow*. • *cbs <value 1-16384>* – 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. • *pir <value 1-16384>* – The Peak information Rate. IP flow rates that exceed this setting will be considered as *red*. This field must be set at an equal or higher value than the CIR. • *pbs <value 1-16384>* – 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. *sr_tcm* – 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. • *cir <value 1-156249>* – 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. • *cbs <value 1-16384>* – 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. • *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.

config flow_meter profile_id

	• *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 and Operator-level users can issue this command. Only two counters may be enabled at any given time.

Example usage:

To enable ACL flow metering:

```
DGS-3426:5#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-3426:5#
```

show flow_meter

Purpose	Used to display the ACL flow meter parameters set on the switch.
Syntax	**show flow_meter {profile_id <value 1-6> {access_id <value 1-128>}}**
Description	This command is used to display the flow meter parameters set on the Switch.
Parameters	*profile_id <value 1-6>* – Enter the profile ID of the ACL entry to be viewed for flow metering. *access_id <value 1-128>* – Enter the access ID corresponding to the ACL entry to be viewed.
Restrictions	None.

Example usage:

To display ACL flow metering:

```
DGS-3426:5#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-3426:5#
```

56

LAYER 2 PROTOCOL TUNNELING (L2PT) COMMANDS

Users at different sites connected across a service-provider network need to use various Layer 2 protocols to scale their topologies to include all remote sites, as well as the local sites. STP must run properly, and every VLAN should build a proper spanning tree that includes the local site and all remote sites across the service-provider network.

Layer 2 Protocol Tunneling (L2PT), also known as BPDU tunneling, is a feature designed for service providers who carry traffic of multiple customers across their networks and are required to maintain the Layer 2 protocol configurations of each customer without impacting the traffic of other customers.

The L2PT commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameters
config bpdu_tunnel ports	[<portlist> | all] type [tunnel {stp|gvrp}|uplink|none]
show bpdu_tunnel	
enable bpdu_tunnel	
disable bpdu_tunnel	

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

config bpdu_tunnel ports	
Purpose	Used to configure L2PT on specified ports.
Syntax	**[<portlist> | all] type [tunnel {stp|gvrp}|uplink|none]**
Description	This command is used to configure L2PT on ports. When Q-in-Q is enabled on the Switch, the DA will be replaced by the tunnel multicast address, and the BPDU will be tagged with the tunnel VLAN based on the Q-in-Q VLAN configuration and the tunnel/uplink settings. When Q-in-Q is enabled on the Switch, the BPDU will have its DA replaced by the tunnel multicast address and be transmitted out based on the VLAN configuration and the tunnel/uplink settings. The tunnel multicast address for STP BPDU is 01-05-5d-00-00-00. The tunnel multicast address for GVRP BPDU is 01-05-5d-00-00-21.
Parameters	*ports* – Specifies the ports on which L2PT will be enabled or disabled. *type* – Specifies the type of ports.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure L2PT on ports:

```
DGS-3426:5#config bpdu_tunnel ports 1:1-1:4 type tunnel stp
Command: config bpdu_tunnel ports 1:1-1:4 type tunnel stp

Success.

DGS-3426:5#
```

show bpdu_tunnel

Purpose	Used to display the L2PT global state, tunnel destination MAC address, and port state.
Syntax	**show bpdu_tunnel**
Description	This command is used to display L2PT global state, tunnel destination MAC address, and port state.
Parameters	None.
Restrictions	None.

Example usage:

To display the L2PT state of all ports:

```
DGS-3426:5#show bpdu_tunnel
Command: show bpdu_tunnel

 BPDU Tunnel : Disabled
 STP Tunnel Multicast Address : 01-05-5D-00-00-00
 STP Tunnel Port : 1:1-1:4
 GVRP Tunnel Multicast Address : 01-05-5D-00-00-21
 GVRP Tunnel Port :
 Uplink Port :

DGS-3426:5#
```

enable bpdu_tunnel

Purpose	Used to enable the L2PT function.
Syntax	**enable bpdu_tunnel**
Description	This command is used to enable the L2PT function. By default, L2PT is disabled.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable L2PT:

```
DGS-3426:5#enable bpdu_tunnel
Command: enable bpdu_tunnel

Success.

DGS-3426:5#
```

disable bpdu_tunnel

Purpose	Used to disable the L2PT function.
Syntax	**disable bpdu_tunnel**
Description	This command is used to disable the L2PT function.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable L2PT:

```
DGS-3426:5#disable bpdu_tunnel
Command: disable bpdu_tunnel

Success.

DGS-3426:5#
```

57

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 } (1)
disable gratuitous_arp	{ipif <ipif_name 12>} {trap |log} (1)
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 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-3426:5#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-3426:5#
```

delete arpentry

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

Example Usage:

To delete an entry of IP address 10.48.74.121.125 from the ARP table:

```
DGS-3426:5#delete arpentry 10.48.74.121
Command: delete arpentry 10.48.74.121

Success.

DGS-3426:5#
```

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 is used to set the maximum amount of time, in minutes, that an ARP entry can remain in the Switch's ARP table, without being accessed, before it is dropped from the table.
Parameters	*time <value 0-65535>* – The ARP age-out time, in minutes. The value may be set in the range of *0* to *65535* minutes with a default setting of *20* minutes.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure ARP aging time:

```
DGS-3426:5#config arp_aging time 30
Command: config arp_aging time 30

Success.

DGS-3426:5#
```

show arpentry

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

Example usage:

To display the ARP table**:**

```
DGS-3426:5#show arpentry
Command: show arpentry

ARP Aging Time : 20

Interface      IP Address       MAC Address        Type
------------   --------------   ----------------   ---------------
System         10.0.0.0         FF-FF-FF-FF-FF-FF  Local/Broadcast
System         10.44.8.253      00-44-08-FD-09-09  Dynamic
System         10.63.67.7       00-09-41-D8-15-0E  Dynamic
System         10.90.90.90      00-19-5B-F5-26-C0  Local
System         10.255.255.255   FF-FF-FF-FF-FF-FF  Local/Broadcast

Total Entries: 5

DGS-3426:5#
```

clear arptable

Purpose	Used to remove all dynamic ARP table entries.
Syntax	**clear arptable**
Description	This command is used to remove dynamic ARP table entries from the Switch's ARP table. Static ARP table entries are not affected.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example Usage:

To remove dynamic entries in the ARP table:

```
DGS-3426:5#clear arptable
Command: clear arptable

Success.

DGS-3426:5#
```

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 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-3426:5#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-3426:5#
```

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 or disable the 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 disabled.
Parameters	*enable* – Enable sending of gratuitous ARP when IPIF status comes up. *disable* – Disable sending of gratuitous ARP when IPIF status comes up.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable send gratuitous ARP request in a normal situation:

```
DGS-3426:5#config gratuitous_arp send ipif_status_up enable
Command: config gratuitous_arp send ipif_status_up enable

Success.

DGS-3426:5#
```

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 or disable the sending of gratuitous ARP request packets while a duplicate IP is being detected. By default, the state is disabled. 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	*enable* – Enable sending of gratuitous ARP when a duplicate IP is detected. *disable* – Disable sending of gratuitous ARP when a duplicate IP is detected.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example Usage:

To enable send a gratuitous ARP request when a duplicate IP is detected:

```
DGS-3426:5#config gratuitous_arp send duplicate_ip_detected enable
Command: config gratuitous_arp send duplicate_ip_detected enable

Success.

DGS-3426:5#
```

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 or disable updating the ARP cache based on the received gratuitous ARP packets. The gratuitous ARP packet is sent by a source IP address that is identical to the IP that the packet is queries for. Note that, with the gratuitous ARP learning, the system will not learn new entry but only do the update on the ARP table based on the received gratuitous ARP packet. By default, the state is disabled.
Parameters	*enable* – Enable learning of ARP entry based on the received gratuitous ARP packet. *disable* – Disable learning of ARP entry based on the received gratuitous ARP packet.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable learning of ARP entry based on the received gratuitous ARP packet:

```
DGS-3426:5#config gratuitous_arp learning enable
Command: config gratuitous_arp learning enable

Success.

DGS-3426:5#
```

enable gratuitous_arp

Purpose	Used to enable gratuitous ARP trap and log state.
Syntax	**enable gratuitous_arp {ipif <ipif_name 12>} {trap |log} (1)**
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 disabled.
Parameters	*ipif <ipif_name 12>* – The name of the IP interface the end node or station for which the ARP table entry was made, resides on. *{trap|log}* – Select gratuitous ARP trap and/or log state.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable system interface's gratuitous ARP log and trap**:**

```
DGS-3426:5#enable gratuitous_arp System trap log
Command: enable gratuitous_arp System trap log

Success.

DGS-3426:5#
```

disable gratuitous_arp

Purpose	Used to disable gratuitous ARP trap and log state.
Syntax	**disable gratuitous_arp {ipif <ipif_name 12>} {trap |log} (1)**
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	*ipif <ipif_name 12>* – The name of the IP interface the end node or station for which the ARP table entry was made, resides on. *{trap|log}* – Select gratuitous ARP trap and/or log state.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example Usage:

To disable the system interface's gratuitous ARP log and trap:

```
DGS-3426:5#disable gratuitous_arp System trap log
Command: disable gratuitous_arp System trap log

Success.

DGS-3426:5#
```

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	<ipif_name 12> – The name of the Layer 3 interface. <value 0-65535> – Periodically send gratuitous ARP interval time in seconds. 0 – means not to send gratuitous ARP periodically.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure gratuitous ARP interval to 5 for IPIF System:

```
DGS-3426:5#config gratuitous_arp send periodically ipif System interval 5
Command: config gratuitous_arp send periodically ipif System interval 5

Success.

DGS-3426:5#
```

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-3426:5#show gratuitous_arp
Command: show gratuitous_arp

Send on IPIF status up        : Disabled
Send on Duplicate_IP_Detected : Disabled
Gratuitous ARP Learning       : Disabled

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

Total Entries: 1

DGS-3426:5#
```

58

COMPOUND AUTHENTICATION COMMANDS

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

Command	Parameters
create authentication guest_vlan	[vlan <vlan_name 32> | vlanid <vlanid 1-4094>]
delete authentication guest_vlan	[vlan <vlan_name 32> | vlanid <vlanid 1-4094>]
config authentication guest_vlan	[vlan <vlan_name 32> | vlanid <vlanid 1-4094>] [add|delete] ports [<portlist> | all]
config authentication ports	[<portlist>| all] {auth_mode [port_based | host_based] | multi_authen_methods [none | any | dot1x_impb | impb_jwac]} (1)
show authentication guest_vlan	
show authentication ports	{<portlist>}
enable authorization network	
disable authorization network	
show authorization	

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

create authentication guest_vlan

Purpose	Used to assign a static VLAN to be guest VLAN.
Syntax	**create authentication guest_vlan [vlan <vlan_name 32> | vlanid <vlanid 1-4094>]**
Description	This command is used to assign a static VLAN to be a guest VLAN. The specific VLAN which is assigned to a guest VLAN must exist first. The specific VLAN which has been assigned to a guest VLAN can't be deleted. For further description of this command please see description for **config authentication guest_vlan ports.**
Parameters	*vlan_name 32* – Specifies the guest vlan by VLAN name. *vlanid* – Specifies the guest VLAN by VLAN ID.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create an authentication guest VLAN:

```
DGS-3426:5#create authentication guest_vlan vlan Accounting
Command: create authentication guest_vlan vlan Accounting

Success.

DGS-3426:5#
```

delete authentication guest_vlan

Purpose	Used to delete a configured authentication guest VLAN.
Syntax	**delete authentication guest_vlan [vlan <vlan_name 32> | vlanid <vlanid 1-4094>]**
Description	This command is used to delete the guest VLAN settings, but will not delete the static VLAN. All ports which have an enabled guest VLAN will move to the original VLAN after the guest VLAN has been deleted.
Parameters	*vlan_name 32* – Specifies the guest vlan by VLAN name. *vlanid* – Specifies the guest vlan by VLAN ID.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete an authentication guest VLAN:

```
DGS-3426:5#delete authentication guest_vlan vlan Accounting
Command: delete authentication guest_vlan vlan Accounting

Success.

DGS-3426:5#
```

config authentication guest_vlan

Purpose	Used to configure the security port(s) as a specific guest VLAN member.
Syntax	**config authentication guest_vlan [vlan <vlan_name 32> | vlanid <vlanid 1-4094>] [add | delete] ports [<portlist> |all]**
Description	The user can use this command to assign or remove ports to/from a guest VLAN. If **multi_authen_methods** mode is **none**, this port is doing a single authentication. The port will operate based on the guest VLAN configured by the single authentication module's command. If the single authentication module's guest VLAN command (for example, JWAC has no guest VLAN command) is not available, the port will not be in guest VLAN mode. If **multi_authen_methods** mode is anything other than **none**, the port is doing compound authentication. The port will operate based on the guest VLAN configured by the common authentication command.
Parameters	*vlan_name* – Assign a name of a guest VLAN. The VLAN must be an existing static VLAN. *vlanid* – Assign a VLAN ID of a guest VLAN. The VLAN must be an existing static VLAN. *add* – Specifies to add a port list to the guest VLAN. *delete* – Specifies to delete a port list from the guest VLAN. *portlist* – Specifies the configured port(s).
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure authentication guest VLAN ports:

```
DGS-3426:5#config authentication guest_vlan vlan RG add ports all
Command: config authentication guest_vlan vlan RG add ports all

Success.

DGS-3426:5#
```

config authentication ports

Purpose	This command is used to configure security ports.
Syntax	**config authentication ports [<portlist>| all] {auth_mode [port_based | host_based] | multi_authen_methods [none | any | dot1x_impb | impb_jwac |]} (1)**
Description	This command is used to configure the authorization mode and authentication method on ports. If **multi_authen_methods** mode is **none**, this port is doing single authentication. The port will operate based on the authentication mode configured by the single authentication module's command. If **multi_authen_methods** mode is anything other than **none**, the port is doing compound authentication. The port will operate based on the authentication mode configured by the compound authentication command. The enable and disable settings of individual authentication willl always take effect. Suppose that a port's **multi_authen_methods** is set to **any** but MBAC is disabled and JWAC and 802.1X are enabled, then the user must pass either JWAC or 802.1X. Similarly, if the **multi_authen_methods** for a port is set to **impb_jwac** but JWAC is disabled and IMPB is enabled, then the authentication result will be the result of IMPB authentication.
Parameters	*portlist* – Specifies the ports to be configured. *auth_mode* – Choose between port-based or host-based. *port-based:* If one of the attached hosts passes the authentication process, all hosts on the same port will be granted access to the network. If the user fails the authorization process, this port will keep trying the next authentication. *host-based:* Every user can be authenticated individually. *multi_authen_methods* – Specifies the method for compound authentication. *none* – Specifies that compound authentication is not enabled. *any* – If any one of the authentication methods (802.1X, MBAC, and JWAC) are passed, then authentication will be passed. *dot1x_impb* – 802.1X will be verified first, and then IMPB will be verified. Both authentication methods need to be passed. *impb_jwac* – JWAC will be verified first, and then IMPB will be verified. Both authentication methods need to be passed.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the authentication mode of all ports to host-based:

```
DGS-3426:5#config authentication ports all auth_mode host_based
Command: config authentication ports all auth_mode host_based

Success.

DGS-3426:5#
```

To configure the compound authentication method of all ports to "any":

```
DGS-3426P:5#config authentication ports all multi_authen_methods any
Command: config authentication ports all multi_authen_methods any

Success.

DGS-3426P:5#
```

show authentication guest_vlan

Purpose	This command is used to display the guest VLAN settings.
Syntax	**show authentication guest_vlan**
Description	This command is used to show the information of the guest VLAN.
Parameters	None.
Restrictions	None.

Example usage:

To display the guest VLAN settings on the Switch**:**

```
DGS-3426:5#show authentication guest_vlan
Command: show authentication guest_vlan

Guest VLAN VID         :1
Guest VLAN Member Ports:4

 Total Entries: 1


DGS-3426:5#
```

show authentication ports

Purpose	This command is used to display authentication settings on port(s).
Syntax	**show authentication ports {<portlist>}**
Description	This command is used to display the authentication method and authorization mode on ports.
Parameters	*portlist* – Displays compound authentication on specific port(s).
Restrictions	None.

Example usage:

To display authentication settings for all ports**:**

```
DGS-3426:5#show authentication ports
Command: show authentication ports

 Port    Methods         Authorized Mode
 ----   --------------- -----------------
 1:1     Any                Host_based
 1:2     Any                Host_based
 1:3     Any                Host_based
 1:4     Any                Host_based
 1:5     Any                Host_based
 1:6     Any                Host_based
 1:7     Any                Host_based
 1:8     Any                Host_based
 1:9     Any                Host_based
 1:10    Any                Host_based
 1:11    Any                Host_based
 1:12    Any                Host_based
 1:13    Any                Host_based
 1:14    Any                Host_based
 1:15    Any                Host_based
 1:16    Any                Host_based
 1:17    Any                Host_based
 1:18    Any                Host_based
 1:19    Any                Host_based
 1:20    Any                Host_based

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

enable authorization network	
Purpose	To enable authorization on the Switch.
Syntax	**enable authorization network**
Description	This command is used to enable authorization of the network. When the authorization for network is enabled, whether the authorized data assigned by the RADUIS server will be accepted will depend on the individual module's setting. Authorization for the network is enabled by default.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable the authorization network**:**

```
DGS-3426:5#enable authorization network
Command: enable authorization network

Success.

DGS-3426:5#
```

disable authorization network	
Purpose	To disable authorization on the Switch.
Syntax	**disable authorization network**
Description	This command is used to disable the authorization of the network. When the authorization for network is disabled, the authorization data assigned by the RADUIS server will not be accepted and take effect. Authorization for the network is enabled by default.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable the authorization network**:**

```
DGS-3426:5#disable authorization network
Command: disable authorization network

Success.

DGS-3426:5#
```

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

Example usage:

To display authorization**:**

```
DGS-3426:5#show authorization
Command: show authorization

Authorization for Network: Enabled

DGS-3426:5#
```

59

WEB-BASED ACCESS CONTROL (WAC) COMMANDS

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 ports	[<portlist> | all] {state [enable | disable] | aging_time [infinite | <min 1-1440>] | idle_time [infinite | <min 1-1440>] | block_time [<sec 0-300>]} (1)
config wac method	[local | radius]
config wac auth_failover	[enable | disable]
config wac default_redirpath	<string 128>
config wac clear_default_redirpath	
config wac virtual_ip	<ipaddr>
config wac switch_http_port	< tcp_port_number 1-65535> {[http | https]}
create wac user	<username 15> {[vlan <vlan_name 32> | vlanid <vlanid 1-4094>]}
delete wac user	[<username 15> | all_users]
config wac user	<username 15> [vlan <vlan_name 32> | vlanid <vlanid 1-4094> | clear_vlan]
config wac authorization network	{radius [enable | disable]| local [enable | disable]} (1)
show wac	
show wac ports	{<portlist>}
show wac user	
show wac auth_state ports	{<portlist> }
clear wac auth_state	[ports [<portlist> | all] {authenticated | authenticating | blocked} | macaddr <macaddr>]

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

enable wac

Purpose	Used to enable Web-based access control on the Switch.
Syntax	**enable wac**
Description	This command is used to enable the WAC function on the Switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable WAC:

```
DGS-3426:5#enable wac
Command: enable wac

Success.

DGS-3426:5#
```

disable wac

Purpose	Used to disable Web-based access control on the Switch.
Syntax	**disable wac**
Description	This command is used to disable the WAC function on the Switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable WAC:

```
DGS-3426:5#disable wac
Command: disable wac

Success.

DGS-3426:5#
```

config wac ports

Purpose	Used to configure WAC port level settings on the Switch.
Syntax	**config wac ports [<portlist> | all] {state [enable | disable] | | aging_time [infinite | <min 1-1440>] | idle_time [infinite | <min 1-1440>] | block_time [<sec 0-300>] }**
Description	This command is used to configure WAC port level settings on the Switch.
Parameters	*state* – Specifies to enable/disable WAC state. *aging_time* – A time period during which an authenticated host will be kept in authenticated state. “infinite” indicates the authenticated host on the port will not ageout. The default value is 24 hours. *idle_time* – A time period after which an authenticated host will be moved to an un-authenticated state if there is no traffic during that period. “infinite” indicates the host will not be removed from the authenticated state due to the idle of traffic. The default value is infinite. *block_time* – If a host fails to pass the authentication, it will be blocked for this period of time before it can be re-authenticated. The default value is 60 seconds.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure port WAC state:

```
DGS-3426:5#config wac ports 1-8 state enable
Command: config wac ports 1:1-1:8 state enable

Success.

DGS-3426:5#
```

config wac method

Purpose	Used to configure the global parameter of the web authentication.
Syntax	**config wac method [local | radius]**
Description	This command is used to configure the global parameter for Web authentication.
Parameters	*method* – Specifies the authenticated method. *local* – The authentication will be done via the local database. *radius* – The authentication will be done via the RADIUS server.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the authentication method:

```
DGS-3426:5#config wac method radius
Command: config wac method radius

Success.

DGS-3426:5#
```

config wac auth_failover

Purpose	Used to configure WAC authorization failover.
Syntax	**config wac auth_failover [enable | disable]**
Description	This command is used to configure WAC authorization failover. When the authentication failover is disabled, if RADIUS servers are unreachable, the authentication will fail. When the authentication failover is enabled, if RADIUS servers authentication are unreachable, the local database will be used to do the authentication. The default state is disabled.
Parameters	*enable* – Enables the protocol authentication failover. *disable* – Disables the protocol authentication failover.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure WAC authentication failover:

```
DGS-3426:5#config wac auth_failover enable
Command: config wac auth_failover enable

Success.

DGS-3426:5#
```

config wac default_redirpath

Purpose	Used to configure WAC default redirect path.
Syntax	**config wac default_redirpath <string 128>**
Description	This command is used to configure WAC default redirect path. If the default redirect path is configured, the user will be redirected to the default redirect path after successful authentication. When the string is cleared, the client will not be redirected to another URL after successful authentication.
Parameters	*<string 128>* – The URL that the client will be redirected to after successful authentication. The redirected path is cleared by default.

config wac default_redirpath

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

Example usage:

To configure the WAC default redirect path:

```
DGS-3426:5#config wac default_redirpath http://2.3.2.3
Command: config wac default_redirpath http://2.3.2.3

Success.

DGS-3426:5#
```

config wac clear_default_redirpath

Purpose	Used to clear the WAC default redirect path.
Syntax	**config wac clear_default_redirpath**
Description	This command is used to clear the WAC default redirect path. When the string is cleared, the client will not be redirected to another URL after successful authentication.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the WAC clear default redirect path:

```
DGS-3426:5#config wac clear_default_redirpath
Command: config wac clear_default_redirpath

Success.

DGS-3426:5#
```

config wac virtual_ip

Purpose	Used to configure the WAC virtual IP address used to accept authentication requests from an unauthenticated host.
Syntax	**config wac virtual_ip <ipaddr>**
Description	When the virtual IP is specified, the TCP packet sent to the virtual IP will get a reply. If the virtual IP is enabled, TCP packets sent to the virtual IP or physical IPIF’s IP address will both get the a reply. When the virtual IP is set 0.0.0.0, the function of virtual IP is disabled. By default, the virtual IP is 0.0.0.0. The virtual IP will not respond to any ARP request or ICMP packets. To make the function work properly, the virtual IP should not be an existing IP address. It also cannot be located on the existing subnet.
Parameters	*<ipaddr>* – Specifies the IP address of the virtual IP.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the WAC virtual IP:

```
DGS-3426:5#config wac virtual_ip 1.1.1.1
Command: config wac virtual_ip 1.1.1.1

Success.

DGS-3426:5#
```

config wac switch_http_port

Purpose	Used to configure the TCP port that the WAC Switch listens to.
Syntax	**config wac switch_http_port < tcp_port_number 1-65535> {[http | https]}**
Description	The TCP port for HTTP or HTTPs is used to identify the HTTP or HTTPs packets that will be trapped to the CPU for authentication processing, or to access the login page. If not specified, the default port number for HTTP is 80, and the default port number for HTTPS is 443. If no protocol is specified, the protocol is HTTP. The HTTP cannot run at TCP port 443, and the HTTPS cannot run at TCP port 80.
Parameters	*<tcp_port_number 1-65535>* – A TCP port which the WAC Switch listens to and uses to finish the authenticating process. *http* – To specify that WAC runs HTTP protocol on this TCP port. *https* – To specify that WAC runs HTTPS protocol on this TCP port.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the WAC switch HTTP port:

```
DGS-3426:5# config wac switch_http_port 8888 http
Command: config wac switch_http_port 8888 http

Success.

DGS-3426:5#
```

create wac user

Purpose	Used to create a user account for Web-based Access control.
Syntax	**create wac user <username 15> {[vlan <vlan_name 32> | vlanid <vlanid 1-4094>]}**
Description	This command is used to create accounts for Web-based access control. This user account is independent from the login user account. If VLAN is not specified, the user will not get a VLAN assigned after the authentication.
Parameters	*username* – User account for Web-based access control. *vlan* – Specifies the authentication VLAN name.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create WAC account:

```
DGS-3426:5#create wac user vlan vlanid 2
Command: create wac user vlan vlanid 2

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

DGS-3426:5#
```

delete wac user

Purpose	Used to delete the Web-based access control.
Syntax	**delete wac user <username 15>**
Description	This command is used to delete an account.
Parameters	*username* – Specifies the user name for Web-based access control.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete WAC account:

```
DGS-3426:5#delete wac user 123
Command: delete wac user 123

Success.

DGS-3426:5#
```

config wac user

Purpose	Used to configure the VLAN ID of the user account.
Syntax	**config wac user <username 15> [vlan <vlan_name 32> | vlanid <vlanid 1-4094> | clear_vlan]**
Description	This command is used to change the VLAN associated with a user.
Parameters	*username* – The name of user account to be configured. *vlan* – Specifies the Authentication VLAN name. *clear_vlan* – Specifies that a previously configured VLAN is to be cleared.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To config the WAC user:

```
DGS-3426:5#config wac user alpha vlan vlan123
Command: config wac user alpha vlan vlan123

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

DGS-3426:5#
```

config wac authorization network

Purpose	To enable the acceptance of an authorized configuration.
Syntax	**config wac authorization network {radius [enable | disable]| local [enable | disable]}**
Description	This command is used to configure the acceptance of an authorized configuration. When the authorization is enabled for WAC's radius, the authorized data assigned by the RADUIS server will be accepted if the global authorization network is also enabled. When the authorization is enabled for WAC's local, the authorized data assigned by the local database will be accepted.
Parameters	*radius* – If enabled, the authorized data assigned by the RADUIS server will be accepted if the global authorization network is enabled. The default state is enabled. *local* – If specified to enable, the authorized data assigned by the local database will be accepted if the global authorization network is enabled. The default state is enabled.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure WAC authorization from the local database:

```
DGS-3426:5#config wac authorization network local disable
Command: config wac authorization network local disable

Success.

DGS-3426:5#
```

show wac

Purpose	Used to display the Web authentication global settings.
Syntax	**show wac**
Description	This command is used to display the WAC global settings.
Parameters	None.
Restrictions	None.

Example usage:

To display WAC:

```
DGS-3426:5#show wac
Command: show wac

 Web-Base Access Control
 --------------------------------
 State                  : Disabled
 Method                 : Local
 Authentication Failover : Disabled
 Redirect Path          :
 Virtual IP             : 0.0.0.0
 Switch HTTP Port       : 80 (HTTP)
 RADIUS Authorization   : Enabled
 Local Authorization    : Disabled

DGS-3426:5#
```

show wac ports

Purpose	Used to display the Web Authentication port level settings.
Syntax	**show wac ports {<portlist>}**
Description	This command is used to display the port level setting.
Parameters	*ports* – A range of member ports to show the status.
Restrictions	None.

Example usage:

To show WAC ports:

```
DGS-3426:5#show wac ports 1-3
Command: show wac ports 1:1-1:3

 Port    State        Aging Time    Idle Time      Block Time
                      (Minutes)     (Minutes)       (Seconds)
 -----  --------    -------------  -------------  -----------
 1:1    Disabled    1440           Infinite       60
 1:2    Disabled    1440           Infinite       60
 1:3    Disabled    1440           Infinite       60

DGS-3426:5#
```

show wac user

Purpose	Used to display the Web Authentication user.
Syntax	**show wac user**
Description	This command is used to display the Web Authentication account.
Parameters	None.
Restrictions	None.

Example usage:

To show Web Authenticaiton account:

```
DGS-3426:5#show wac user
Command: show wac user

 Username           Password      VLAN ID
 ---------------    -----------   ---------
 vlan               1              2

 Total Entries:1

DGS-3426:5#
```

show wac auth_state

Purpose	Used to display the authentication state of a port.
Syntax	**show wac auth_state ports {<portlist>}**
Description	This command is used to display the authentication state for ports. If port 1 is in host-based mode: (1) mac 00-00-00-00-00-01 is authenticated without VLAN assigned (may be the specified target VLAN does not exist or the target VLAN has not been specified), the ID of RX VLAN will be displayed (RX VLAN ID is 4004 in this example). (2) mac 00-00-00-00-00-02 is authenticated with target VLAN assigned, the ID of target VLAN will be displayed (target VLAN ID is 1234 in this example) (3) mac 00-00-00-00-00-03 failed to pass authentication, the VID field will be shown as “-” indicating that packets with SA 00-00-00-00-00-03 will be droped no matter which VLAN these packets are from. (4) mac 00-00-00-00-00-04 attempts to start authentication, the VID field will be shown as “-“ until authentication completed. If port 2 is in port-based mode: (1) mac 00-00-00-00-00-10 is the mac which made port 2 pass authentication, mac address with “(P)” in the end indicats that this authentication is from a port in port-based mode. If port 3 is in port-based mode: (1) mac 00-00-00-00-00-20 attempts to start authentication, mac address with “(P)” in the end indicats the port-based mode authentication. (2) mac 00-00-00-00-00-21 failed to pass authentication, mac address with “(P)” in the end indicats the port-based mode authentication. **NOTE :** In port-based mode, the VLAN ID field is displayed in the same way as host-based mode
Parameters	*ports* – Specifies the list of ports whose WAC state will be displayed.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To display the WAC authentication state:

```
DGS-3426:5# show wac auth_state ports 1-3
Command: show wac auth_state ports 1:1-1:3

Port MAC Address            State              VID       Priority     Aging Time/
Idle Time
                                                                       Block Time
---- ------------------ ------------- ------- --------- ------------- --------
1     00-00-00-00-00-01     Authenticated    4004          3              Infinite
40
1     00-00-00-00-00-02     Authenticated    1234          -              Infinite
50
1     00-00-00-00-00-03     Blocked               -             -               60
-
1      00-00-00-00-00-04      Authenticating    -              -               10
-
2      00-00-00-00-00-10(P)  Authenticated    1234          2               1440
20
3      00-00-00-00-00-20(P)  Authenticating   -              -                 5
-
3     00-00-00-00-00-21(P)  Blocked              -            -               100
-

Total Authenticating Hosts :2
Total Authenticated Hosts  :3
Total Blocked Hosts        :2

DGS-3426:5#
```

clear wac auth_state

Purpose	Used to clear the authentication state of a port.
Syntax	**clear wac auth_state [ports [<portlist> | all] {authenticated | authenticating | blocked} | macaddr <macaddr>]**
Description	This command is used to clear the authentication state of a port. If the port is in port-based mode, the port will return to an un-authenticated state. All the timers associated with the port will be reset. If the port is in host based mode, users on this port will be cleared. The user needs to be re-authenticated to access the network.
Parameters	*ports* – Specifies the list of ports whose WAC state will be cleared. *authenticated* – Specifies that all authenticated users for a port will be cleared. *authenticating* – Specifies that all authenticating users for a port will be cleared. *blocked* – Specifies to clear all blocked users for a port. *macaddr* – Specifies to clear a specific user by their MAC address.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To clear WAC authentication state:

```
DGS-3426:5#clear wac auth_state ports 1-5
Command: clear wac auth_state ports 1:1-1:5

Success.

DGS-3426:5#
```

60

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	Parameters
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> | vlanid <vlanid>] | delete protocol_group [group_id <id>|all]]
show port dot1v	{ports <portlis> }

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 is used to 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	*group_id <id>* – Enter an integer from *1* to *16* to identify the protocol VLAN group being created here.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create a protocol group:

```
DGS-3426:5#create dot1v_protocol_group group_id 1
Command: create dot1v_protocol_group group_id 1

Success.

DGS-3426:5#
```

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 is used to configure a protocol template for a group. Users may set the frame type to be added or deleted, along with the appropriate *protocol_value* in hexidecimal form. After being configured, this group may be attached to a port or range of ports using the **config port dot1v** command.
Parameters	*group_id <id>* – Enter an integer from *1* to *16* to identify the protocol VLAN group being configured here. *add* | *delete* – Choose whether to add or delete the protocol to this group. This protocol is identified using the following *protocol* parameter. *protocol* – 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 *protocol_value* stated here. This frame type must be followed by the correct *protocol_value*. The user has three choices: • *ethernet_2* – 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 *protocol_value.* • *ieee802.3_snap* – 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 *protocol_value.* • *ieee802.3_llc* – 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 *protocol_value*. The first octet defines the Destination Service Access Point value and the second octet is the Source Service Access Point (SSAP) value. *<protocol_value>* – Enter the corresponding protocol value of the protocol identified in the previous field. This value must be stated in a hexadecimal form.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure a protocol template:

```
DGS-3426:5#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-3426:5#
```

delete dot1v_protocol_group

Purpose	Used to delete a protocol VLAN group.
Syntax	**delete dot1v_protocol_group group_id <id>**
Description	This command is used to delete a protocol VLAN group.
Parameters	*group_id <id>* – Enter an integer from *1* to *16* to identify the protocol VLAN group being deleted here.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete a protocol VLAN group:

```
DGS-3426:5#delete dot1v_protocol_group group_id 1
Command: delete dot1v_protocol_group group_id 1

Success.

DGS-3426:5#
```

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 is used to display the configurations of a protocol VLAN group.
Parameters	*group_id <id>* – 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-3426:5#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-3426:5#
```

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 32> | vlanid <vlanid>] | delete protocol_group [group_id <id>|all]]**
Description	This command is used to bind a VLAN with a protocol template on one or more ports. When an ingress untagged packet is identified by the *protocol_value* 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	*ports* – Use this parameter to specify ports. • *<portlist>* – Use this parameter to assign a port or group of ports. • *all* – Use this parameter to specify all ports on the system. *add protocol_group group_id <id>* – 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. *vlan* – Use this parameter bind a VLAN with a specific protocol template using either of the following parameters: • *vlan_name 32* – Identify the VLAN name for which to add a tag to ingress untagged packets. • *<vlanid>*- Identify the VLAN-ID for which to add a tag to ingress untagged packets *delete protocol_group* – Use this parameter to remove this protocol VLAN group's association with the ports stated in this command, by using the following parameters: • *group_id <id>* – Enter this parameter with its corresponding group number, to remove this pre-defined protocol group from the ports specified here. • *all* – Use this parameter to remove all protocol VLAN groups from the ports specified in this command.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To bind a VLAN with a protocol template:

```
DGS-3426:5#config port dot1v ports 1:6-1:8 add protocol_group group_id 1 vlan
vlan_name building1
Command: config port dot1v ports 1:6-1:8 add protocol_group group_id 1 vlan
vlan_name building1

Success.

DGS-3426:5#
```

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 is used to display the protocol VLAN group and VLANs for individual ports.
Parameters	*ports <portlist>* – 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-3426:5#show port dot1v ports 1:6-1:8
Command: show port dot1v ports 1:6-1:8

Port: 1:6
Protocol Group ID             VLAN Name
-------------------------     ----------------
1                             RG1

Port: 1:7
Protocol Group ID             VLAN Name
-------------------------     ----------------
1                             RG1

Port: 1:8
Protocol Group ID             VLAN Name
-------------------------     ----------------
1                             RG1

Total Entries: 3

DGS-3426:5#
```

61

MULTICAST VLAN REPLICATION COMMANDS

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

Command	Parameters
enable ipmc_vlan_replication	
disable ipmc_vlan_replication	
config ipmc_vlan_replication	{ttl [decrese | no_decrease] | src_mac [replace | no_replace]} (1)
create ipmc_vlan_replication_entry	<name 16>
config ipmc_vlan_replication_entry source	<name 16> [[vlan <vlan_name 32> | vlanid <vlanid 1-4094>] | group [add | delete] [mcast_ip <mcast_address_list>| mcast_ipv6 <mcastv6_address_list>]{[source_ip<ipaddr>|source_ipv6 <ip6addr>]}]
config ipmc_vlan_replication_entry destination	<name 16> [add | delete] [vlan <vlan_name 32> | vlanid <vidlist>] ports <portlist>
delete ipmc_vlan_replication_entry	{<name 16>}
show ipmc_vlan_replication	
show ipmc_vlan_replication_entry	{<name 16>}

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

enable ipmc_vlan_replication

Purpose	Used to enable static IP multicast VLAN replication on the Switch.
Syntax	**enable ipmc_vlan_replication**
Description	This command is used to enable static IP multicast VLAN replication on the Switch. The replication function is enabled by default.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable static IP multicast VLAN replication:

```
DGS-3426:5#enable ipmc_vlan_replication
Command: enable ipmc_vlan_replication

Success.

DGS-3426:5#
```

disable ipmc_vlan_replication

Purpose	Used to disable the static IP multicast VLAN replication on the Switch.
Syntax	**disable ipmc_vlan_replication**
Description	This command is used to disable the static IP multicast VLAN replication on the switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable the static IP multicast VLAN replication:

```
DGS-3426:5#disable ipmc_vlan_replication
Command: disable ipmc_vlan_replication

Success.

DGS-3426:5#
```

config ipmc_vlan_replication

Purpose	Used to configure the IP multicast VLAN replication global settings.
Syntax	**config ipmc_vlan_replication {ttl [decrese | no_decrease] | src_mac [replace | no_replace]} (1)**
Description	Generally, when a multicast packet is forwarded across VLANs, the ttl will be decreased by one. If no_decrease is specified, the ttl will not be decreased. Similarly, it can be specified to replace source Mac address for packet to be forwarded across VLAN.
Parameters	*ttl [decrese*|*no_decrease]* – Species whether to decrease the time to live of packet. By default, the ttl will be decreased. *src_mac [replace*| *no_replace]* – Specifies whether to replace the source Mac address of the packet. By default, the source MAC address will be replaced.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To specify that the ttl decreases for the IP multicast VLAN replicated packet:

```
DGS-3426:5#config ipmc_vlan_replication ttl decrease
Command: config ipmc_vlan_replication ttl decrease

Success.

DGS-3426:5#
```

create ipmc_vlan_replication_entry

Purpose	Used to create an IP multicast VLAN replication entry.
Syntax	**create ipmc_vlan_replication_entry <name 16>**
Description	This command is used to create an IPMC VLAN replication entry. The entry will be identified by name. An IP multicast VLAN replication entry defines what traffic will be replicated and how the packet will be replicated.
Parameters	<*name 16*> – The name of the IP multicast VLAN replication entry.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create an IP multicast VLAN replication entry:

```
DGS-3426:5#create ipmc_vlan_replication_entry rg1
Command: create ipmc_vlan_replication_entry rg1

Success.

DGS-3426:5#
```

config ipmc_vlan_replication_entry source

Purpose	Used to configure the source traffic of an IP multicast VLAN replication entry.
Syntax	**config ipmc_vlan_replication_entry source <name 16> [[vlan <vlan_name 32> | vlanid <vlanid 1-4094>] | group [add | delete] [mcast_ip <mcast_address_list> | mcast_ipv6 <mcastv6_address_list>] {[source_ip <ipaddr> | source_ipv6 <ip6addr>]}]**
Description	This command is used to configure the traffic to be replicated by the IP multicast VLAN replication entry. The traffic is described by a source VLAN, a list of multicast group addresses and an optional source IP address associated with the multicast group. Each (V, G, S) will consume one resource entry. Therefore, the resource entry consumed by a replication entry is not constant and it will be determined by the number of (V, G, S) pair defined by the entry. If the entries (V, G, S) and (V, G, *) both exist in the table, the entries (V,G, *) will not take effect.
Parameters	*<name 16>* – The name of the IP multicast VLAN replication entry. *vlan <vlan_name 32>* – The source VLAN name. *vlanid <vlanid 1-4094>* – The source vlan id. *group [add | delete]* – Specifies to add or delete multicast IP address. *mcast_ip <mcast_address_list>* – IPv4 multicast address list. *mcast_ipv6 <mcastv6_address_list>* – IPv6 multicast address list. *source_ip <ipaddr>* – IPv4 source address. *source_ipv6 <ip6addr>]* – IPv6 source address.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To set the source VLAN of an IP multicast VLAN replication entry to VLAN v2:

```
DGS-3426:5#config ipmc_vlan_replication_entry source rg1 vlan v2
Command: config ipmc_vlan_replication_entry source rg1 vlan v2

Success

DGS-3426:5#
```

config ipmc_vlan_replication_entry destination

Purpose	Used to configure the destination of an IP multicast VLAN replication entry.
Syntax	**config ipmc_vlan_replication_entry destination <name 16> [add|delete] [vlan <vlan_name 32> | vlanid <vidlist>] ports <portlist>**
Description	For the traffic that matches an IPMC VLAN replication entry, it will be replicated based on the destination settings. Multiple destination entries can be defined for an IPMC VLAN replication entry. Each destination entry specifies the VLAN and the outgoing port on which the traffic will be replicated. The outgoing port must be a member port of the VLAN. Whether a packet egress to a port is tagged or untagged will be determined by the VLAN setting.
Parameters	*<name 16>* – The name of the IP multicast VLAN replication entry. *[add|delete]* – add or delete destination. *vlan <vlan_name 32>* – The outgoing vlan name. *vlanid <vidlist>* – The outgoing vlan ID. *ports <portlist>* – The outgoing port list.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the destination of an IP multicast VLAN replication entry:

```
DGS-3426:5#config ipmc_vlan_replication_entry destination rg1 add vlanid 5 ports
10-17
Command: config ipmc_vlan_replication_entry destination rg1 add vlanid 5 ports
1:10-1:17

Success.

DGS-3426:5#
```

delete ipmc_vlan_replication_entry

Purpose	Used to delete an IP multicast VLAN replication entry.
Syntax	**delete ipmc_vlan_replication_entry <name 16>**
Description	This command is used to delete an IP multicast VLAN replication entry.
Parameters	*<name 16>* – The name of the IP multicast VLAN replication entry.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete an IP multicast VLAN replication entry:

```
DGS-3426:5#delete ipmc_vlan_replication_entry rg1
Command: delete ipmc_vlan_replication_entry rg1

Success.

DGS-3426:5#
```

show ipmc_vlan_replication

Purpose	Used to display the IP multicast VLAN replication global settings.
Syntax	**show ipmc_vlan_replication**
Description	This command is used to display the IP multicast VLAN replication global settings.
Parameters	None.
Restrictions	None.

Example usage:

To display an IP multicast VLAN replication global configure:

```
DGS-3426:5#show ipmc_vlan_replication
Command: show ipmc_vlan_replication

IP Multicast VLAN Replication State :  Disabled

TTL                                 : No Decrease

Source MAC Address                  : Replace


DGS-3426:5#
```

show ipmc_vlan_replication_entry

Purpose	Used to display the IP multicast VLAN replication entries.
Syntax	**show ipmc_vlan_replication_entry {<name 16>}**
Description	This command is used to display the IP multicast VLAN replication entry.
Parameters	*<name 16>* – The name of the IP multicast VLAN replication entry.
Restrictions	None.

Example usage:

To display an IP multicast VLAN replication entry:

```
DGS-3426:5# show ipmc_vlan_replication entry rg1
Command: show ipmc_vlan_replication entry rg1

IP Multicast VLAN Replication Name   : rg1
---------------------------------------------
Source
VLAN ID/Name : 1/default
Multicast Group Address  List (G/S)
            225.1.1.1-225.1.1.10   /  *
            225.1.1.1-225.1.1.10   /  10.0.0.1

Destination
VLAN  ID/Name : 2/ VLAN2
    Portlist   : 1:1-1:11,1:13

DGS-3426:5#
```

Appendix A

TECHNICAL SPECIFICATIONS

Specifications listed here apply to all Switches in the xStack® DGS–3400 Series except where otherwise noted.

General	
Standards	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 802.3ae (10G Optional Modules) IEEE 802.1D/w/s Spanning Tree (Rapid, Multiple) IEEE 802.1P/Q VLAN IEEE 802.1p Priority Queues IEEE 802.1v Protocol VLAN IEEE 802.1X Network Access Control IEEE 802.3 Nway auto–negotiation IEEE 802.3ad Link Aggregation Control IEEE 802.3x Full–duplex Flow Control IEEE 802.1u Fast Ethernet IEEE 802.3af Power–over–Ethernet
Protocols	CSMA/CD
Data Transfer Rates:	Half–duplex Full–duplex
Ethernet	10 Mbps 20Mbps
Fast Ethernet	100Mbps 200Mbps
Gigabit Ethernet	1000Mbps 2000Mbps
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) WDM Single Mode Transceiver 10km (DEM–330T/R) WDM Single Mode Transceiver 40km (DEM–331T/R)
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)

Physical and Environmental		
Internal power supply **Redundant power supply**	AC Input: 100 – 240 VAC, 50–60 Hz	
Power Consumption	**DGS–3400 Series Switch** DGS–3426 (78.2 Watts) DGS–3426P (517.0 Watts) DGS–3427 (86.68 Watts) DGS–3450 (144.47 Watts)	**Module Inserts** DEM–410CX (0.015 Watts) DEM–410X (6.16 Watts)
DC fans:	12 V fans	
Operating Temperature	0 – 40°C	
Storage Temperature	–40 – 70°C	
Humidity	5 – 95% non–condensing	
Dimensions	441mm x 389mm x 44mm	
Weight	**DGS–3400 Series Switch** DGS–3426 (5.42 kg) DGS–3426P (6 kg) DGS–3427 (5.51 kg) DGS–3450 (5.74 kg)	**Module Inserts** DEM–410CX (0.16 kg) DEM–410X (0.18 kg)
EMI:	CE class A, FCC Class A	
Safety:	CSA International, CB Report	

Performance	
Transmission Method	Store–and–forward
Packet Buffer	0.75 MB per device
Packet Filtering / Forwarding Rate	Full–wire speed for all connections. 1,488,095 pps per port (for 1000Mbps)
MAC Address Learning	Automatic update. Supports 8K MAC address.
Priority Queues	8 Priority Queues per port.
Forwarding Table Age Time	Max age: 10–1000000 seconds. Default = 300.