D-Link®

DGS-3224TGR
Layer 2 Switch

Command Line Interface Reference Manual

Second Edition (February 2004)

6S24TGRCLI02

Printed In China

Trademarks

Copyright Statement

Table of Contents

1

INTRODUCTION

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

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

Accessing the Switch via the Serial Port

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

- 9600 baud
- no parity
- 8 data bits
- 1 stop bit

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

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

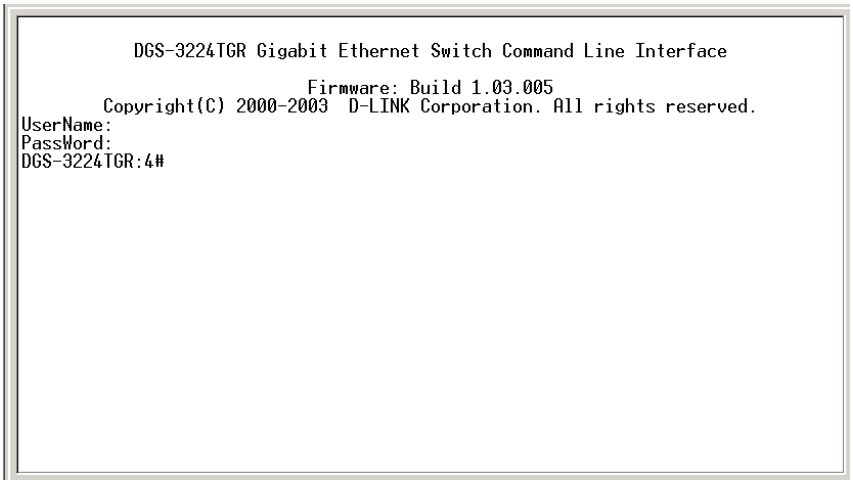

Figure 1-1. Initial Console screen.

There is no initial username or password. Just press the **Enter** key twice to display the CLI input cursor – **DGS-3224TGR:4#.** 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 or 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 that cannot be changed.

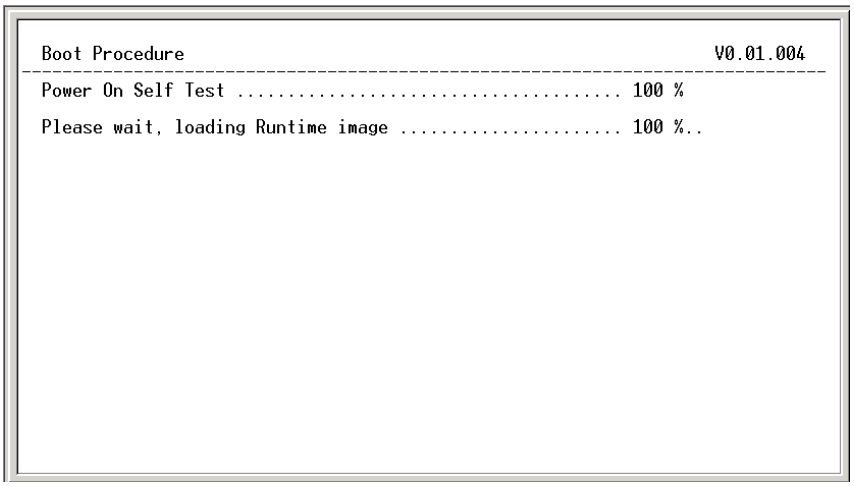

Figure 1-2. Boot Screen

The switch's MAC address can be found from the console program under the Switch Information menu item, as shown below.

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.

By default, an IP interface named System is configured on the switch and contains all of the ports on the switch. The System interface can be used initially to assign a range of IP addresses to the switch. Later, when you configure VLANs and IP interfaces on the switch, the ports you assign to these VLANs and IP interfaces will be removed from the System interface.

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 **DGS-3224TGR:4#** – 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. Alternaltively, you can enter **DGS3224TGR:4#** – enter the commands **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.

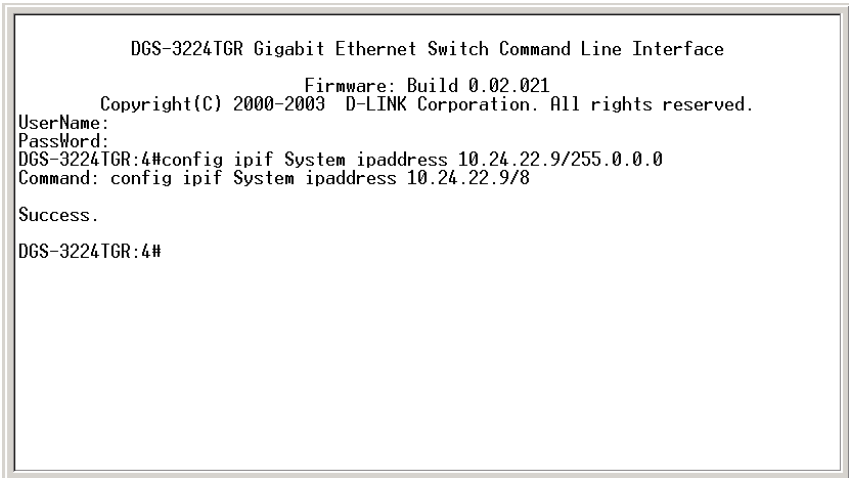

Figure 1-3. Assigning the Switch an IP Address

In the above example, the switch was assigned an IP address of 10.24.22.9 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 and the CLI or via the Web-based management agent using the above IP address to connect to the switch.

2

USING THE CONSOLE CLI

The DGS-3224TGR 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.

Switch configuration settings are saved to non-volatile RAM using *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
- 9,600 baud
- 8 data bits
- No parity
- One stop bit
- No flow control

You can 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:

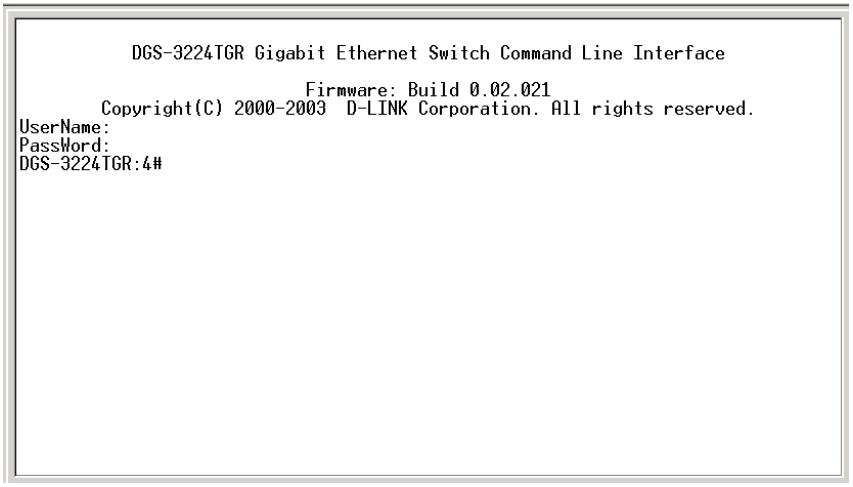

Figure 2-1. Initial Console Screen

Commands are entered at the command prompt, **DGS-3224TGR:4#.**

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.

Figure 2-2. The ? Command

The **dir** command has the same function as the **?** command.

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

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 you 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.

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.

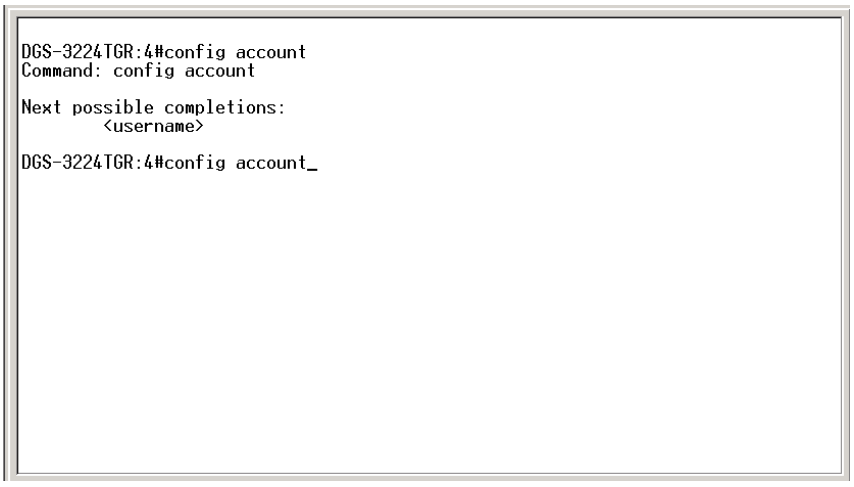

Figure 2-4. Using the Up Arrow to Re-enter a Command

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 User name 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.

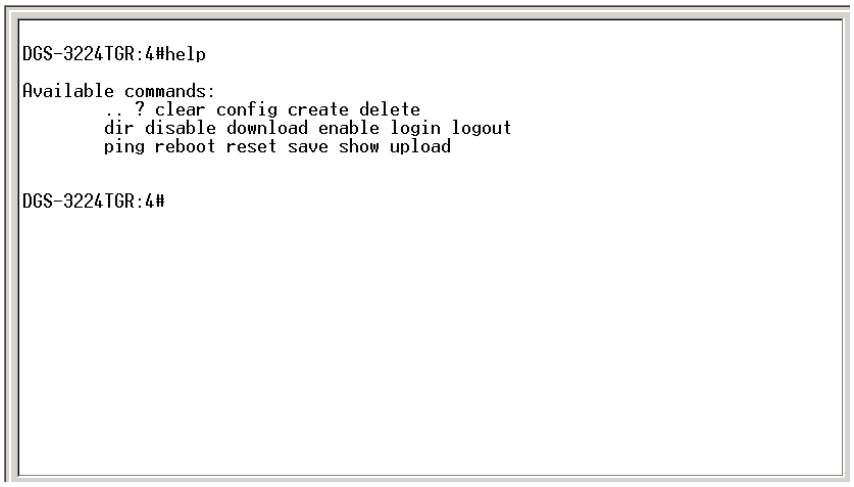

Figure 2-5. The Available Commands Prompt

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

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

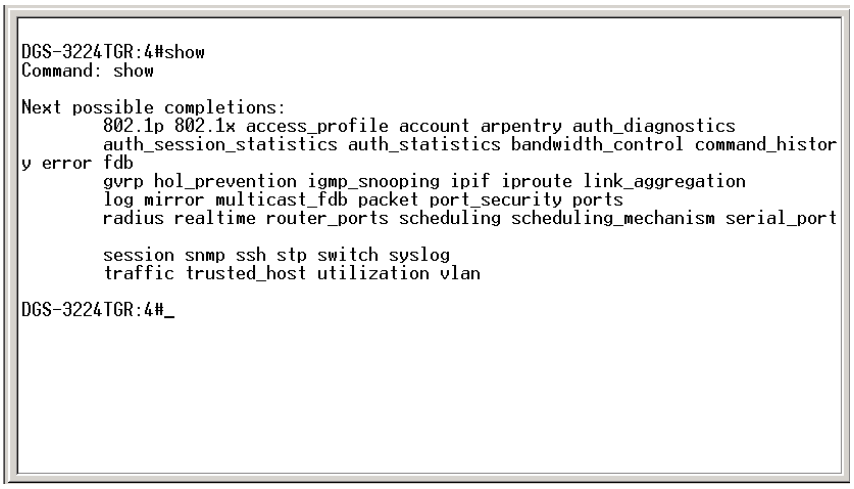

Figure 2-6. Next possible completions: Show Command

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 in this manual 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.

<angle brackets>	
Purpose	Encloses a variable or value that must be specified.
Example Syntax	**config ipif System ipaddress <network_address>**
Description	In the above syntax example, you must supply the network address in the <network_address> space. Do not type the angle brackets.
Example Command	**config ipif System ipaddress 10.24.22.9/255.0.0.0**

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

| vertical bar	
Purpose	Separates two or more mutually exclusive items in a list – one of which must be entered.
Example Syntax	**show snmp [community|trap receiver|detail]**
Description	In the above syntax example, you must specify either **community, trap receiver,** or **detail**. Do not type the vertical bar.
Example Command	**show snmp community**

{braces}	
Purpose	Encloses an optional value or set of optional arguments.
Example Syntax	**config igmp [<ipif_name>|all] {version <value>|query_interval <sec>|max_response_time <sec>| robustness_variable <value>|last_member_query_interval <value>|state [enabled|disabled]}**
Description	In the above syntax example, you must choose to enter an IP interface name in the **<ipif_name>** space or **all,** but **version <value>, query_interval <sec>, max_response_time <sec>, robustness_variable <value>, last_member_query_interval <value>, and state [enabled|disabled]** are all optional arguments. You can specify any or all of the arguments contained by braces. Do not type the braces.
Example command	**config igmp all version 2**

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

Line Editing Key Usage	
	line to the left**.**
Insert	Can be toggled on or off. When toggled on, inserts text at the current cursor position and shifts the remainder of the line to the left.
Left Arrow	Moves the cursor to the left.
Right Arrow	Moves the cursor to the right.
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 displaying.
a	Displays the remaining pages without pausing between pages.

Line Editing Key Usage	
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|user] <username 15>
config account	<username>
show account	
delete account	<username>
show session	
show switch	
show serial_port	
config serial_port	{baud_rate [9600|19200|38400|115200] auto_logout(2) [never(0)|2_minutes(2)|5_minutes(5) |10_minutes(10)|15_minutes(15)]}(1)
enable jumbo_frame	
disable jumbo_frame	

Command	Parameters
show jumbo_frame	
enable clipaging	
disable clipaging	
enable telnet	{<tcp_port_number 1-65535>}
disable telnet	
enable web	{<tcp_port_number 1-65535>}
disable web	
save	
reboot	
reset	{config|system}
login	
logout	
config realtime date	<date ddmthyyyy> <time hour:min:sec>
show realtime	

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

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

create account	
Parameters	Admin <username> User <username>
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-3224TGR:4#create account admin dlink
Command: create account admin dlink

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

DGS-3224TGR:4#
```

config account	
Purpose	Used to configure user accounts

config account

Syntax	**config account <username>**
Description	The config account command configures a user account that has been created using the **create account** command.
Parameters	<username>
Restrictions	Only Administrator-level users can issue this command. Usernames can be between 1 and 15 characters. Passwords can be between 0 15 characters.

Example Usage:

To configure the user password of "dlink" account:

```
DGS-3224TGR:4#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-3224TGR:4#
```

show account

show account

Purpose	Used to display user accounts
Syntax	**show account**
Description	Displays all user accounts created on the switch. Up to eight user accounts can exist on the switch at one time.
Parameters	None.
Restrictions	None.

Example Usage:

To display the accounts that have been created:

```
DGS-3224TGR:4#show account
Command: show account

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

DGS-3224TGR:4#
```

delete account

Purpose	Used to delete an existing user account
Syntax	**delete account <username>**

delete account

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

Example Usage:

To delete the user account "System":

```
DGS-3224TGR:4#delete account System
Command: delete account System

Success.

DGS-3224TGR:4#
```

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

show session

Restrictions	None.

Example Usage:

To display the way that the users logged in:

```
DGS-3224TGR:4#show session

ID   Login Time          Live Time           From          Level   Name
---  ------------------- ------------------- ------------- ------- ----------------
8    2003/10/01 15:13:40  00:17:27           Serial Port   4       Anonymous
8    2003/10/01 15:13:40  00:17:29           Serial Port   4       Anonymous
8    2003/10/01 15:13:40  00:17:31           Serial Port   4       Anonymous
8    2003/10/01 15:13:40  00:17:35           Serial Port   4       Anonymous
```

show switch

Purpose	Used to display 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 information:

```
DGS-3224TGR:4#show switch
Command: show switch

Device Type            : DGS-3224TGR Gigabit-Ethernet Switch
MAC Address            : 00-01-02-03-04-00
IP Address             : 10.90.90.90 (Manual)
VLAN Name              : default
Subnet Mask            : 255.0.0.0
Default Gateway        : 0.0.0.0
Boot PROM Version      : Build 0.01.004
Firmware Version       : Build 0.03.005
Hardware Version       : 2A1
System Name            :
System Location        :
System Contact         :
Spanning Tree          : Disabled
GVRP                   : Disabled
IGMP Snooping          : Disabled
TELNET                 : Enabled(TCP  23)
SSH                    : Enabled(TCP 22)
WEB                    : Enabled(TCP  80)
RMON                   : Disabled
RPS State              : Disabled

DGS-3224TGR:4#
```

show serial_port

Purpose	Used to display the current serial port settings.

show 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-3224TGR:4#show serial_port
Command: show serial_port

Baud Rate     : 9600
Data Bits     : 8
Parity Bits   : None
Stop Bits     : 1
Auto-Logout   : 10 mins

DGS-3224TGR:4#
```

config serial_port

Purpose	Used to configure the serial port.
Syntax	**config serial_port {baud_rate[9600|19200|38400|115200]|auto_logout**

config serial_port	
	[never|2_minutes|5_minutes|10_minutes|15_minutes]}
Description	This command is used to configure the serial port's baud rate and auto logout settings.
Parameters	[9600|19200|38400|115200] – The serial bit rate that will be used to communicate with the management host. 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-level users can issue this command.

Example Usage:

To configure baud rate:

```
DGS-3224TGR:4#config serial_port baud_rate 9600
Command: config serial_port baud_rate 9600

Success.

DGS-3224TGR:4#
```

enable jumbo_frame

Purpose	Used to enable support for Jumbo Frames.
Syntax	**enable jumbo_frame**
Description	This command is used to enable support for Jumbo Frames up to 9216 bytes.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To enable jumbo frame support on the switch:

```
DGS-3224TGR:4#enable jumbo_frame
Command: enable jumbo_frame

Success.

DGS-3224TGR:4#
```

disable jumbo_frame	
Purpose	Used to disable support for Jumbo Frames.
Syntax	**disable jumbo_frame**
Description	This command is used to disable support for Jumbo Frames of up to 9216 bytes.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To disable jumbo frame support on the switch:

```
DGS-3224TGR:4#disable jumbo_frame
Command: disable jumbo_frame

Success.

DGS-3224TGR:4#
```

show jumbo_frame	
Purpose	Used to display whether support for Jumbo Frames is currently enabled.
Syntax	**show jumbo_frame**
Description	This command is used to display whether support for Jumbo Frames of up to 9216

show jumbo_frame	
	bytes is enabled.
Parameters	None.
Restrictions	None.

Example Usage:

To display jumbo frame support on the switch:

```
DGS-3224TGR:4#show jumbo_frame
Command: show jumbo_frame

On.

DGS-3224TGR:4#
```

enable clipaging	
Purpose	Used to pause the scrolling of the console screen when the show command displays more than one page.
Syntax	**enable clipaging**
Description	This command is used when issuing the show command will cause 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.

enable clipaging

Restrictions	Only administrator-level users can issue this command.

Example Usage:

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

```
DGS-3224TGR:4#enable clipaging
Command: enable clipaging

Success.

DGS-3224TGR:4#
```

disable clipaging

Purpose	Used to disable the pausing of the console screen scrolling at the end of each page when the show command would display more than one screen of information.
Syntax	**disable clipaging**
Description	This command is used to disable the pausing of the console screen at the end of each page when the show command would display more than one screen of information.
Parameters	None.

disable clipaging

Restrictions	Only administrator-level users can issue this command.

Example Usage:

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

```
DGS-3224TGR:4#disable clipaging
Command: disable clipaging

Success.

DGS-3224TGR:4#
```

enable telnet

Purpose	Used to enable communication with and management of the switch using the Telnet protocol.
Syntax	**enable telnet <tcp_port_number>**
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> – the TCP port number. TCP ports are numbered between 1 and 65535. The "well-known" TCP port

enable telnet	
	for the Telnet protocol is 23.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To enable Telnet and configure port number:

```
DGS-3224TGR:4#enable telnet 23
Command: enable telnet 23

Success.

DGS-3224TGR:4#
```

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-level users can issue this command.

Example Usage:

To disable the Telnet protocol on the switch:

```
DGS-3224TGR:4#disable telnet
Command: disable telnet

Success.

DGS-3224TGR:4#
```

enable web

Purpose	Used to enable the HTTP-based management software on the switch.
Syntax	**enable web <tcp_port_number>**
Description	This command is used to enable the Web-based management software on the switch. The user can specify the TCP port number the switch will use to listen for Telnet requests.
Parameters	<tcp_port_number> – The TCP port number. TCP ports are numbered between 1 and 65,535. The "well-known" port for the Web-based management software is 80.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To enable HTTP and configure port number:

```
DGS-3224TGR:4#enable web 80
Command: enable web 80

Success.

DGS-3224TGR:4#
```

disable web

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

Example Usage:

To disable HTTP:

```
DGS-3224TGR:4#disable web
Command: disable web

Success.

DGS-3224TGR:4#
```

save	
Purpose	Used to save changes in the switch's configuration to non-volatile RAM.
Syntax	**save**
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	None.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

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

```
DGS-3224TGR:4#save
Command: save

Saving all settings to NV-RAM... 100%
done.
DGS-3224TGR:4#
```

reboot	
Purpose	Used to restart the switch.

reboot	
Syntax	**reboot**
Description	This command is used to restart the switch.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To restart the switch:

```
DGS-3224TGR:4#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**}
Description	This command is used to restore the switch's configuration to the default settings assigned from the factory.

reset	
Parameters	config – If config is specified, all of the factory default settings are restored on the switch except for the IP address, user accounts, and the switch history log. system – If system is specified all of the factory default settings are restored on the switch. If no parameter is specified, the switch's current IP address, user accounts, and switch history log are retained. All other parameters are restored to their factory default settings.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

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

```
DGS-3224TGR:4#reset config
Command: reset config

Success.

DGS-3224TGR:4#
```

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 his Username and Password.
Parameters	None.
Restrictions	None.

Example Usage:

To initiate the login procedure:

```
DGS-3224TGR:4#login
Command: login

UserName:
```

logout	
Purpose	Used to log out a user from the switch's console.
Syntax	**logout**
Description	This command terminates the current user's session on the switch's console.

logout	
Parameters	None.
Restrictions	None.

Example Usage:

To terminate the current user's console session:

```
DGS-3224TGR:4#logout
```

config realtime date	
Purpose	Used to configure the date and time on the switch.
Syntax	**config realtime date <date ddmthyyyy> <time hour:min:sec>**
Description	This command is used to set the date and time on the switch.
Parameters	<date ddmthyyyy> – Use this format for setting the date. <time hour:min:sec> – Use this format for setting the time.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To configure the date:

```
DGS-3224TGR:4#config realtime date 23sep2003 10:59:30
Command: config realtime date 23sep2003 10:59:30

Success.

DGS-3224TGR:4#
```

show realtime

Purpose	Used to display the date and time on the switch.
Syntax	**show realtime**
Description	This command is used to display the date and time on the switch.
Parameters	None.
Restrictions	None.

Example Usage:

To display the date:

```
DGS-3224TGR:4#show realtime
Command: show realtime

The current time   :  2003/09/23  11:00:59

DGS-3224TGR:4#
```

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>] {speed [auto | 10_half | 10_full | 100_half | 100_full | 1000_full {[master | slave]} flow_control [enable | disable] learning [enable | disable] state [enable | disable]}
show ports	<portlist>

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>] {speed [auto | 10_half | 10_full | 100_half | 100_full | 1000_full {[master | slave]}] | flow_control [enable | disable] learning [enable | disable] state [enable | disable]}**
Description	This command allows for the configuration of the switch's Ethernet ports. Only the ports listed in the <portlist> will be effected.
Parameters	all – Displays all ports on the switch. portlist – Specifies a range of ports to be configured. The port list is specified by listing the beginning port number and the highest port number of the range. The beginning and end of the port list range are separated by a dash. For example, 3 would specify port 3. 4 specifies port 4. 3-4 specifies all of the ports between port 3 and port 4 – in numerical order. auto – Enables auto-negotiation for the specified range of ports. [10|100|1000] – Configures the speed in Mbps for the specified range of ports. Gigabit ports are statically set to 1000 and cannot be set to slower speeds. [half|full] – Configures the specified range of

config ports	
	ports as either full- or half-duplex. master | slave – The *master* and *slave* parameters refer to connections running a 1000BASE-T cable for connection between the switch port and another device capable of a gigabit connection. If one connection is set for *1000 master*, the other side of the connection must be set for *1000 slave,* for devices with the *master/slave* capability. For connection to a device without this capability, the port speed must be set to *1000_full*. Any other configuration will result in a link down status for both ports. flow_control [enable|disable] – Enables or disables flow control for the specified range of 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.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

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

```
DGS-3224TGR:4#config ports 1-3 speed 10_full learning enable state enable

Command: config ports 1-3 speed 10_full learning enable state enable

Success.
```

show ports

Purpose	Used to display the current configuration of a range of ports.
Syntax	**show ports** {**<portlist>**}
Description	This command is used to display the current configuration of a range of ports.
Parameters	<portlist> – Specifies a range of ports to be configured. The port list is specified by listing the beginning port number and the highest port number of the range. The beginning and end of the port list range are separated by a dash. For example, 3 would specify port 3. 4 specifies port 4. 3-4 specifies all of the ports between port 3 and port 4 – in numerical order.
Restrictions	None.

Example Usage:

To display the configuration of the ports 1-7:

```
DGS-3224TGR:4#show ports 1-7

Port  Port        Settings              Connection              Address
      State   Speed|Duplex|FlowCtrl  Speed|Duplex|FlowCtrl   Learning
----  --------  --------------------  --------------------    --------
1     Enabled       Auto|Disabled        Link Down            Enabled
2     Enabled       Auto|Disabled        Link Down            Enabled
3     Enabled       Auto|Disabled        Link Down            Enabled
4     Enabled       Auto|Disabled        Link Down            Enabled
5     Enabled       Auto|Disabled        Link Down            Enabled
6     Enabled       Auto|Disabled        Link Down            Enabled
7     Enabled       Auto|Disabled        Link Down            Enabled
```

6

NETWORK MANAGEMENT COMMANDS

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

Command	Parameters
create snmp community	<community_string 33> view <view_name> [read_only|read_write]
delete snmp community	<community_string>
enable rmon	
disable rmon	
config snmp system_contact	<sw_contact>
enable snmp traps	
disable snmp traps	
enable snmp authenticate traps	
disable snmp authenticate traps	
show	<ipaddr>

Command	Parameters
trusted_hosts	
ping	<ipaddr> times <value> timeout <sec>
create snmp user	<username 32> <groupname 32> {encrypted(1) [by_password auth [md5 <auth_password 8-16> | sha(3) <auth_password 8-20>] priv [none| des <priv_password 8-16>] | by_key auth [md5 <auth_key 32-32> | sha(3) <auth_key 40-40>] priv [none| des <priv_key 32-32>]]}
delete snmp user	<username 32>
create snmp view	<view_name 32> [all | <oid>]
delete snmp view	<view_name 32> <oid> view_type[included(1 | excluded)
create snmp view	<view_view 32> [all | <oid>]
config snmp engineID	<snmp_engineID 10-64>
create snmp group	<groupname 32> [v1 | v2c | v3 [noauth_nopriv | auth_nopriv| auth_priv]] {read_view <view_name 32> | write_view <view_name 32> | notify_view <view_name 32>}
delete snmp group	<goupname 32>
create snmp host	<ipaddr> [v1 | v2c |v3 [noauth_nopriv | auth_nopriv | auth_priv]] <auth_string 32>
delete snmp host	<ipaddr>
show snmp engineID	
show snmp groups	
show snmp user	

Command	Parameters
show snmp view	{<view_name 32>}
show snmp community	{<community_string 33>}
show snmp host	{ipaddr>}
show snmp traps	
create trusted_host	<ipaddr>
delete trusted_host	<ipaddr>
config snmp system_name	<sw_name>
config snmp system_location	<sw_location>

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

create snmp community	
Purpose	Used to create an SNMP community string.
Syntax	**create snmp community <community_string 33> view <view_name> [read_only|read_write]**
Description	This command is used to create an SNMP community string and to specify the string as enabling read only or read-write privileges for the SNMP management host.
Parameters	<community_string 33> – An alphanumeric string of up to 33 characters used to authentication of users wanting access to

create snmp community	
	the switch's SNMP agent. <view_name> – An alphanumeric string of up to 32 characters that identifies the SNMP view that will be created. read_only – Allows the user using the above community string to have read only access to the switch's SNMP agent. The default read only community string is public. read_write – Allows the user using the above community string to have read and write acces to the switch's SNMP agent. The default read write community string is private.
Restrictions	Only administrator-level users can issue this command. A maximum of four community strings can be specified.

Example Usage:

To create a read-only level SNMP community "System":

```
DGS-3224TGR:4#create snmp community System
readwrite
Command: create snmp community System readwrite

 Success.

DGS-3224TGR:4#
```

delete snmp community	
Purpose	Used to delete an SNMP community string previously entered on the switch.
Syntax	**delete snmp community <community_string 33>**
Description	This command is used to delete an SNMP community string entered on the switch using the create snmp community command above.
Parameters	<community_string 33> – An alphanumeric string of up to 32 characters used to authentication of users wanting access to the switch's SNMP agent.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To delete a read-only level SNMP community "System":

```
DGS-3224TGR:4#delete snmp community System
Command: delete snmp community System

Success.

DGS-3224TGR:4#
```

delete trusted_host

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

Example Usage:

To delete a trusted host with an IP address 10.48.74.121:

```
DGS-3224TGR:4#delete trusted_host 10.48.74.121
Command: delete trusted_host 10.48.74.121

Success.

DGS-3224TGR:4#
```

config snmp system_name

config snmp system_name	
Purpose	Used to configure a name for the switch.
Syntax	**config snmp system_name <sw_name>**
Description	This command is used to give the switch an alpha-numeric name of up to 128 characters.
Parameters	<sw_name> – An alpha-numeric name for the switch of up to 128 characters.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To configure the switch name for "DGS3224TGR":

.

```
DGS-3224TGR:4#config snmp system_name
DGS3224TGR
Command: config snmp system_name DGS3224TGR

Success.

DGS-3224TGR:4#
```

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

config snmp system_location	
	<sw_location>
Description	This command is used to enter a description of the location of the switch. A maximum of 128 characters can be used.
Parameters	<sw_location> – A description of the location of the switch. A maximum of 128 characters can be used.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To configure the switch location for "Timbuktu":

.

```
DGS-3224TGR:4#config snmp system_location
Timbuktu
Command: config snmp system_location Timbuktu

Success.

DGS-3224TGR:4#
```

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>**

config snmp system_contac :	
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 128 character can be used.
Parameters	<sw_contact> – A maximum of 128 characters used to identify a contact person who is responsible for the switch.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To configure the switch contact to "dlink":

.

```
DGS-3224TGR:4#config snmp system_contact dlink
Command: config snmp system_contact dlink

Success.

DGS-3224TGR:4#
```

enable rmon	
Purpose	Used to enable RMON on the switch.
Syntax	**enable rmon**
Description	This command is used, in conjunction with the disable rmon command below, to

enable rmon	
	enable and disable remote monitoring (RMON) on the switch.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To enable RMON:

```
DGS-3224TGR:4#enable rmon
Command: enable rmon

Success.

DGS-3224TGR:4#
```

disable rmon	
Purpose	Used to disable RMON on the switch.
Syntax	**disable rmon**
Description	This command is used, in conjunction with the enable rmon command above, to enable and disable remote monitoring (RMON) on the switch.
Parameters	None.

disable rmon

Restrictions	Only administrator-level users can issue this command.

Example Usage:

To disable RMON:

```
DGS-3224TGR:4#disable rmon
Command: disable rmon

Success.

DGS-3224TGR:4#
```

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**
Description	This command is used to display a list of trusted hosts entered on the switch using the create trusted_host command above.
Parameters	None.

show trusted_host

Restrictions	None.

Example Usage:

To display the list of trust hosts:

```
DGS-3224TGR:4#show trusted_host
Command: show trusted_host

 Management Station IP Addresses:
 IP Address: 10.48.74.121  Port: 23
 IP Address: 10.48.75.100  Port: 23
 IP Address: 10.48.69.23   Port: 21

DGS-3224TGR:4#
```

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-level users can issue this command.

Example Usage:

To turn on SNMP trap support:

```
DGS-3224TGR:4#enable snmp traps
Command: enable snmp traps

Success.

DGS-3224TGR:4#
```

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

Example Usage:

To prevent SNMP traps from being sent from the switch:

```
DGS-3224TGR:4#disable snmp traps
Command: disable snmp traps

Success.

DGS-3224TGR:4#
```

enable snmp authenticate t 'aps	
Purpose	Used to enable SNMP authentication trap support.
Syntax	**enable snmp authenticate traps**

enable snmp authenticate traps	
Description	This command is used to enable SNMP authentication trap support on the switch.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To turn on SNMP authentication trap support:

```
DGS-3224TGR:4#enable snmp authenticate traps
Command: enable snmp authenticate traps

Success.

DGS-3224TGR:4#
```

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

disable snmp authenticate traps	
	this command.

Example Usage:

To turn off SNMP authentication trap support:

```
DGS-3224TGR:4#disable snmp authenticate traps
Command: disable snmp authenticate traps

 Success.

DGS-3224TGR:4#
```

ping	
Purpose	Used to test the connectivity between network devices.
Syntax	**ping <ipaddr> {times <value>} {timeout <sec>}**
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> – The IP address of the remote device. times <value> – The number of individual

ping	
	ICMP echo messages to be sent. A value of 0 will send an infinite ICMP echo messages. The maximum value is 255. The default is 0. timeout <sec> – 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	Only administrator-level users can issue this command.

Example Usage:

To send ICMP echo message to "10.48.74.121" for 4 times:

```
DGS-3224TGR:4#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-3224TGR:4#
```

7

DOWNLOAD/UPLOAD COMMANDS

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

Command	Parameters
download	firmware <ipaddr> <path_filename> configuration <ipaddr> <path_filename> {increment}
upload	configuration log <ipaddr> <path_filename>

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

download	
Purpose	Used to download and install new firmware or a switch configuration file from a TFTP server.
Syntax	**download [firmware <ipaddr> <path_filename> |configuration <ipaddr> <path_filename> {increment}]**
Description	This command is used to download a new firmware or a switch configuration file from a TFTP server.
Parameters	firmware – Download and install new firmware on the switch from a TFTP server. configuration – Download a switch configuration file from a TFTP server. <ipaddr> – The IP address of the TFTP server. <path_filename> – The DOS path and filename of the firmware or switch configuration file on the TFTP server. For example, C:\3224tgr.had. increment – Allows the download of a partial switch configuration file. This allows a file to be downloaded that will change only the switch parameters explicitly stated in the configuration file. All other switch parameters will remain unchanged.
Restrictions	The TFTP server must be on the same IP subnet as the switch. Only administrator-

download	
	level users can issue this command.

Example Usage:

```
DGS-3224TGR:4#download configuration 10.48.74.121
c:\cfg\setting.txt
Command: download configuration 10.48.74.121
c:\cfg\setting.txt

 Connecting to server..... Done.
 Download configuration..... Done.
DGS-3224TGR:4#
```

upload	
Purpose	Used to upload the current switch settings or the switch history log to a TFTP server.
Syntax	**upload [configuration|log] <ipaddr> <path_filename>**
Description	This command is used to upload either the switch's current settings or the switch's history log to a TFTP server.
Parameters	configuration – Specifies that the switch's current settings will be uploaded to the TFTP server. log – Specifies that the switch history log will be uploaded to the TFTP server.

upload	
	<ipaddr> – The IP address of the TFTP server. The TFTP server must be on the same IP subnet as the switch. <path_filename> – Specifies the location of the switch configuration file on the TFTP server. This file will be replaced by the uploaded file from the switch.
Restrictions	The TFTP server must be on the same IP subnet as the switch. Only administrator-level users can issue this command.

Example Usage:

To upload a configuration file:

```
DGS-3224TGR:4#upload configuration 10.48.74.121
c:\cfg\log.txt
Command: upload configuration 10.48.74.121
c:\cfg\log.txt

 Connecting to server..... Done.
 Upload configuration.....Done.
DGS-3224TGR:4#
```

8

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 utilitzation	
clear counters	ports <portlist>
clear log	
show log	index <value>
enable syslog	
disable syslog	
show syslog	
config syslog	{host(1) [all|<index 1-4>]}(1) { severity(2) [informational(21)|local1(22)|local2(23)|local3(24)|local4(25)|local5(26)|local6(27)|local7(28)] |udp_port(3) <int> | ipaddress(4) <ipaddr> |

Command	Parameters
	state(5) [enabled(51)|disabled(52)]}
delete syslog host	[<index 1-4> |all]
show syslog host	[index 1-4>]

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 port list.
Parameters	<portlist> – specifies a range of ports to be configured. The port list is specified by listing the beginning port number and the highest port number of the range. The beginning and end of the port list range are separated by a dash. For example, 3 would specify port 3. 4 specifies port 4. 3-4 specifies all of the ports between port 3 and port 4 – in numerical order.
Restrictions	None.

Example Usage:

To display the packets analysis for port 7:

```
DGS-3224TGR:4# show packet port 7

Port number : 7
Frame Size    Frame Counts  Frames|sec    Frame Type    Total    Total|sec
------------  ------------  ----------  ----------  -------  ---------
64            3275          10          RX Bytes    408973   1657
65-127        755           10          RX Frames   4395     19
128-255       316           1
256-511       145           0           TX Bytes    7918     178
512-1023      15            0           TX Frames   111      2
1024-1518     0             0
Unicast RX    152           1
Multicast RX  557           2
Broadcast RX  3686          16

Broadcast RX  4495          42
```

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 swtich for a given port list.
Parameters	<portlist> – Specifies a range of ports to be configured. The port list is specified by listing the beginning port number and the

show error ports

	highest port number of the range. The beginning and end of the port list range are separated by a dash. For example, 3 would specify port 3. 4 specifies port 4. 3-4 specifies all of the ports between port 3 and port 4 – in numerical order.
Restrictions	None.

Example Usage:

To display the errors of the port 3:

```
DGS-3224TGR:4# show errors port 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 Collission     0
Drop Pkts       0          Collision             0
```

show utilization

Purpose	Used to display real-time port utilization statistics.
Syntax	**show utilization**

show utilization

Description	This command will display the real-time port utilitization statistics for the switch.
Parameters	None.
Restrictions	None.

Example Usage:

To display the port utilization statistics:

```
DGS-3224TGR:4# show utilization

Port   TX|sec      RX|sec      Util    Port   TX|sec      RX|sec      Util
----   ---------- ---------- ----    ----   ---------- ---------- ----
1      0          0          0       22     0          0          0
2      0          0          0       23     0          0          0
3      0          0          0       24     0          0          0
4      0          0          0
5      0          0          0
6      0          0          0
7      0          0          0
8      0          0          0
9      0          0          0
10     0          0          0
11     0          0          0
12     0          0          0
13     0          0          0
14     0          0          0
15     0          0          0
16     0          0          0
17     0          0          0
18     0          0          0
```

```
 19        0        0        0
 20        0        0        0
 21        0        0        0
```

clear counters

Purpose	Used to clear the switch's statistics counters.
Syntax	**clear counters** {**ports <portlist>**}
Description	This command will clear the counters used by the switch to compile statistics.
Parameters	<portlist> – Specifies a range of ports to be configured. The port list is specified by listing the beginning port number and the highest port number of the range. The beginning and end of the port list range are separated by a dash. For example, 3 would specify port 3. 4 specifies port 4. 3-4 specifies all of the ports between port 3 and port 4 – in numerical order.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To clear the counters:

```
DGS-3224TGR:4#clear counters ports 7-9
Command: clear counters ports 7-9
```

```
Success.

DGS-3224TGR:4#
```

clear log

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

Example Usage:

To clear the log information:

```
DGS-3224TGR:4#clear log
Command: clear log

 Success.

DGS-3224TGR:4#
```

show log

Purpose	Used to display the switch history log.

show log

Syntax	**show log {index <value>}**
Description	This command will display the contents of the switch's history log.
Parameters	index <value> – The show log command will display the history log until the log number reaches this value.
Restrictions	None.

Example Usage:

To display the switch history log:

```
DGS-3224TGR:4# show log

Index   Time                  Log Text
-----   ----------            --------------------------------------------------------------------------------
8       2003/09/18  09:03:45  Successful login through Console (Username:
Anonymous)
7       2003/09/18  09:03:30  Logout through Console (Username: Anonymous)
6       2003/09/18  09:03:28  Successful login through Console (Username:
Anonymous)
5       2003/09/18  09:03:26  System started up
4       2003/09/18  16:13:39  Port 1 link down
3       2003/09/18  16:13:38  System started up
2       2003/09/18  16:13:36  Spanning Tree Protocol is disabled
1       2003/09/18  16:13:35  Port 9 link up, 100Mbps FULL duplex

DGS-3224TGR:4#
```

9

SPANNING TREE COMMANDS

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

Command	Parameters
config stp	{maxage <value 6-40>| hellotime <value 1-10>| forwarddelay <value 4-30>| priority <value 0-61440>| version [rstp|stp] | txholdcount <value 1-10>| fbpdu [enable|disable]}
config stp ports	<portlist> {cost [auto| <value 1-200000000>| priority <value 0-240>| migrate [yes|no] | edge [true|false] | p2p [true|false|auto] | state [enable|disable]
enable stp	
disable stp	
show stp	
show stp ports	<portlist>

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

config stp	
Purpose	Used to configure Bridge management parameters for STP on the switch.
Syntax	config stp {maxage <value 6-40>|hellotime <value 1-10> |forwarddelay <value 4-30>|priority <value 0-61440>|version [rstp|stp] |txholdcount <value 1-10>|fbpdu [enabled|disabled]}
Description	This command is used to setup the Spanning Tree Protocol (STP) for the entire switch.
Parameters	maxage <value 6-40> – The maximum amount of time (in seconds) that the switch will wait to receive a BPDU packet before reconfiguring STP. The default is 20 seconds. hellotime <value 1-10> – The time interval between transmission of configuration messages by the root device. The default is 2 seconds. forwarddelay <value 4-30> – The maximum amount of time (in seconds) that the root device will wait before changing states. The default is 15 seconds. priority <value 0-61440> – A numerical value between 0 and 61,440 that is used in determining the root device, root port, and designated port. The device with the highest priority becomes the root device.

config stp	
	The lower the numerical value, the higher the priority. The default is 32,768. version [rstp|stp] – Allows the selection of either Rapid Spanning Tree or regular STP. fbpdu [enabled|disabled] – Allows the forwarding of STP BPDU packets from other network devices when STP is disabled on the switch. The default is enabled.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To set maxage to 18 and hellotime to 4:

```
DGS-3224TGR:4#config stp maxage 18 hellotime 4
Command: config stp maxage 18 hellotime 4

Success.

DGS-3224TGR:4#
```

config stp ports	
Purpose	Used to setup STP on the port level.
Syntax	**config stp ports <portlist> {cost [auto|<value 1-200000000>]|priority <value 0-240>|migrate [yes|no] | edge [true|false]|p2p [true|false|auto]|state**

config stp ports	
	[enable|disable]
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 beginning port number and the highest port number of the range. The beginning and end of the port list range are separated by a dash. For example, 3 would specify port 3. 4 specifies port 4. 3-4 specifies all of the ports between port 3 and port 4 – in numerical order. cost [auto|<value 1-200000000>] – This defines a metric that indicates the relative cost of forwarding packets to the specified port list. The default cost for a 1000 Mbps port is 20,000, a 100 Mbps port is 200,000, and for a 10 Mbps port the default cost is 2,000,000. priority <value 0-240> – A numeric value between 0 and 240 that is used in determining the root and designated port in an STP port list. The default is 128, with 0 indicating the highest priority. migrate [yes|no] – yes will enable the port to migrate from 802.1d STP status to 802.1w RSTP status. RSTP can coexist with standard STP, however the benefits of RSTP are not realized on a port where an 802.1d network connects to an 802.1w enabled network. Migration should be enabled (yes)

config stp ports	
	on ports connected to network stations or segments that will be upgraded to 802.1w RSTP on all or some portion of the segment. edge [true|false] – true designates the port as an edge port. Edge ports cannot create loops, however an edge port can lose edge port status if a topology change creates a potential for a loop. An edge port normally should not receive BPDU packets. If a BPDU packet is received it automatically loses edge port status. False indicates the port does not have edge port status. p2p [true|false|auto] – The administrative point-to-point status of the LAN segment attached to this port. A value of true indicates that this port should always be treated as if it is connected to a point-to-point link. A value of false indicates that this port should be treated as having a shared media connection. A value of auto indicates that this port is considered to have a p2p link if it is an aggregator and all of its members are aggregatable, or if the MAC entity is configured for full duplex operation, either through auto-negotiation or by management means. state [enable|disable] – Allows STP to be enabled or disabled for the ports specified in the port list. The default is disabled.
Restrictions	Only administrator-level users can issue this command.

config stp ports	
	this command.

Example Usage:

To set the path cost 19, the priority 15, and the state enabled of the ports 1-5:

```
DGS-3224TGR:4#config stp ports 1-5 cost 19 priority 15 state enabled
Command: config stp ports 1-5 cost 19 priority 15 state enabled

Success.

DGS-3224TGR:4#
```

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

Example Usage:

To enable STP on the switch:

```
DGS-3224TGR:4#enable stp
Command: enable stp

Success.

DGS-3224TGR:4#
```

disable stp

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

Example Usage:

To disable STP on the switch:

```
DGS-3224TGR:4#disable stp
Command: disable stp

Success.

DGS-3224TGR:4#
```

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:

Status 1: STP enabled

```
DGS-3224TGR:4#show stp
Command: show stp

STP Status                : Enabled
Max Age                   : 20
Hello Time                : 2
Forward Delay             : 15
Priority                  : 32768
Default Path Cost         : 802.1T
STP Version               : RSTP
TX Hold Count             : 3
Forwarding BPDU           : Enabled

 Designated Root Bridge   : 00-00-00-12-00-00
 Root Priority            : 32768
 Cost to Root             : 19
 Root Port                : 33
```

```
Last Topology Change      : 13sec
Topology Changes Count    : 0
Protocol Specification    : 3
Max Age                   : 20
Hello Time                : 2
Forward Delay             : 15
Hold Time                 : 3
```

Status 2: STP disabled

```
DGS-3224TGR:4#show stp
Command: show stp

STP Status                : Disabled
Max Age                   : 18
Hello Time                : 4
Forward Delay             : 15
Priority                  : 32768
Default Path Cost         : 802.1T
STP Version               : RSTP
TX Hold Count             : 3
Forwarding BPDU           : Enabled

DGS-3224TGR:4#
```

show stp ports

Purpose	Used to display the switch's current per-port group STP configuration.
Syntax	**show stp ports <portlist>**
Description	This command displays the switch's current per-port group STP configuration.

show stp ports

Parameters	<portlist> – Specifies a range of ports to be configured. The port list is specified by listing the beginning port number and the highest port number of the range. The beginning and end of the port list range are separated by a dash. For example, 3 would specify port 3. 4 specifies port 4. 3-4 specifies all of the ports between port 3 and port 4 – in numerical order.
Restrictions	None

Example Usage:

To display STP state of port 1-2:

```
DGS-3224TGR:4#show stp ports 1-2

Port  Connection       State    Cost   Pri  Edge  P2P   Status      Role
----  ---------------  -------- ----  -----  -----  ------  ---------  ------------
1     100M/Full/None   Yes *200000  128  No    Yes  Forwarding  NonStp
2     Link Down        Yes *200000  128  No    Yes  Disabled    Disabled
```

10

LAYER 2 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> <macaddr> port <port>
create multicast_fdb	<vlan_name> <macaddr>
config multicast_fdb	<vlan_name> <macaddr> [add|delete] <portlist>
delete fdb	<vlan_name> <macaddr> [add|delete] <portlist>
clear fdb	vlan <vlan_name> port <port>|all
show multicast_fdb	vlan <vlan_name> mac_address <macaddr>
show fdb	port <port>

Command	Parameters
	vlan <vlan_name> mac_address <macaddr> static aging_time
config fdb aging_time	<sec 10-1000000>

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> <macaddr> [port <port>]**
Description	This command will make an entry into the switch's unicast MAC address forwarding database.
Parameters	<vlan_name> – The name of the VLAN on which the MAC address resides. <macaddr> – The MAC address that will be added to the forwarding table. <port> – The port number corresponding to the MAC destination address. The switch will always forward traffic to the specified device through this port.

create fdb	
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To create an unicast MAC forwarding:

```
DGS-3224TGR:4#create fdb default 00-00-00-00-01-02
port 5
Command: create fdb default 00-00-00-00-01-02 port 5

Success.
```

create multicast_fdb	
Purpose	Used to create a static entry to the multicast MAC address forwarding table (database)
Syntax	**create multicast_fdb <vlan_name> <macaddr>**
Description	This command will make an entry into the switch's multicast MAC address forwarding database.
Parameters	<vlan_name> – The name of the VLAN on which the MAC address resides. <macaddr> – The MAC address that will be

create multicast_fdb	
	added to the forwarding table.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To create multicast MAC forwarding:

```
DGS-3224TGR:4# create multicast_fdb default 01-00-5E-00-00-00
Command: create multicast_fdb default 01-00-5E-00-00-00

Success.

DGS-3224TGR:4#
```

config multicast_fdb	
Purpose	Used to configure the switch's multicast MAC address forwarding database.
Syntax	**config multicast_fdb <vlan_name> <macaddr> [add|delete] <portlist>**
Description	This command configures the multicast MAC address forwarding table.
Parameters	<vlan_name> – The name of the VLAN on which the MAC address resides. <macaddr> – The MAC address that will be

config multicast_fdb	
	added to the forwarding table. [add|delete] – Add will add the MAC address to the forwarding table, delete will remove the MAC address from the forwarding table. <portlist> – Specifies a range of ports to be configured. The port list is specified by listing the beginning port number and the highest port number of the range. The beginning and end of the port list range are separated by a dash. For example, 3 would specify port 3. 4 specifies port 4. 3-4 specifies all of the ports between port 3 and port 4 – in numerical order.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To add multicast MAC forwarding:

```
DGS-3224TGR:4# config multicast_fdb default 01-00-5E-00-00-00 add 1-5
Command: config multicast_fdb default 01-00-5E-00-00-00 add 1-5

Success.


DGS-3224TGR:4#
```

delete fdb

Purpose	Used to delete an entry to the switch's forwarding database.
Syntax	**delete fdb <vlan_name> <macaddr>**
Description	This command is used to delete a previous entry to the switch's MAC address forwarding database.
Parameters	<vlan_name> – The name of the VLAN on which the MAC address resides. <macaddr> – The MAC address that will be added to the forwarding table.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To delete a permanent FDB entry:

```
DGS-3224TGR:4#delete fdb default 00-00-00-00-01-02
Command: delete fdb default 00-00-00-00-01-02

Success.

DGS-3224TGR:4#
```

clear fdb

clear fdb

Purpose	Used to clear the switch's forwarding database of all dynamically learned MAC addresses.
Syntax	**clear fdb [vlan <vlan_name>|port <port>|all]**
Description	This command is used to clear dynamically learned entries to the switch's forwarding database.
Parameters	<vlan_name> – The name of the VLAN on which the MAC address resides. <port> – The port number corresponding to the MAC destination address. The switch will always forward traffic to the specified device through this port. all – Clears all dynamic entries to the switch's forwarding database.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To clear all FDB dynamic entries**:**

```
DGS-3224TGR:4#clear fdb all
Command: clear fdb all

Success.
```

```
DGS-3224TGR:4#
```

show multicast_fdb

Purpose	Used to display the contents of the switch's multicast forwarding database.
Syntax	**show mulitcast_fdb [vlan <vlan_name>|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> – The name of the VLAN on which the MAC address resides. <macaddr> – The MAC address that will be added to the forwarding table.
Restrictions	None.

Example Usage:

To display multicast MAC address table:

```
DGS-3224TGR:4#show multicast_fdb
Command: show multicast_fdb

VLAN Name      : default
MAC Address    : 01-00-5E-00-00-00
Egress Ports   : 1-5, 21, 22
Mode           : Static

Total Entries : 1
```

```
DGS-3224TGR:4#
```

show fdb

Purpose	Used to display the current unicast MAC address forwarding database.
Syntax	**show fdb {port <port>|vlan <vlan_name>|mac_address <macaddr>|static|aging_time}**
Description	This command will display the current contents of the switch's forwarding database.
Parameters	<port> – The port number corresponding to the MAC destination address. The switch will always forward traffic to the specified device through this port. <vlan_name> – The name of the VLAN on which the MAC address resides. <macaddr> – The MAC address that will be added to the forwarding 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-3224TGR:4#show fdb
Command: show fdb

 Unicast MAC Address Aging Time  = 300

 VID   VLAN Name      MAC Address        Port    Type
 ----   ----------------      -----------------          ----      ---------
 1      default            00-00-00-00-01-02    5       Permanent
 1      default            00-50-BA-6B-2A-29   9       Dynamic

 Total Entries = 2

DGS-3224TGR:4#
```

11

BROADCAST STORM CONTROL COMMANDS

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

Command	Parameters
config traffic control	<storm_portlist> all broadcast [enable|disable] multicast [enable|disable] dlf [enable|disable]
show traffic control	port_list <storm_portlist>

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

config traffic control

Purpose	Used to configure broadcast|multicast traffic control.
Syntax	**config traffic control [<storm_portlist>|all] broadcast [enable|disable]|multicast [enable|disable]|dlf [enable|disable]|threshold <value>**
Description	This command is used to configure broadcast storm control.
Parameters	<storm_grouplist> – Used to specify a broadcast storm control group with the syntax: module_id:group_id. all – Specifies all broadcast storm control groups 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. threshold <value> – The upper threshold at which the specified traffic control is switched on. The <value> is the number of broadcast|multicast|dlf packets, in Kbps, received by the switch that will trigger the storm traffic control measures.

config traffic control

Restrictions	Only administrator-level users can issue this command.

Example Usage:

To configure traffic control and state:

```
DGS-3224TGR:4#config traffic control 2-3 broadcast
enable
Command: config traffic control 2-3 broadcast enable

Success.

DGS-3224TGR:4#
```

show traffic control

Purpose	Used to display current traffic control settings.
Syntax	**show traffic control <storm_portlist>**
Description	This command displays the current storm traffic control configuration on the switch.
Parameters	group_list <storm_portlist> – Used to specify a broadcast storm control group with the syntax: port_number.
Restrictions	None.

Example Usage:

To display traffic control setting:

```
DGS-3224TGR:4#show traffic control
Command: show traffic control

Traffic Control

Port        Broadcast              Multicast              Destination Lookup Fail
            State/Threshold (kbps) State/Threshold (kbps) State/Threshold (kbps)
------ ---------------------- ---------------------- ----------------------------------
1      Disabled/128           Disabled/128           Disabled/128
2      Disabled/128           Disabled/128           Disabled/128
3      Disabled/128           Disabled/128           Disabled/128
4      Disabled/128           Disabled/128           Disabled/128
5      Disabled/128           Disabled/128           Disabled/128
6      Disabled/128           Disabled/128           Disabled/128
7      Disabled/128           Disabled/128           Disabled/128
8      Disabled/128           Disabled/128           Disabled/128
9      Disabled/128           Disabled/128           Disabled/128
10     Disabled/128           Disabled/128           Disabled/128
11     Disabled/128           Disabled/128           Disabled/128
12     Disabled/128           Disabled/128           Disabled/128
13     Disabled/128           Disabled/128           Disabled/128
14     Disabled/128           Disabled/128           Disabled/128
15     Disabled/128           Disabled/128           Disabled/128
16     Disabled/128           Disabled/128           Disabled/128
17     Disabled/128           Disabled/128           Disabled/128
```

12

ARP COMMANDS

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

Command	Parameters
config arp_aging	time <min 0-65535>
show arpentry	{ipif(1) <ipif_name 12> | ipaddress(2) <ipaddr> | static(3)}
clear arptable	

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

config arp_aging	
Purpose	Used to configure the age-out timer for ARP table entries on the switch.
Syntax	**config arp_aging time <min 0-65535>**

config arp_aging

Description	This command sets the maximum amount of time, in minutes, that a ARP entry can remain in the switch's ARP table, without being accessed, before it is dropped from the table.
Parameters	time <min 0-65535> – The ARP age-out time, in minutes. The default is 20.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To configure ARP aging time:

```
DGS-3224TGR:4#config arp_aging time 30
Command: config arp_aging time 30

Success.

DGS-3224TGR:4#
```

show arpentry

Purpose	Used to display the ARP table.
Syntax	**show arpentry {ipif <ipif_name>|ipaddress <network_address>|static}**
Description	This command is used to display the current contents of the switch's ARP table.

show arpentry	
	current contents of the switch's ARP table.
Parameters	<ipif_name> – The name of the IP interface the end node or station for which the ARP table entry was made, resides on. <network_address> – 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-3224TGR:4#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          10.1.1.169      00-50-BA-70-E4-4E    Dynamic
System          10.1.1.254      00-01-30-FA-5F-00    Dynamic
System          10.9.68.1       00-A0-C9-A4-22-5B    Dynamic
System          10.9.68.4       00-80-C8-2E-C7-45    Dynamic
System          10.10.27.51     00-80-C8-48-DF-AB    Dynamic
System          10.11.22.145    00-80-C8-93-05-6B    Dynamic
System          10.11.94.10     00-10-83-F9-37-6E    Dynamic
```

```
System      10.14.82.24     00-50-BA-90-37-10     Dynamic
System      10.15.1.60      00-80-C8-17-42-55     Dynamic
System      10.17.42.153    00-80-C8-4D-4E-0A     Dynamic
System      10.19.72.100    00-50-BA-38-7D-5E     Dynamic
System      10.21.32.203    00-80-C8-40-C1-06     Dynamic
System      10.40.44.60     00-50-BA-6B-2A-1E     Dynamic
System      10.42.73.221    00-01-02-03-04-00     Dynamic
System      10.44.67.1      00-50-BA-DA-02-51     Dynamic
System      10.47.65.25     00-50-BA-DA-03-2B     Dynamic
System      10.50.8.7       00-E0-18-45-C7-28     Dynamic
System      10.90.90.90     00-01-02-03-04-00     Local
System      10.255.255.255  FF-FF-FF-FF-FF-FF     Local|Broadcast

Total Entries = 20

DGS-3224TGR:4#
```

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 effected.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To remove dynamic entries in the ARP table:

```
DGS-3224TGR:4#clear arptable
Command: clear arptable

Success.

DGS-3224TGR:4#
```

13

QOS COMMANDS

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

Command	Parameters
config scheduling	<class_id 0-7> weight <value 1-15>
config scheduling_mechanism	[strict|weight_fair]
show scheduling	
show scheduling_mechanism	
config 802.1p user_priority	<priority 0-7> <class_id 0-7>
show 802.1p user_priority	
config 802.1p default_priority	[<portlist>|all] <priority 0-7>
show 802.1p default_priority	<portlist>
disable hol_prevention	
enable hol_prevention	

Command	Parameters
show hol_prevention	
config bandwidth_control	<portlist>{rx_rate [no_limit | <value 1-1000>] | tx_rate [no_limit | <value 1-1000>]}
show bandwidth_control	{<portlist>}

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

config scheduling

Purpose	Used to configure the traffic scheduling mechanism for each COS queue.
Syntax	**config scheduling <class_id 0-7> weight <value 1-15>**
Description	The switch contains eight hardware priority queues. Incoming packets must be mapped to one of these eight queues. This command is used to specify the rotation by which these eight hardware priority queues are emptied. The switch's default (if the config scheduling command is not used) is to empty the eight hardware priority queues in order – from the highest priority queue (hardware queue 8) 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

config scheduling

	queue has finished transmitting all of its packets, the highest hardware priority queue can again transmit any packets it may have received.
Parameters	<class_id> – This specifies which of the eight hardware priority queues the config scheduling command will apply to. The eight hardware priority queues are identified by number – from 0 to 7 – with the 0 queue being the lowest priority.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To configure scheduling:

```
DGS-3224TGR:4# config scheduling 7 weight 2
Command: config scheduling 7 weight 2

Success.

DGS-3224TGR:4#
```

show scheduling

Purpose	Used to display the current traffic scheduling mechanisms in use on the switch.

show scheduling

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 show scheduling:

```
DGS-3224TGR:4# show scheduling
Command: show scheduling


QOS Output Scheduling

Class ID      MAX. Weight
------------  ------------------
Class-0           1
Class-1           2
Class-2           3
Class-3           4
Class-4           5
Class-5           6
Class-6           7
Class-7           8

DGS-3224TGR:4#
```

config scheduling_mechanis n	
Purpose	Used to configure the traffic scheduling mechanism for each COS queue.
Syntax	**config scheduling_mechanism [strict|weight_fair]**
Description	This command is use to specify how the switch handle packets in priority queues.
Parameters	strict – The highest queue is the first to process traffic. That is, the highest queue should be finished at first. weight_fair – Ue the weight fair algorithm to handle packets in priority queues.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To configure the traffic scheduling mechanism for each COS queue:

```
DGS-3224TGR:4# config scheduling_mechanism strict
Command: config scheduling_mechanism strict

Success.

DGS-3224TGR:4#
```

show scheduling_mechanism

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

Example Usage:

To show the scheduling mechanism:

```
DGS-3224TGR:4# show scheduling_mechanism
Command: show scheduling_mechanism

Scheduling Mechanism : weight_fair

DGS-3224TGR:4#
```

config 802.1p user_priority

Purpose	Used to map the 802.1p user priority of an incoming packet to one of the eight hardware queues available on the switch.

config 802.1p user_priority

Syntax

config 802.1p user_priority <priority 0-7> <class_id 0-7>

Description

The config 802.1p user_priority command allows you to configure the way the switch will map an incoming packet, based on its 802.1p user priority, to one of the eight available hardware priority queues on the switch. The switch's default is to map the following incoming 802.1p user priority values to the eight hardware priority queues:

The suggested mapping is included in the following table:

802.1p	Hardware Queue	Remark
0	2	Mid-low
1	0	Lowest
2	1	Low
3	3	Mid-low
4	4	Mid-high
5	5	Mid-high
6	6	High
7	7	Highest.

This mapping scheme is based upon recommendations contained in IEEE 802.1D (page 40).

config 802.1p user_priority

	You can change this mapping by specifying the 802.1p user priority you want to go to the <class_id> (the number of the hardware queue). <priority> – The 802.1p user priority you want to associate with the <class_id> (the number of the hardware queue) with. <class_id> – The number of the switch's hardware priority queue. The switch has eight hardware priority queues available. They are numbered between 0 (the lowest priority) and 7 (the highest priority).
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To configure 802.1p user priority:

```
DGS-3224TGR:4# config 802.1p user_priority 1 3
Command: config 802.1p user_priority 1 3

Success.

DGS-3224TGR:4#
```

show 802.1p user_priority

Purpose	Used to display the current 802.1p user priority-to-hardware priority queue mapping

show 802.1p user_priority

	priority to hardware priority queue mapping in use by the switch.
Syntax	**show 802.1p user_priority**
Description	This command will display the current 802.1p user priority to hardware priority queue mapping in use by the switch.
Parameters	None.
Restrictions	None.

Example Usage:

To show 802.1p user priority:

```
DGS-3224TGR:4# show 802.1p user_priority
Command: show 802.1p user_priority

QOS Class of Traffic

Priority-0  ->  <Class-1>
Priority-1  ->  <Class-3>
Priority-2  ->  <Class-0>
Priority-3  ->  <Class-1>
Priority-4  ->  <Class-2>
Priority-5  ->  <Class-2>
Priority-6  ->  <Class-3>
Priority-7  ->  <Class-3>

DGS-3224TGR:4#
```

config 802.1p default_priori y

Purpose	Used to configure the 802.1p default priority settings on the switch. If an untagged packet is received by the switch, the priority configured with this command will be written to the packet's priority field.
Syntax	**config 802.1p default_priority [<portlist>|all] <priority 0-7>**
Description	This command allows you to specify default priority handling of untagged packets received by the switch. The priority value entered with this command will be used to determine which of the eight hardware priority queues the packet is forwarded to.
Parameters	<portlist> – Specifies a range of ports that will belong to the link aggregation group. That is, a range of ports for which all untagged packets received will be assigned the priority specified below. The beginning and end of the port list range are seperated by a dash. For example, 3 would specify port 3. 4 specifies port 4. 1-4 specifies all of the ports between port 1 and port 4 – in numerical order. all – Specifies that the command applies to all ports on the switch (or in the switch stack). <priority 0-7> – The priority value you want to assign to untagged packets received by the switch or a range of ports on the switch.

config 802.1p default_priority	
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To configure 802.1p default priority:

```
DGS-3224TGR:4#config 802.1p default_priority all 5
Command: config 802.1p default_priority all 5

Success.

DGS-3224TGR:4#
```

show 802.1p default_priority	
Purpose	Used to display the current default priority settings on the switch.
Syntax	**show 802.1p default_priority**
Description	This command is used to display the current default priority settings on the switch.
Parameters	None.
Restrictions	None.

Example Usage:

To show 802.1p default priority:

```
DGS-3224TGR:4# show 802.1p default_priority
Command: show 802.1p default_priority

Port     Priority
-------  -----------
  1       0
  2       0
  3       0
  4       0
  5       0
  6       0
  7       0
  8       0
  9       0
 10       0
 11       0
 12       0
 13       0
 14       0
 15       0
 16       0
 17       0
 18       0
 19       0
 20       0
 21       0
 22       0
 23       0
 24       0

DGS-3224TGR:4#
```

enable hol_prevention

enable hol_prevention

Purpose	Used to enable HOL prevention.
Syntax	**enable hol_prevention**
Description	The enable hol_prevention command enables Head of Line prevention.
Parameters	None.
Restrictions	You must have administrator privileges.

Example Usage:

To enable HOL prevention:

```
DGS-3224TGR:4# enable hol_prevention
Command: enable hol_prevention

Success.

DGS-3224TGR:4#
```

disable hol_prevention

Purpose	Used to disable HOL prevention.
Syntax	**disable hol_prevention**
Description	The disable hol_prevention command disables Head of Line prevention.
Parameters	None.

disable hol_prevention

Restrictions	You must have administrator privileges.

Example Usage:

To disable HOL prevention:

```
DGS-3224TGR:4# disable hol_prevention
Command: disable hol_prevention

Success.

DGS-3224TGR:4#
```

show hol_prevention

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

Example Usage:

To show HOL prevention:

```
DGS-3224TGR:4# show hol_prevention
```

```
Command: show hol_prevention

Success.

DGS-3224TGR:4#
```

14

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 conigure a mirror port – source port pair on the switch.
Syntax	**config mirror port <port> add source ports <portlist> [rx|tx|both]**

config mirror port

Description	This command allows a range of ports to have all of their traffic also sent to a desnigated port – where a network sniffer or other device can monitor the network traffic. In addition, you can specify that only traffic received by or sent by or both is mirrored to the Target port.
Parameters	<port> – This specifies the Target port (the port where mirrored packets will be sent). <portlist> – This specifies a range of ports that will be mirrored. That is, a range of ports for which all traffic will be copied and sent to the Target port. The port list is specified by listing the beginning port number on that switch and the highest port number of the range. The beginning and end of the port list range are separated by a dash. For example, 3 would specify port 3. 4 specifies port 4. 3-4 specifies all of the ports between port 3 and port 4 – in numerical order. rx – Allows the mirroring of only packets received (flowing into) the port or ports in the port list. tx – Allows the mirroring of only packets sent (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.

config mirror port	
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To add the mirroring ports:

```
DGS-3224TGR:4#config mirror port 10 add source ports 1-5 both
Command: config mirror port 10 add source ports 1-5 both

Success.

DGS-3224TGR:4#
```

config mirror delete	
Purpose	Used to delete a port mirroring configuration|
Syntax	**config mirror <port> delete source <portlist> [rx|tx|both]**
Description	This command is used to delete a previously entered port mirroring configuration.
Parameters	<port> – This specifies the Target port (the port where mirrored packets will be sent). <portlist> – This specifies a range of ports that will be mirrored. That is, a range of ports for which all traffic will be copied and

config mirror delete	
	sent to the Target port. rx – Allows the mirroring of only packets received (flowing into) the port or ports in the port list. tx – Allows the mirroring of only packets sent (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	Only administrator-level users can issue this command.

Example Usage:

To delete the mirroring ports:

```
DGS-3224TGR:4#config mirror 5 delete source 1-5 both
Command: config mirror 5 delete source 1-5 both

Success.

DGS-3224TGR:4#
```

enable mirror	
Purpose	Used to enable a previously entered port mirroring configuration.
Syntax	**enable mirror**

enable mirror	
Description	This command, combined with the disable mirror command below, allows you to enter a port mirroring configuration into the switch, and then turn the port mirroring on and off without having to modify the port mirroring configuration.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To enable mirroring configurations:

```
DGS-3224TGR:4#enable mirror
Command: enable mirror

Success.

DGS-3224TGR:4#
```

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 you to enter a port mirroring configuration into the

disable mirror	
	switch, and then turn the port mirroring on and off without having to modify the port mirroring configuration.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To disable mirroring configurations:

```
DGS-3224TGR:4#disable mirror
Command: disable mirror

Success.

DGS-3224TGR:4#
```

show mirror	
Purpose	Used to show the current port mirroring configuration on the switch.
Syntax	**show mirror**
Description	This command displays the current port mirroring configuration on the switch.
Parameters	None
Restrictions	None.

Example Usage:

To display mirroring configuration:

```
DGS-3224TGR:4#show mirror
Command: show mirror

 Current Settings
 Target Port: 9
 Mirrored Port:
        RX:
        TX: 1-5

DGS-3224TGR:4#
```

15

PORT SECURITY COMMANDS

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

Command	Parameters
config port_security	ports [<portlist>| all] {admin_state [enable | disable]max_learning_addr<max_lock_no 0-10>|lock_address_mode [permanent| deleteontimeout|deleteonreset]}
delete port_security_entry	vlan_name <vlan_name 32> mac_address <macaddr> port <port>
clear port_security_entry	port <portlist>
show port_security	{ports <portlist>}

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

config port_security

Purpose	Used to configure port security.
Syntax	**ports [<portlist>| all] {admin_state [enable | disable]max_learning_addr<max_lock_no 0-10>|lock_address_mode [permanent| deleteontimeout|deleteonreset]}**
Description	This command allows you to configure port security, including admin state, maximum learning address, and lock address mode.
Parameters	<portlist> – Specifies a range of ports to be configured. all – Instructs all ports to be configured. admin_state – Allows the port security to be enabled or disabled for the ports specified in the port list. max_learning_addr – The maximum number of addresses that can be learned. lock_address_mode – Indicates the mode of locking address. Three choices are offered: Permanent – Indicates the locked addresses will not age out, even when the system is rebooted. These locked addresses can be deleted when the system is reset. DeleteOnTimeout – Indicates the locked addresses can be aged out after the aging timer expires.

config port_security

	DeleteOnReset – Indicates never age out the locked addresses unless the system is rebooted or reset in order to prevent port movement or intrusion.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To config port security:

```
DGS-3224TGR:4#config port_security ports 1-6
admin_state enable max_learning_addr 10
lock_address_mode Permanent
Command: config port_security ports 1-6 admin_state
enable max_learning_addr 10 lock_address_mode
Permanent

Success.

DGS-3224TGR:4#
```

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> mac_address <macaddr> port <port>**

delete port_security_entry	
Description	This command is used to delete a port security entry by MAC address, port number, and VLAN ID.
Parameters	<vlan_name> – The vlan name the port belongs to. mac_address – The MAC address to be deleted which was learned by the port. port – The port number which has learned the MAC address.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To delete a default route from the routing table:

```
DGS-3224TGR:4#delete port_security_entry vlan_name
default mac_address 00-01-30-10-2C-C7 port 1:6
Command: delete port_security_entry vlan_name default
mac_address 00-01-30-10-2C-C7 port 1:6

 Success.

DGS-3224TGR:4#
```

clear port_security_entry	
Purpose	Used to clear the MAC entries learned from the specified port(s) for the port security

clear port_security_entry	
	the specified port(s) for the port security function.
Syntax	**clear port_security_entry port <portlist>**
Description	Used to clear the MAC entries learned from the specified port(s) for the port security function.
Parameters	<portlist> – A range of ports to be configured.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To clear port security entry by port(s):

```
DGS-3224TGR:4#clear port_security_entry port 1-6
Command: clear port_security_entry port 1-6

Success.

DGS-3224TGR:4#
```

show port_security	
Purpose	Used to display the port security related information of the switch ports.
Syntax	**show port_security {ports<portlist>}**

show port_security

Description	The show port_security command displays the port security related information of the switch ports, including port security admin state, maximum number of learning addresses, and lock mode.
Parameters	<portlist> – A range of ports you want to delete from the above specified VLAN. The port list is specified by listing the beginning port number and the highest port number of the range. The beginning and end of the port list range are separated by a dash. For example, 3 would specify port 3. 4 specifies port 4. 3-4 specifies all of the ports between port 3 and port 4 – in numerical order.
Restrictions	None.

Example Usage:

To display the port security information of switch ports:

```
DGS-3224TGR:4#show port_security ports 1-3
Command: show port_security ports 1-3

Port    Admin State     Max. Learrning Addr.     Lock Address Mode
-------  ---------------  ---------------------------------- ----------------------------
1        Disabled      1                        DeleteOnReset
2        Disabled      1                        DeleteOnReset
3        Disabled      1                        DeleteOnReset

DGS-3224TGR:4#
```

16

VLAN COMMANDS

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

Command	Parameters
create vlan	<vlan_name 32> tag <vlanid 1-4094> advertisement
delete vlan	<vlan_name 32>
config vlan	<vlan_name 32> add [tagged|untagged|forbidden] <portlist>
config vlan	<vlan_name 32> delete <portlist>
config vlan	<vlan_name 32> advertisement [enable|disable]
config gvrp	<portlist> all {state [enable|disable] ingress_checking [enable|disable] pvid <vlanid 1-4094>}
enable gvrp	
disable gvrp	

Command	Parameters
show vlan	<vlan_name 32>
show gvrp	<portlist>
enable asymmetric_vlan	
disable asymmetric_vlan	
show asymmetric_vlan	

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>|advertisement**}
Description	This command allows you to create a VLAN on the switch.
Parameters	<vlan_name 32> – The name of the VLAN to be created. <vlanid 1-4094> – The VLAN ID of the VLAN to be created. advertisement – Specifies the VLAN participates normally in GARP/GVRP protocol exchanges. If this parameter is not set, the switch cannot send any

create vlan	
	GARP/GVRP messages about the VLAN.
Restrictions	Each VLAN name can be up to 32 characters. If the VLAN is not given a tag, it will automatically allocate a VID value. Only administrator-level users can issue this command.

Example Usage:

To create a VLAN v1, tag 2:

```
DGS-3224TGR:4#create vlan v1 tag 2
Command: create vlan v1 tag 2

Success.

DGS-3224TGR:4#
```

delete vlan	
Purpose	Used to delete a previously configured VLAN on the switch.
Syntax	**delete vlan <vlan_name 32>**
Description	This command will delete a previously configured VLAN on the switch.
Parameters	<vlan_name 32> – The VLAN name of the VLAN you want to delete.

delete vlan

Restrictions	Only administrator-level users can issue this command.

Example Usage:

To remove a vlan v1:

```
DGS-3224TGR:4#delete vlan v1
Command: delete vlan v1

 Success.

DGS-3224TGR:4#
```

config vlan add ports

Purpose	Used to add additional ports to a previously configured VLAN.
Syntax	**config vlan <vlan_name 32> add [tagged|untagged|forbidden] <portlist>**
Description	This command allows you to add ports to the port list of a previously configured VLAN. You can specifiy the additional ports as tagging, untagging, or forbidden.
Parameters	<vlan_name 32> – The name of the VLAN you want to add ports to. tagged – Specifies the additional ports as tagged.

config vlan add ports

	untagged – Specifies the additional ports as untagged. forbidden – Specifies the additional ports as forbidden. <portlist> – A range of ports to add to the VLAN. The port list is specified by listing the beginning port number and the highest port number of the range. The beginning and end of the port list range are separated by a dash. For example, 3 would specify port 3. 4 specifies port 4. 3-4 specifies all of the ports between port 3 and port 4 – in numerical order.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

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

```
DGS-3224TGR:4#config vlan v1 add tagged 4-8
Command: config vlan v1 add tagged 4-8

Success.

DGS-3224TGR:4#
```

config vlan delete ports

Purpose	Used to delete one or more ports from a previously configured VLAN|
Syntax	**config vlan <vlan_name 32> delete <portlist>**
Description	This command allows you to delete ports from a previously configured VLAN's port list.
Parameters	<vlan_name 32> – The name of the VLAN you want to delete ports from. <portlist> – A range of ports you want to delete from the above specified VLAN. The port list is specified by listing the beginning port number and the highest port number of the range. The beginning and end of the port list range are separated by a dash. For example, 3 would specify port 3. 4 specifies port 4. 3-4 specifies all of the ports between port 3 and port 4 – in numerical order.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To delete 4 through 8 to the VLAN v1:

```
DGS-3224TGR:4#config vlan v1 delete 4-8
Command: config vlan v1 delete 4-8
```

```
Success.

DGS-3224TGR:4#
```

config vlan advertisement

Purpose	Used to enable or disable the VLAN advertisement.
Syntax	**config vlan <vlan_name 32> advertisement [enable|disable]**
Description	This command is used to enable or disable sending GVRP messages on the specified VLAN.
Parameters	<vlan_name 32> – The name of the VLAN on which you want to enable or disable sending GVRP messages. enable – Enables sending GVRP messages on the specified VLAN. disable – Disables sending GVRP messages on the specified VLAN.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To enable the VLAN default advertisement:

```
DGS-3224TGR:4#config vlan default advertisement
enable
Command: config vlan default advertisement enable
```

```
Success.

DGS-3224TGR:4#
```

config gvrp

Purpose	Used to configure GVRP on the switch.
Syntax	**config gvrp [<portlist>|all] {state [enable|disable]|ingress_checking [enable|disable] |pvid <vlanid 1-4094>}**
Description	This command is used to configure the Group VLAN Registration Protocol on the switch. You can configure ingress checking and the GVRP status for each port. If the asymmetric VLAN is enabled, you can configure PVID. If it is disabled, you can not configure PVID.
Parameters	<portlist> – A range of ports for which you want ingress checking. The port list is specified by listing the beginning port number and the highest port number of the range. The beginning and end of the port list range are separated by a dash. For example, 3 would specify port 3. 4 specifies port 4. 3-4 specifies all of the ports between port 3 and port 4 – in numerical order. all – Specifies all of the ports on the switch. state [enable|disable] – Enables or disables

config gvrp	
	GVRP for the ports specified in the port list. ingress_checking [enable|disable] – Enables or disables ingress checking for the specified port list. pvid – Specifies the default VLAN will associate with the port.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To sets the ingress checking status and the GVRP status:

```
DGS-3224TGR:4#config gvrp 1-5 state enable
ingress_checking enable pvid 2
Command: config gvrp 1-5 state enable
ingress_checking enable pvid 2

Success.

DGS-3224TGR:4#
```

enable gvrp	
Purpose	Used to enable GVRP on the switch.

enable gvrp	
Syntax	**enable gvrp**
Description	This command, along with disable gvrp below, is used to enable and disable GVRP on the switch – without changing the GVRP configuration for each port on the switch.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To enable the generic VLAN Registration Protocol (GVRP):

```
DGS-3224TGR:4#enable gvrp
Command: enable gvrp

Success.

DGS-3224TGR:4#
```

disable gvrp	
Purpose	Used to disable GVRP on the switch.
Syntax	**disable gvrp**
Description	This command, along with disable gvrp below, is used to enable and disable GVRP

disable gvrp	
	on the switch – without changing the GVRP configuration for each port on the switch.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To disable the Generic VLAN Registration Protocol (GVRP):

```
DGS-3224TGR:4#disable gvrp
Command: disable gvrp

Success.

DGS-3224TGR:4#
```

show vlan	
Purpose	Used to display the current VLAN configuration on the switch
Syntax	**show vlan** {**<vlan_name 32>**}
Description	This command displays summary information about each VLAN including the VLAN ID, VLAN name, the Tagging/Untagging status, and the

show vlan	
	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 you want to display a summary of settings.
Restrictions	None.

Example Usage:

To display VLAN settings:

```
DGS-3224TGR:4#show vlan
Command: show vlan

VID              : 1          VLAN Name       : default
VLAN TYPE        : static     Advertisement   : Enabled
Member ports     : 1-24
 Static ports    : 1-24
Untagged ports   : 1-23
Forbidden ports  :

Total Entries : 1

DGS-3224TGR:4#
```

show gvrp	
Purpose	Used to display the GVRP status for a port list on the switch.

show gvrp	
Syntax	**show gvrp** {**<portlist>**}
Description	This command displays the
Parameters	<portlist> – Specifies a range of ports for which the GVRP statust is to be displayed. The port list is specified by listing the beginning port number and the highest port number of the range. The beginning and end of the port list range are separated by a dash. For example, 3 would specify port 3. 4 specifies port 4. 3-4 specifies all of the ports port 3 and port 4 – in numerical order.
Restrictions	None.

Example Usage:

To display 802.1Q port setting:

```
DGS-3224TGR:4#show gvrp
Command: show gvrp

Global GVRP : Disabled

Port   PVID    GVRP        Ingress Checking
----   ------- --------    --------------------
1      1       Enable      Enable
2      1       Enable      Enable
3      1       Enable      Enable
4      1       Enable      Enable
5      1       Enable      Enable
6      1       Disable     Disable
```

```
7       1       Disable     Disable
8       1       Disable     Disable
9       1       Disable     Disable
10      1       Disable     Disable
11      1       Disable     Disable
12      1       Disable     Disable
13      1       Disable     Disable
14      1       Disable     Disable
15      1       Disable     Disable
16      1       Disable     Disable
17      1       Disable     Disable
18      1       Disable     Disable
19      1       Disable     Disable
20      1       Disable     Disable
21      1       Disable     Disable
22      1       Disable     Disable
23      1       Disable     Disable
24      1       Disable     Disable

Total Entries : 24

DGS-3224TGR:4#
```

enable asymmetric_vlan

Purpose	Used to enable asymmetric VLANs on the switch.
Syntax	**enable asymmetric_vlan**
Description	This command enables asymmetric VLANs.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To enable asymmetric VLANs:

```
DGS-3224TGR:4#enable asymmetric_vlan
Command: enable asymmetric_vlan

Success.

DGS-3224TGR:4#
```

disable asymmetric_vlan

Purpose	Used to disable asymmetric VLANs on the switch.
Syntax	**disable asymmetric_vlan**
Description	This command disables asymmetric VLANs.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To disable asymmetric VLANs:

```
DGS-3224TGR:4#disable asymmetric_vlan
Command: disable asymmetric_vlan
```

```
Success.

DGS-3224TGR:4#
```

show asymmetric_vlan

Purpose	Used to display the current asymmetric VLAN status on the switch.
Syntax	**show asymmetric_vlan**
Description	This command displays asymmetric VLAN status.
Parameters	None.
Restrictions	None.

Example Usage:

To display asymmetric VLAN status:

```
DGS-3224TGR:4#show asymmetric_vlan
Command: show asymmetric_vlan

Asymmetric Vlan          : Enabled

DGS-3224TGR:4#
```

17

LINK AGGREGATION COMMANDS

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

Command	Parameters
create link_aggregation	group_id <value 1-32>{type [lacp|static]}
delete link_aggregation	group_id <value 1-32>
config link_aggregation	group_id <value 1-32> {master_port <port>| ports <portlist> state [enable|disable]}
config link_aggregation algorithm	[mac_source| mac_destination| mac_source_dest ip_source ip_destination ip_source_dest
show link_aggregation	group_id <value 1-32> algorithm
config lacp_ports	<portlst> mode [active|passive]

Command	Parameters
show lacp_ports	{<portlist>}

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

create link_aggregation group_id	
Purpose	Used to create a link aggregation group on the switch.
Syntax	**create link_aggregation group_id <value 1-32>(type [lacp|static]}**
Description	This command will create a link aggregation group.
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. type [lacp|static] – Indicates the group type belongs to *static* or *lacp*. If type is not specified, the default is *static*.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To create link aggregation group:

```
DGS-3224TGR:4#create link_aggregation group_id 1
Command: create link_aggregation group_id 1

Success.

DGS-3224TGR:4#
```

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-level users can issue this command.

Example Usage:

To delete link aggregation group:

```
DGS-3224TGR:4#delete link_aggregation group_id 6
Command: delete link_aggregation group_id 6

 Success.
```

```
DGS-3224TGR:4#
```

config link_aggregation

Purpose	Used to configure a previously created link aggregation group.
Syntax	**config link_aggregation group_id <value 1-32> {master_port <port>|ports <portlist>| state [enable|disable]**
Description	This command allows you to configure a link aggregation group that was created with the create link_aggregation command above.
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. <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. <portlist> – Specifies a range of ports that will belong to the link aggregation group. The beginning and end of the port list range are separated by a dash. For example, 3 would specify port 3. 4 specifies port 4. 1-4 specifies all of the ports between port 1 and port 4 – in numerical order.

config link_aggregation

	state [enable|disable] – Allows you to enable or disable the specified link aggregation group.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To define a load-sharing group of ports, group-id 1, master port 17:

```
DGS-3224TGR:4#config link_aggregation group_id 1 master_port 17 ports 5-10
Command: config link_aggregation group_id 1 master_port 17 ports 5-10

Success.

DGS-3224TGR:4#
```

config link_aggregation algorithm

Purpose	Used to configure the link aggregation algorithm.
Syntax	**config link_aggregation algorithm [mac_source|mac_destination|mac_source_dest| ip_source|ip_destination|ip_source_dest]**
Description	This command configures to part of the packet examined by the switch when selecting the

config link_aggregation algorithm	
	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 examin the MAC destination address. mac_source_dest – Indicates that the switch should examine the MAC source and ddestination 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-level users can issue this command.

Example Usage:

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

```
DGS-3224TGR:4#config link_aggregation algorithm
mac_source_dest
Command: config link_aggregation algorithm
mac_source_dest

Success.

DGS-3224TGR:4#
```

show link_aggregation

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

Example Usage:

To show link aggregation:

```
DGS-3224TGR:4#show link_aggregation
Command: show link_aggregation

Link Aggregation Algorithm = MAC-source
Group ID          : 1
Master Port       : 1
Member Port       : 1-8
Status            : Disabled
Flooding Port     : 5

DGS-3224TGR:4#
```

config lacp_ports

Purpose	Used to configure the current mode of LACP for specified ports.
Syntax	**config lacp_ports <portlist> mode [active|passive]**
Description	This command configures per-port LACP mode.
Parameters	<portlist> – Specifies a range of ports to be configured. The beginning and end of the port list range are separated by a dash. For example, 3 would specify port 3. 4 specifies port 4. 1-4 specifies all of the ports between port 1 and port 4 – in numerical order. mode [active|passive] – If neither *active* or *passive* is specified, the system will display the current LACP status for all ports.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To configure ports for LACP:

```
DGS-3224TGR:4#config lacp_port 1-12 mode active
Command: config lacp_port 1-12 mode active

Success.

DGS-3224TGR:4#
```

show lacp_ports

Purpose	Used to display the current mode of LACP ports.
Syntax	**show lacp_ports <portlist>**
Description	This command will display per-port LACP mode.
Parameters	<portlist> – Specifies a range of ports to be configured. If no parameter is specified, the system will display the current LACP status of all ports. The beginning and end of the port list range are separated by a dash. For example, 3 would specify port 3. 4 specifies port 4. 1-4 specifies all of the ports between port 1 and port 4 – in numerical order.
Restrictions	None.

Example Usage:

To show the LACP status for ports 1 to 3:

```
DGS-3224TGR:4#show lacp_ports
Command: show lacp_ports 1-3

Port      Activity
--------  ------------
1         Active
2         Active
3         Active

DGS-3224TGR:4#
```

18

IP INTERFACE COMMANDS

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

Command	Parameters
config ipif System	vlan <vlan_name> ipaddress <network_address> state [enable|disable] bootp dhcp
show ipif	<ipif_name>

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

config ipif System	
Purpose	Used to configure the System IP interface.

config ipif System

Syntax	**config ipif System [{vlan <vlan_name>|ipaddress <network_address>|state [enable|disable]|bootp|dhcp}]**
Description	This command is used to configure the System IP interface on the switch.
Parameters	<vlan_name> – The name of the VLAN corresponding to the System IP interface. <network_address> – IP address and netmask of th IP interface to be created. You 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, 10.1.2.3/16). state [enable|disable] – Allows you to enable or disable the IP interface. bootp – Allows the selection of the BOOTP protocol for the assignment of an IP address to the switch's System IP interface. dhcp – Allows the selection of the DHCP protocol for the assignment of an IP address to the switch's System IP interface.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To configure the IP interface System:

```
DGS-3224TGR:4#config ipif System ipaddress
10.48.74.122/8
Command: config ipif System ipaddress 10.48.74.122/8

Success.

DGS-3224TGR:4#
```

config ipif

Purpose	Used to configure an IP interface on the switch.
Syntax	**config ipif <ipif_name> {vlan <vlan_name>|ipaddress <network_address>|state [enabled|disabled]}**
Description	This command is used to configure an IP interface on the switch.
Parameters	<ipif_name> – The name of the IP interface to be configured on the switch. <vlan_name> – The name of the VLAN that corresponds to the IP interface above. <network_address> – IP address and netmask of th IP interface to be created. You 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, 10.1.2.3/16). state [enabled|disabled] – Allows you to

config ipif	
	enable or disable the IP interface.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To configure the IP interface ip2:

```
DGS-3224TGR:4#config ipif ip2 vlan vlan1
Command: config ipif ip2 vlan vlan1

Success.

DGS-3224TGR:4#
```

show ipif	
Purpose	Used to display the configuration of an IP interface on the switch.
Syntax	**show ipif** {**<ipif_name>**}
Description	This command will display the configuration of an IP interface on the switch.
Parameters	<ipif_name> – The name of the IP interface you want to disable. all – Specifies that all IP interfaces configured on the switch will be disabled.

show ipif

Restrictions None.

Example Usage:

To display IP interface settings:

```
DGS-3224TGR:4#show ipif System
Command: show ipif System

 IP Interface Settings

 Interface Name  : System
 IP Address      : 10.48.74.122    (MANUAL)
 Subnet Mask     : 255.0.0.0
 VLAN Name       : default
 Admin. State    : Disabled
 Link Status     : Link UP
 Member Ports    : 1-24

 Total Entries   : 1

DGS-3224TGR:4#
```

19

IGMP SNOOPING 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 igmp_snooping	<vlan_name 32> all host_timeout <sec 1-16711450> router_timeout <sec 1-16711450> leave_timer <sec 1-16711450> state [enable|disable]
config igmp_snooping querier	<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 1-65535> state [enable|disable]
config router_ports	<vlan_name 32> [add|delete] <portlist>
enable igmp snooping	forward_mcrouter_only

Command	Parameters
show igmp_ snooping	vlan <vlan_name 32>
show router ports	vlan <vlan_name 32> static dynamic
show igmp_snooping group	{vlan <vlan_name 32>}
config router_ports	<vlan_name 32> [add|delete] <portlist>
disable igmp_snooping	

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

config igmp_snooping

Purpose	Used to configurer IGMP snooping on the switch.
Syntax	**config igmp_snooping [<vlan_name 32>|all] {host_timeout <sec 1-16711450>|router_timeout <sec 1-16711450>|leave_timer <sec 1-16711450>|state [enable|disable]}**
Description	This command allows you to configure IGMP snooping on the switch.
Parameters	<vlan_name 32> – The name of the VLAN for which IGMP snooping is to be configured.

config igmp_snooping	
	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. router_timeout <sec 1-16711450> – Specifies the maximum amount of time a route will remain in the switch's can be a member of a multicast group without the switch receiving a host membership report. The default is 260 seconds. leave_timer <sec 1-16711450> – Leave timer. The default is 2 seconds. state [enable|disable] – Allows you to enable or disable IGMP snooping for the specified VLAN.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To configure the IGMP snooping:

```
DGS-3224TGR:4#config igmp_snooping default
host_timeout 250 state enabled
Command: config igmp_snooping default host_timeout
250 state enabled

Success.
```

```
DGS-3224TGR:4#
```

config igmp_snooping queri :r

Purpose	Used to configure the time in seconds between general query transmissions, the maximum time in seconds to wait for reports from members, the permitted packet loss that guarantees IGMP snooping.
Syntax	**config igmp_snooping querier [<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 1-65535>|state [enable|disable]**
Description	This command configures IGMP snooping querier.
Parameters	<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

config igmp_snooping querier	
	packet loss on a subnet. The value of the robustness variable is used in calculating the following IGMP message intervals: • Group member interval—Amount of time that must pass before a multicast router decides there are no more members of a group on a network. This interval is calculated as follows: `(robustness variable x query interval) + (1 x query response interval).` • Other querier present interval—Amount of time that must pass before a multicast router decides that there is no longer another multicast router that is the querier. This interval is calculated as follows: `(robustness variable x query interval) + (0.5 x query response interval).` • Last member query count—Number of group-specific queries sent before the router assumes there are no local members of a group. The default number is the value of the robustness variable. • By default, the robustness variable is set to 2. You might want to increase this value if you expect a subnet to be lossy. last_member_query_interval <sec 1-65535>

config igmp_snooping queri :r	
	– The maximum amount of time between group-specific query messages, including those sent in response to leave-group messages. You might lower this interval to reduce the amount of time it takes a router to detect the loss of the last member of a group. state [enable|disable] – Allows the switch to be specified as an IGMP Querier or Non-querier.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To configure IGMP snooping:

```
DGS-3224TGR:4#config igmp_snooping querier default
query_interval 125 state enable

Command: config igmp_snooping querier default
query_interval 125 state enable

Success.

DGS-3224TGR:4#
```

config router_ports	
Purpose	Used to configure ports as router ports.

config router_ports

Syntax	**config router_ports <vlan_name 32> [add|delete] <portlist>**
Description	This command allows you 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. <portlist> – Specifies a range of ports which will be configured as router ports. The port list is specified by listing the beginning port number and the highest port number of the range. The beginning and end of the port list range are separated by a dash. For example, 3 would specify port 3. 4 specifies port 4. 3-4 specifies all of the ports between port 3 and port 4 – in numerical order.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To set up static router ports:

```
DGS-3224TGR:4#config router_ports default add1-10
Command: config router_ports default add 1-10
```

```
Success.

DGS-3224TGR:4#
```

enable igmp_snooping

Purpose	Used to enable IGMP snooping on the switch.
Syntax	**enable igmp_snooping {forward_mcrouter_only}**
Description	This command allows you 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 mulitcast traffic to any IP router.
Parameters	forward_mcrouter_only – Specifies that the switch should forward all multicast traffic to a multicast-enabled router only. Otherwise, the switch will forward all multicast traffic to any IP router.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To enable IGMP snooping on the switch:

```
DGS-3224TGR:4#enable igmp_snooping
Command: enable igmp_snooping
```

```
Success.

DGS-3224TGR:4#
```

disable igmp_snooping

Purpose	Used to enable IGMP snooping on the switch.
Syntax	**disable igmp_snooping**
Description	This command disables IGMP snooping on the switch. 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	None.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To disable IGMP snooping on the switch:

```
DGS-3224TGR:4#disable igmp_snooping
Command: disable igmp_snooping

Success.

DGS-3224TGR:4#
```

show igmp_snooping

Purpose	Used to show the current status of IGMP snooping on the switch.
Syntax	**show igmp_snooping** {**vlan <vlan_name 32>**}
Description	This command will display the current IGMP snooping configuration on the switch.
Parameters	<vlan_name 32> – The name of the VLAN for which you want to view the IGMP snooping configuration.
Restrictions	None.

Example Usage:

To show IGMP snooping:

```
DGS-3224TGR:4#show igmp_snooping
Command: show igmp_snooping

IGMP Snooping Global State   : Disabled
Multicast router Only        : Disabled

VLAN  Name                   : default
Query Interval               : 125
Max Response Time            : 10
Robustness Value             : 2
Last Member Query Interval   : 1
Host Timeout                 : 260
Route Timeout                : 260
Leave Timer                  : 2
```

```
Querier State                 : Disabled
Querier Router Behavior       : Non-Querier
State                         : Disabled

VLAN  Name                    : vlan2
Query Interval                : 125
Max Response Time             : 10
Robustness Value              : 2
Last Member Query Interval    : 1
Host Timeout                  : 260
Route Timeout                 : 260
Leave Timer                   : 2
Querier State                 : Disabled
Querier Router Behavior       : Non-Querier
State                         : Disabled

Total Entries: 2

DGS-3224TGR:4#
```

show igmp_snooping group

Purpose	Used to display the current IGMP snooping group configuration on the switch.
Syntax	**show igmp_snooping group {vlan <vlan_name 32>}**
Description	This command will display the current IGMP snooping group configuration on the swtich.
Parameters	<vlan_name 32> – The name of the VLAN for which you want to view IGMP snooping group configuration information.

show igmp_snooping group

Restrictions None.

Example Usage:

To show IGMP snooping group:

```
DGS-3224TGR:4#show igmp_snooping group
Command: show igmp_snooping group

 VLAN Name      : default
 Multicast group: 224.0.0.2
 MAC address    : 01-00-5E-00-00-02
 Reports        : 1
 Port Member    :  7

 VLAN Name      : default
 Multicast group: 224.0.0.9
 MAC address    : 01-00-5E-00-00-09
 Reports        : 1
 Port Member    :  7

 VLAN Name      : default
 Multicast group: 234.5.6.7
 MAC address    : 01-00-5E-05-06-07
 Reports        : 1
 Port Member    :  9

 Total Entries : 3

DGS-3224TGR:4#
```

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}**
Description	This command will display the router ports currently configured on the switch.
Parameters	<vlan_name 32> – The name of the VLAN on which the router port resides. static – Displays router ports that have been statically configured. dynamic – Displays router ports that have been dynamically configued.
Restrictions	None.

Example Usage:

To display the router ports:

```
DGS-3224TGR:4#show router_ports
Command: show router_ports

VLAN Name             : default
Static router port    : 1-10
Dynamic router port   :

VLAN Name             : vlan2
Static router port    :
Dynamic router port   :
```

```
Total Entries: 2

DGS-3224TGR:4#
```

20

ROUTING TABLE COMMANDS

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

Command	Parameters
create iproute	default <network_address> <ipaddr> <metric>
delete iproute	default <network_address>
show iproute	<network_address> static rip ospf

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

create iproute	
Purpose	Used to create an IP route entry to the switch's IP routing table.
Syntax	**create iproute [default|<network_address>] <ipaddr> {<metric>}**
Description	This command is used to create an IP route entry to the switch's IP routing table.
Parameters	default – creates a default IP route entry. <network_address> – IP address and netmask of the IP interface that is the destination of the route. You 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, 10.1.2.3/16). <ipaddr> – The IP address for the next hop router. <metric> – The default setting is 1.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To add a static address 10.48.74.121, mask 255.0.0.0, and gateway 10.1.1.254 to the routing table:

```
DGS-3224TGR:4#create iproute 10.48.74.121/255.0.0.0
10.1.1.254 1
Command: create iproute 10.48.74.121/8 10.1.1.254 1

Success.

DGS-3224TGR:4#
```

delete iproute

Purpose	Used to delete an IP route entry from the switch's IP routing table.
Syntax	**delete iproute [default|<network_address>]**
Description	This command will delete an existing entry from the switch's IP routing table.
Parameters	default – Deletes a default IP route entry. <network_address> – IP address and netmask of the IP interface that is the destination of the route. You 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, 10.1.2.3/16).
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To delete a static address 10.48.75.121, mask 255.0.0.0 from the routing table:

```
DGS-3224TGR:4#delete iproute 10.48.74.121/255.0.0.0
Command: delete iproute 10.48.74.121/8

Success.

DGS-3224TGR:4#
```

show iproute

Purpose	Used to display the switch's current IP routing table.
Syntax	**show iproute** {**<network_address>**} {**static|rip|ospf**}
Description	This command will display the switch's current IP routing table.
Parameters	<network_address> – IP address and netmask of the IP interface that is the destination of the route. You 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, 10.1.2.3/16).
Restrictions	none.

Example Usage:

To display the contents of the IP routing table:

```
DGS-3224TGR:4#show iproute
Command: show iproute

IP Address      Netmask       Gateway       Interface  Name  Hops  Protocol
--------------- --------------- --------------- --------------- ---- -----------
  0.0.0.0       0.0.0.0       10.1.1.254    System          1     Default
 10.0.0.0       255.0.0.0     10.48.74.122  System          1     Local

Total Entries: 2

DGS-3224TGR:4#
```

21

802.1X COMMANDS

The DGS-3224TGR implements the server-side of the IEEE 802.1x Port-based Network Access Control. This mechanism is intended to allow only authorized users, or other network devices, access to network resources by establishing criteria for each port on the switch that a user or network device must meet before allowing that port to forward or receive frames.

Command	Parameters
enable 802.1x	
disable 802.1x	
config 802.1x auth_protocol	[local|radius_eap]
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 1-999999999>

Command	Parameters
	enable_reauth [enabled|disabled]
config 802.1x init	ports [<portlist>|all]
config 802.1x reauth	ports [<portlist>|all]
config radius add	<server_index 1-3> <server_ip> key <passwd 32> default auth_port <udp_port_number 1-65535> acct_port <udp_port_number 1-65535>
config radius delete	<server_index 1-3>
config radius	<server_index 1-3> ipaddress <server_ip> key <passwd 32> auth_port <udp_port_number 1-65535> acct_port <udp_port_number 1-65535>
show radius	
show 802.1x user	
create 802.1x user	<username 15>
delete 802.1x user	<username 15>
show auth_statistics	{ports <portlist>}
show auth_diagnostics	{ports <portlist>}
show auth_session_statistics	{ports <portlist>}
show radius auth_client	
show radius acct_client	

enable 802.1x

enable 802.1x	
Purpose	Used to enable the 802.1x server on the switch.
Syntax	**enable 802.1x**
Description	The enable 802.1x command enables the 802.1x Port-based Network Access control server application on the switch.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To enable 802.1x switch-wide:

```
DGS-3224TGR:4#enable 802.1x
Command: enable 802.1x

Success.

DGS-3224TGR:4#
```

disable 802.1x	
Purpose	Used to disable the 802.1x server on the switch.
Syntax	**disable 802.1x**
Description	The disable 802.1x command is used to disable the 802.1x Port-based Network

disable 802.1x	
	Access control server application on the switch.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To disable 802.1x on the switch:

```
DGS-3224TGR:4#disable 802.1x
Command: disable 802.1x

Success.

DGS-3224TGR:4#
```

config 802.1x auth_protoco	
Purpose	Used to configure the 802.1x authentication protocol on the switch.
Syntax	**config 802.1x auth_protocol [local|radius_eap]**
Description	The config 802.1x auth_protocol command enables you to configure the authentication protocol.
Parameters	local|radius_EAP – Specify the type of authentication protocol desired.

config 802.1x auth_protoco	
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To configure 802.1x authentication protocol:

```
DGS-3224TGR:4# config 802.1x auth_protocol
Command: config 802.1x auth_protocol

Success.

DGS-3224TGR:4#
```

config 802.1x capability	
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	The config 802.1x command has two capabilities that can be set for each port: Authenticator and None.
Parameters	<portlist> – Specifies a range of ports. The port list is specified by listing the beginning port number and the highest port number of the range. The beginning and end of the port list range are separated by a dash. For example, 3 would specify port 3. 4 specifies port 4. 3-4 specifies all of the ports between port 3 and port 4 – in numerical order.

config 802.1x capability	
	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-level users can issue this command.

Example Usage:

To configure 802.1x capability on ports 1-10:

```
DGS-3224TGR:4#config 802.1x capability ports 1 – 10 authenticator
Command: config 802.1x capability ports 1-10 authenticator

Success.

DGS-3224TGR:4#
```

config 802.1x auth_parameter	
Purpose	Used to configure the 802.1x Authentication parameters on a range of ports. The default parameter will return all ports in the specified range to their default 802.1x settings.
Syntax	**config 802.1x auth_parameter ports [<portlist>|all] [default|{direction [both|in]|port_control [force_unauth|auto|force_auth]| quiet_period <sec 0-65535>| max_req**

config 802.1x auth_parameter	
	<value 1-10>|reauth_period <sec 1-65535>|enable_reauth [enabled|disabled]}]
Description	The config 802.1x auth_parameter command is used to configure the 802.1x Authentication parameters on a range of ports. The default parameter will return all ports in the specified range to their default 802.1x settings.
Parameters	<portlist> – Specifies a range of ports. The port list is specified by listing the beginning port number and the highest port number of the range. The beginning and end of the port list range are separated by a dash. For example, 3 would specify port 3. 4 specifies port 4. 3-4 specifies all of the ports between port 3 and port 4 – in numerical order. 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. force_auth – Forces the Authenticator for the port to become authorized. Network access is allowed.

config 802.1x auth_parameter	
	auto – Allows the port's status to reflect the outcome of the authentication process. force_unauth – Forces the Authenticator for the port to become unauthorized. Network access will be blocked. quiet_period <sec 0-65535> – Configures the time interval between authentication failure and the start of a new authenticaiton attempt. max_req <value 1-10> – Configures the number of times to retry sending packets to a supplicant (user). reauth_period <sec 1-65535> – Configures the time interval between successive re-authentications. enable_reauth [enabled|disabled] – Determines whether or not the switch will re-authenticate. Enabled causes re-authentication of users at the time interval specified in the Re-authentication Period field, above.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To configure 802.1x authentication parameters for ports 1 to 20:

```
DGS-3224TGR:4#config 802.1x auth_parameter ports 1 – 20
direction both
Command: config 802.1x auth_parameter ports 1-20 direction
```

```
both

Success.

DGS-3224TGR:4#
```

config 802.1x init

Purpose	Used to initialize the 802.1x functions on a range of ports.
Syntax	**config 802.1x init ports [<portlist>|all]**
Description	The config 802.1x init command is used to immediately initialize the 802.1x functions on a range of ports.
Parameters	<portlist> – Specifies a range of ports. The port list is specified by listing the beginning port number and the highest port number of the range. The beginning and end of the port list range are separated by a dash. For example, 3 would specify port 3. 4 specifies port 4. 3-4 specifies all of the ports between port 3 and port 4 – in numerical order. all – Specifies all of the ports on the switch.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To initialize 802.1x port-based functions on ports 1 to 15:

```
DGS-3224TGR:4#config 802.1x init ports 1-15
Command: config 802.1x init ports 1-15

Success.

DGS-3224TGR:4#
```

config 802.1x reauth

Purpose	Used to configure the 802.1x re-authentication feature of the switch.
Syntax	**config 802.1x reauth ports [<portlist>|all]**
Description	The config 802.1x reauth command is used to enable the 802.1x re-authentication feature on the switch.
Parameters	<portlist> – Specifies a range of ports. The port list is specified by listing the beginning port number and the highest port number of the range. The beginning and end of the port list range are separated by a dash. For example, 3 would specify port 3. 4 specifies port 4. 3-4 specifies all of the ports between port 3 and port 4 – in numerical order. all – Specifies all of the ports on the switch.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To configure 802.1x reauthentication for ports 1-15:

```
DGS-3224TGR:4#config 802.1x reauth ports 1-15
Command: config 802.1x reauth ports 1-15

Success.

DGS-3224TGR:4#
```

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_numbe 1-65535>| acct_port <udp_port_number 1-65535>}]**
Description	The config radius add 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

config radius add

	switch. Up to 32 characters can be used. default – Returns all of the ports in the range to their default RADIUS settings. auth_port <udp_port_number 1-65535> – The UDP port number for authentication requests. The default is 1812. acct_port <udp_port_number 1-65535> – The UDP port number for accounting requests. The default is 1813.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To configure RADIUS server communication settings:

```
DGS-3224TGR:4#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-3224TGR:4#
```

config radius delete

Purpose	Used to delete a previously entered RADIUS server configuration.
Syntax	**config radius delete <server_index 1-3>**

config radius delete

Description	The config radius delete command is used to delete a previously entered RADIUS server configuration.
Parameters	<server_index 1-3> – Assigns a number to the current set of RADIUS server settings. Up to three groups of RADIUS server settings can be entered on the switch.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To delete previously configured RADIUS server communication settings:

```
DGS-3224TGR:4#config radius delete 1
Command: config radius delete 1

Success.

DGS-3224TGR:4#
```

config radius

Purpose	Used to configure the switch's RADIUS settings.
Syntax	**config radius <server_index 1-3> {ipaddress <server_ip> {ipaddress <server_ip>|key <passwd 32>|auth_port <udp_port_number 1-65535>|acct_port <udp_port_number 1-65535>}**

config radius	
Description	The config radius 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. <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 – Returns all of the ports in the range to their default RADIUS settings. auth_port <udp_port_number 1-65535> – The UDP port number for authentication requests. The default is 1812. acct_port <udp_port_number 1-65535> – The UDP port number for accounting requests. The default is 1813.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To configure RADIUS settings:

```
DGS-3224TGR:4#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-3224TGR:4#
```

show radius

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

Example Usage:

To display RADIUS settings on the switch:

```
DGS-3224TGR:4#show radius
Command: show radius

Index  IP Address       Auth-Port Number   Acct-Port Number   Status      Key
-----  ---------------  ---------          ---------          ----------  ----------
1      10.1.1.1         1812               1813               Active      switch
2      20.1.1.1         1800               1813               Active      des3250
3      30.1.1.1         1812               1813               Active      dlink

Total Entries : 3

DGS-3224TGR:4#
```

show 802.1x user	
Purpose	Used to display the current configuration of the 802.1x server on the switch.
Syntax	**show 802.1x user**
Description	The show 802.1x user command is used to display the current configuration of the 802.1x Port-based Network Access Control server application on the switch.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To show the 802.1x user:

```
DGS-3224TGR:4#show 802.1x user
Command: show 802.1x user

Index   UserName
-------  --------------------
1        ctsnow

DGS-3224TGR:4#
```

create 802.1x user	
Purpose	Used to create a new 802.1x user.
Syntax	**create 802.1x user <username 15>**
Description	The create 802.1x user command is used to create new 802.1x users.
Parameters	<username 15> – A username can be as

create 802.1x user	
	many as 15 alphanumeric characters.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To create an 802.1x user:

```
DGS-3224TGR:4#create 802.1x user ctsnow
Command: create 802.1x user ctsnow

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

DGS-3224TGR:4#
```

delete 802.1x user	
Purpose	Used to delete the switch's 802.1x users.
Syntax	**delete 802.1x user <username 15>**
Description	The delete 802.1x user command is used to delete 802.1x users.
Parameters	<username 15> – A username can be as many as 15 alphanumeric characters.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To delete 802.1x users:

```
DGS-3224TGR:4# delete 802.1x user
```

```
Command: delete 802.1x user ctsnow

Are you sure to delete the user?(y/n)
Success.

DGS-3224TGR:4#
```

show auth_statistics

Purpose	Used to display the switch's authentication statistics.
Syntax	**show auth_statistics** {**ports <portlist>**}
Description	The show auth_statistics command is used to display authentication statistics.
Parameters	ports <portlist> – Specifies a range of ports. The port list is specified by listing the beginning port number and the highest port number of the range. The beginning and end of the port list range are separated by a dash. For example, 3 would specify port 3. 4 specifies port 4. 3-4 specifies all of the ports between port 3 and port 4 – in numerical order.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To display authentication statistics:

```
DGS-3224TGR:4#show auth_statistics
Command: show auth_statistics
```

```
Port number  : 1

EapolFramesRx                0
EapolFramesTx                0
EapolStartFramesRx           0
EapolReqIDFramesTx           0
EapolLogoffFramesRx          0
EapolReqFramesTx             0
EapolRespIdFramesRx          0
EapolRespFramesRx            0
InvalidEapolFramesRx         0
EapLengthErrorFramesRx       0
LastEapolFrameVersion        0
LastEapolFrameSource         00-00-00-00-00-00

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

show auth_diagnostics

Purpose	Used to display the switch's authentication diagnostics statistics.
Syntax	**show auth_diagnostics** {**ports <portlist>**}
Description	The show auth_diagnostics command is used to display authentication diagnostics statistics.
Parameters	ports <portlist> – Specifies a range of ports. The port list is specified by listing the beginning port number and the highest port number of the range. The beginning and end of the port list range are separated by a dash. For example, 3 would specify port 3. 4 specifies port 4. 3-4 specifies all of the ports between port 3 and port 4 – in numerical order.
Restrictions	None.

Example Usage:

To display authentication diagnostics statistics:

```
DGS-3224TGR:4# show auth_diagnostics
Command: show auth_diagnostics

Port number    : 1


EntersConnecting                          0
EapLogoffsWhileConnecting                 0
EntersAuthenticating                      0
SuccessWhileAuthenticating                0
TimeoutsWhileAuthenticating               0
FailWhileAuthenticating                   0
ReauthsWhileAuthenticating                0
EapStartsWhileAuthenticating              0
EapLogoffWhileAuthenticating              0
ReauthsWhileAuthenticated                 0
EapStartsWhileAuthenticated               0
EapLogoffWhileAuthenticated               0
BackendResponses                          0
BackendAccessChallenges                   0
BackendOtherRequestsToSupplicant          0
BackendNonNakResponsesFromSupplicant      0
BackendAuthSuccesses                      0
BackendAuthFails                          0

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

show auth_session_statistics	
Purpose	Used to display the authentication session statistics.
Syntax	**show auth_session_statistics {ports <portlist>}**

show auth_session_statistic s	
Description	The show auth_session_statistics command is used to display the switch's authentication session statistics.
Parameters	ports <portlist> – Specifies a range of ports. The port list is specified by listing the beginning port number and the highest port number of the range. The beginning and end of the port list range are separated by a dash. For example, 3 would specify port 3. 4 specifies port 4. 3-4 specifies all of the ports between port 3 and port 4 – in numerical order.
Restrictions	None.

Example Usage:

To display authentication session statistics:

```
DGS-3224TGR:4# show auth_session_statistics
Command: show auth_session_statistics

Port number : 1

SessionOctetsRx                 0
SessionOctetsTx                 0
SessionFramesRx                 0
SessionFramesTx                 0
SessionId
SessionAuthenticMethod          Remote Authentication Server
SessionTime                     0
SessionTerminateCause           SupplicantLogoff
SessionUserName

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

show radius auth_client	
Purpose	Used to display the switch's RADIUS authentication client statistics.
Syntax	**show radius auth_client**
Description	The show radius auth_client command is used to display RADIUS authentication client statistics.
Parameters	None.
Restrictions	None.

Example Usage:

To display RADIUS authentication client statistics:

```
DGS-3224TGR:4# show radius auth_client
Command: show radius auth_client

radiusAuthClient ==>
radiusAuthClientInvalidServerAddresses        0
radiusAuthClientIdentifier                    D-Link


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 radius acct_client

Purpose	Used to configure the switch's RADIUS account client statistics.
Syntax	**show radius acct_client**
Description	The show radius acct_client command is used to display the switch's RADIUS account client statistics.
Parameters	None.
Restrictions	None.

Example Usage:

To display the RADIUS account client statistics:

```
DGS-3224TGR:4# show radius acct_client
Command: show radius acct_client

radiusAcctClient ==>
radiusAcctClientInvalidServerAddresses   0
radiusAcctClientIdentifier              D-Link


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
```

22

ACCESS CONTROL LIST (ACL) COMMANDS

The DGS-3224TGR implements Access Control Lists that enable the switch to deny network access to specific devices or device groups based on IP settings or MAC address.

Command	Parameters
create access_profile	ethernet vlan source_mac <macmask> destination_mac <macmask> 802.1p ethernet_type ip vlan source_ip_mask <netmask> destination_ip_mask <netmask> dscp tos icmp type code igmp type tcp src_port_mask <hex 0x0-0xffff>

Command	Parameters
	dst_port_mask <hex 0x0-0xffff> udp udp src_port_mask <hex 0x0-0xffff> dst_port_mask <hex 0x0-0xfff> protocol_id user_mask <hex 0x0-0xffffffff> permit deny profile_id <value 1-8>}
delete access_profile	profile_id <value 1-8>
config access_profile	profile_id <value 1-8> add access_id <value 1-255> ethernet vlan <vlan_name 32> source_mac <macaddr> destination_mac <macaddr> 802.1p <value 0-7> ethernet_type <hex 0x0-0xfff> ip vlan <vlan_name 32> source_ip <ipaddr> destination_ip <ipaddr> dscp <value 0-63>|tos <value 0-127> icmp type <value 0-255> code <value 0-255> igmp type <value 0-255> tcp src_port <value 0-65535> dst_prot <value 0-65535> udp src_port <value 0-65535> dst_port <value 0-65535>

Command	Parameters
	protocol_id <value 0-255> user_define <hex 0x0-0xffffffff> priority <value 0-7> replace_priority replace_dscp <value 0-63> delete <value 1-255>

Due to a chipset limitation, the switch currently supports a maximum of ten access profiles, each containing a maximum of 50 rules – with the additional limitation of 50 rules total for all ten access profiles.

Access profiles allow you to establish criteria to determine whether 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, and specify deny:

create access_profile ip source_ip_mask 255.255.255.0 profile_id 1 deny

Here we have created an access profile that will examine the IP field of each frame received by the switch. Each source IP address the switch finds will be combined with the source_ip_mask with a logical AND operation. The profile_id parameter is used to give the access profile an identifying number – in this case, 1. The deny parameter instructs the switch to filter any frames that meet the criteria – in this case,

when a logical AND operation between an IP address specified in the next step and the ip_source_mask match.

The default for an access profile on the switch is to permit traffic flow. If you want to restrict traffic, you must use the deny parameter.

Now that an access profile has been created, you must add the criteria the switch will use to decide if a given frame should be forwarded or filtered. Here, we want to filter any packets that have an IP source address between 10.42.73.0 and 10.42.73.255:

config access_profile profile_id 1 add access_id 1 ip source_ip 10.42.73.1

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.

create access_profile

Purpose	Used to create an access profile on the switch and to define which parts of each incoming frame's header the switch will examine. Masks can be entered that will be combined with the values the switch finds in the specified frame header fields. Specific values for the rules are entered using the config access_profile command, below.
Syntax	**create access_profile [ethernet {vlan|source_mac <macmask>|destination_mac <macmask> |802.1p|ethernet_type}|ip {vlan|source_ip_mask <netmask>|destination_ip_mask <netmask>|dscp <value 0-63>|tos <0-127>|[icmp {type|code}|igmp {type}|tcp {src_port_mask <hex 0x0-0xffff>|dst_port_mask <hex 0x0-0xffff>}|udp {src_port_mask <hex 0x0-0xfff>|dst_port_mask <hex 0x0-0xffff>}|protocol_id {user_mask <hex 0x0-0xffffffff>}]}]{[permit|deny]|profile_id <value 1-8>}**
Description	The create access_profile command is used to create an access profile on the switch and to define which parts of each incoming frame's header the switch will examine. Masks can be entered that will be combined with the values the switch finds in the specified frame header fields.

create access_profile

	Specific values for the rules are entered using the config 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 <macmask> – Specifies a MAC address mask for the source MAC address. This mask is entered in the following hexadecimal format,
	destination_mac <macmask> – Specifies a MAC address mask for the destination MAC address.
	802.1p – Specifies that the switch will examine the 802.1p priority value in the frame's header.
	ethernet_type – Specifies that the switch will examine the Ethernet type value in each frame's header.
	ip – Specifies that the switch will examine the IP address in each frame's header.
	vlan – Specifies a VLAN mask.
	source_ip_mask <netmask> – Specifies an IP address mask for the source IP address.
	destination_ip_mask <netmask> – Specifies an IP address mask for the destination IP address.

create access_profile

dscp <value 0-63> – Specifies that the switch will examine the DiffServ Code Point (DSCP) field in each frame's header.

tos <value 0-127>– Specifies that the switch will examine the Type of Service value 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.

udp – Specifies that the switch will examine each frame's Universal Datagram

create access_profile	
	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 – Specifies that the switch will examine each frame's Protocol ID field. user_mask <hex 0x0-0xffffffff> – Specifies that the rule applies to the IP protocol ID and the mask options behind the IP header. permit – Specifies that packets that match the access profile are permitted to be forwarded by the switch. deny – Specifies that packets that do not match the access profile are not permitted to be forwarded by the switch and will be filtered. profile_id <value 1-255> – Specifies an index number that will identify the access profile being created with this command.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To create an access profile that will deny service to the subnet ranging from 10.42.73.0 to 10.42.73.255:

```
DGS-3224TGR:4#create access_profile ip source_ip_mask
255.255.255.0 profile_id 1 deny
Command: create access_profile ip source_ip_mask
255.255.255.0 profile_id 1 deny

Success.

DGS-3224TGR:4#
```

delete access_profile

Purpose	Used to delete a previously created access profile.
Syntax	**delete access_profile [profile_id <value 1-255>]**
Description	The delete access_profile command is used to delete a previously created access profile on the swtich.
Parameters	profile_id <value 1-255> – An integer between 1 and 255 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.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To delete the access profile with a profile ID of 1:

```
DGS-3224TGR:4#delete access_profile profile_id 1
Command: delete access_profile profile_id 1

Success.

DGS-3224TGR:4#
```

config access_profile

Purpose	Used to configure an access profile on the switch and to define specific values that will be used to by the switch to determine if a given packet should be forwarded or filtered. Masks entered using the create access_profile command will be combined, using a logical AND operation, with the values the switch finds in the specified frame header fields. Specific values for the rules are entered using the config access_profile command, below.
Syntax	**config access_profile profile_id <value 1-255> [add access_id <value 1-255>] [ethernet {vlan <vlan_name 32>|source_mac <macaddr>|destination_mac <macaddr>|802.1 <value 0-7>|ethernet_type <hex 0x0-0xffff}|ip{vlan <vlan_name>|source_ip <ipaddr>|destination_ip <ipaddr>|dscp <value 0-63>|[icmp {type <value 0-65535> code <value 0-255>}|igmp {type <value 0-255>}|tcp {src_port <value 0-65535>|dst_port <value 0-65535>}| udp {src_port <value 0-65535>|dst_port**

config access_profile

	<value 0-65535>}|protocol_id <value 0-255> {user_define <hex 0x0-0xffffffff>}]}]{priority <value 0-7> {replace_priority}|replace_dscp <value 0-63>}|delete <value 1-255>]
Description	The config access_profile command is used to configure an access profile on the switch and to enter specific values that will be combined, using a logical AND operation, with masks entered with the create access_profile command, above.
Parameters	profile_id <value 1-255> – add access_id <value 1-255> – Adds an additional rule to the above specified access profile. The value specifies the relative priority of the additional rule. A lower access ID, the higher the priority the rule will be given. 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> – Specifies that the access profile will apply to only packets with this source MAC address. destination_mac <macaddr> – Specifies that the access profile will apply to only packets with this destination MAC address.

config access_profile

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 hexidecimal 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 to this VLAN.

source_ip <ipaddr> – Specifies that the access profile will apply to only packets with this source IP address.

destination_id <value 0-255> – Specifies that the access profile will apply to only packets with this destination IP address.

dscp <value 0-63> – Specifies that the access profile will apply only to packets that have this value in their Type-of-Service (DiffServ code point, DSCP) field in their IP packet header.

icmp – Specifies that the switch will examine the Internet Control Message Protocol (ICMP) field within each packet.

type <value 0-65535> – Specifies that the access profile will apply to this ICMP type value.

code <value 0-255> – Specifies that the

config access_profile

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 exmamine 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 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

config access_profile	
	field in each packet and if this field contains the value entered here, apply the following rules. user_define <hex 0x0-0xffffffff> – Specifies a mask to be combined with the value found in the frame header using a logical AND operaiton. priority <value 0-7> – Specifies that the access profile will apply to packets that contain this value in their 802.1p priority field of their header. replace_priority – This parameter is specified if you want to change the 802.1p user priority of a packet that meets the specified criteria. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being transmitted from 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. delete <value 1-255> – Specifies that the access ID of a rule you want to delete.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To configure the access profile with the profile ID of 1 to filter frames that have IP addresses in the range between 10.42.73.0 to 10.42.73.255:

```
DGS-3224TGR:4#config access_profile profile_id 1 add access_id
1 ip source_ip 10.42.73.1
Command: config access_profile profile_id 1 add access_id 1 ip
source_ip 10.42.73.1

Success.

DGS-3224TGR:4#
```

show access_profile

Purpose	Used to display the currently configured access profiles on the switch.
Syntax	**show access_profile**
Description	The show access_profile command is used to display the currently configured access profiles
Parameters	None.
Restrictions	None.

Example Usage:

To display all of the currently configured access profiles on the switch:

```
DGS-3224TGR:4#show access_profile
Command: show access_profile
```

```
Access Profile Table

Access Profile  ID:1                                Mode : Deny
                                                   TYPE : IP
==================================================
MASK  Option  Source IP MASK
                  255.255.255.0
------------------  ---------------------
Access ID
------------------  ---------------------
1                   10.42.73.0
```

23

SSH COMMANDS

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

Command	Parameters
config ssh algorithm	[3DES|Blowfish|MD5|SHA1| DSA|RSA] [enable|disable]
show ssh algorithm	
config ssh authmode	[password |publickey| hostbased] [enable|disable]
show ssh authmode	
config ssh user	<username> authmode [Publickey |Password | Hostbased [host_name <domain_name 32> |hostname_IP <domain_name 32> <ipaddr>]]
show ssh user	
config ssh server	{maxsession <int 1-8>| contimeout <min 2-20> | authfail <int 2-20> |rekey [10min |30min | 60min |never]}
show ssh server	
enable ssh	

Command	Parameters
disable ssh	

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

config ssh algorithm

Purpose	Used to configure the SSH algorithm.
Syntax	**config ssh algorithm [3DES|Blowfish|MD5|SHA1|DSA|RSA] [enable|disable]**
Description	This command allows you to configure the desired type of SSH algorithm.
Parameters	[3DES|Blowfish|MD5|SHA1|DSA|RSA] – Choose the desired security algorithm. [enable|disable] – This allows you to enable or disable the SSH algorithm.
Restrictions	Only administrator-level users can issue this command.

Usage Example:

To configure SSH algorithm:

```
DGS-3224TGR:4#config ssh algorithm Blowfish enable
Command: show ssh algorithm Blowfish enable

Success.
```

```
DGS-3224TGR:4#
```

show ssh algorithm

Purpose	Used to display the SSH algorithm setting.
Syntax	**show ssh algorithm**
Description	This command will display the current SSH algorithm setting status.
Parameters	None.
Restrictions	None.

Usage Example:

To display the SSH algorithm:

```
DGS-3224TGR:4#show ssh algorithm
Command: show ssh algorithm

Encryption Algorithm
MD5         : Enabled
SHA         : Enabled
DSA         : Enabled
RSA         : Enabled
3DES        : Enabled
Blowfish    : Enabled

DGS-3224TGR:4#
```

config ssh authmode	
Purpose	Used to configure the SSH authentication mode setting.
Syntax	**config ssh authmode [password |publickey|hostbased] [enable|disable]**
Description	This command will allow you to configure the SSH authentication mode.
Parameters	[password |publickey|hostbased] – Choose the desired SSH authentication mode. [enable|disable] – This allows you to enable or disable SSH authentication.
Restrictions	Only administrator-level users can issue this command.

Usage Example:

To display the SSH algorithm:

```
DGS-3224TGR:4#show ssh algorithm
Command: show ssh algorithm

Encryption Algorithm
MD5          : Enabled
SHA1         : Enabled
DSA          : Enabled
RSA          : Enabled
3DES         : Enabled
Blowfish     : Enabled
```

```
DGS-3224TGR:4#
```

show ssh authmode

Purpose	Used to display the SSH authentication mode setting.
Syntax	**show ssh authmode**
Description	This command will allow you to display the current SSH authentication mode.
Parameters	None.
Restrictions	None.

Usage Example:

To display the SSH authmode:

```
DGS-3224TGR:4#show ssh authmode
Command: show ssh authmode

Authentication Algorithm
Hostbased  : Enabled
Password   : Enabled
Publickey  : Enabled

DGS-3224TGR:4#
```

config ssh user

config ssh user	
Purpose	Used to configure the SSH user.
Syntax	**config ssh user <username> authmode [Publickey |Password|Hostbased [host_name <domain_name 32>|hostname_IP <domain_name 32> <ipaddr>]]**
Description	This command allows you to modify the parameters of the SSH user.
Parameters	<username> – Enter an optional SSH user name. authmode – Select the type of security authentication mode: [Publickey |Password |Hostbased [host_name <domain_ name 32>|hostname_IP <domain_name 32> <ipaddr>]] .
Restrictions	Only administrator-level users can issue this command.

Usage Example:

To configure the SSH user:

```
DGS-3224TGR:4#config ssh user Sibyl authmode Hostbased
hostname_IP 172.18.211.200
Command: config ssh user Sibyl authmode Hostbased
 hostname_IP 172.18.211.200

Success.
```

```
DGS-3224TGR:4#
```

show ssh user

Purpose	Used to display the SSH user setting.
Syntax	**show ssh user**
Description	This command allows you to display the current SSH user setting.
Parameters	None.
Restrictions	None.

Usage Example:

To display the SSH user:

```
DGS-3224TGR:4#show ssh user
Command: show ssh user

Account is empty!

DGS-3224TGR:4#
```

config ssh server

Purpose	Used to configure the SSH server.
Syntax	**config ssh server** {**maxsession <int 1-8>| contimeout <min 2-20> | authfail <int 2**-

config ssh server	
	contimeout <min 2-20> | authfail <int 2-20> |rekey [10min |30min | 60min |never]}
Description	This command allows you to configure the SSH server.
Parameters	maxsession <int 1-8> – Allows the user to set the number of times an outside guest may attempt to log on to the switch. contimeout <min 2-20> – Allows the user to set the connection timeout. authfail <int 2-20> – Allows the user to set the maximum number of authentication fail attempts. rekey [10min |30min | 60min |never] – Sets the time period that the switch will change the security shell encryptions.
Restrictions	Only administrator-level users can issue this command.

Usage Example:

To configure the SSH server:

```
DGS-3224TGR:4#config ssh server maxsession 8 contimeout 300
authfail 2
Command: config ssh server maxsession 8 contimeout 300 authfail
 2

Success.
```

```
DGS-3224TGR:4#
```

show ssh server

Purpose	Used to display the SSH server setting.
Syntax	**show ssh server**
Description	This command allows you to display the current SSH server setting.
Parameters	None.
Restrictions	None.

Usage Example:

To display the SSH server:

```
DGS-3224TGR:4#show ssh server
Command: show ssh server

The SSH server configuration
Max Session             : 8
Connection Timeout   : 300
Authfail Attempts      : 2
Rekey Timeout          : 60min

DGS-3224TGR:4#
```

enable ssh

enable ssh	
Purpose	Used to enable SSH.
Syntax	**enable ssh**
Description	This command allows you to enable SSH on the switch.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Usage Example:

To enable SSH:

```
DGS-3224TGR:4#enable ssh
Command: enable ssh

Success.

DGS-3224TGR:4#
```

disable ssh	
Purpose	Used to disable SSH.
Syntax	**disable ssh**
Description	This command allows you to disable SSH on the switch.
Parameters	None.

disable ssh	
Restrictions	Only administrator-level users can issue this command.

Usage Example:

To disable SSH:

```
DGS-3224TGR:4#disable ssh
Command: disable ssh

Success.

DGS-3224TGR:4#
```

24

TACACS COMMANDS

The Terminal Access Controller Access Control System (TACACS) protocol commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameters
create authentication login method_list_name	<method_list_name>
config authentication login	[default | method_list_name <method_list_name>] method <string> {<string> {<string> {<string>}}}
show authentication login	[default | method_list_name <method_list_name>]
delete authentication login	[default| method_list_name <method_list_name>]
config login_authentication	{console[default| method_list_name <method_list_name>] |telnet[default| method_list_name <method_list_name>] |all[default| method_list_name <method_list_name>]}
show	

Command	Parameters
login_authentication	
enable authentication_policy	{maxsession <int 1-8>| contimeout <min 2-20> | authfail <int 2-20> |rekey [10min |30min | 60min |never]}
disable authentication_policy	
show authentication_policy	
create authentication server_group	<string 15>
config authentication server_group	<string 15> [add | delete] server_host <ip_address> protocol [tacacs|xtacacs]
delete authentication server_group	<string 15>
show authentication server_group	{<string 15>}
create authentication server_host	<ip_address> protocol [tacacs|xtacacs]
config authentication server_host	<server_ip> protocol [tacacs|xtacacs] {port <int 1-65535> | key <key_string 254> | timeout <int 1-255> | retransmit<int 1-255>}
delete authentication server_host	<ip_address> protocol [tacacs|xtacacs]
show authenticationa server_host	
config login_authentication response_timeout	<int 1-255>
config login_authentication attempt	<int 1-255>

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

create authentication login method_list_name	
Purpose	Used to create authentication login method list database.
Syntax	**create authentication login method_list_name <method_list_name>**
Description	This command configuration the authentication login method list database.
Parameters	<method_list_name> – The list name you want to configure.
Restrictions	Only administrator-level users can issue this command.

Usage Example:

To create an authentication login method list:

```
DGS-3224TGR:4# create authentication login method_list_name
list1
Command: create authentication login method_list_name list1

Success.

DGS-3224TGR:4#
```

config authentication login	
Purpose	Used to configure the authentication login method list database.
Syntax	**config authentication login [default | method_list_name <method_list_name>]** **method <string> {<string> {<string> {<string>}}}**
Description	This command configures the authentication login method list database.
Parameters	<method_list_name> – The list name you want to configuration. <string> – The method you want to add to the list.
Restrictions	Only administrator-level users can issue this command.

Usage Example:

To configure the authentication login method list database:

```
DGS-3224TGR:4#config authentication login method_list_name
list1 method group1 local
Command: config authentication login method_list_name list1
 method group1 local

Success.

DGS-3224TGR:4#

DGS-3224TGR:4#
```

show authentication login

Purpose	Used to show the authentication login method from the database.
Syntax	**show authentication login [default | method_list_name <method_list_name>]**
Description	This command displays the authentication login method from the database.
Parameters	<method_list_name> – The list name you want to show.
Restrictions	None.

Usage Example:

To display the authentication login:

```
DGS-3224TGR:4# show authentication login method_list_name
list1
Command: show authentication login method_list_name list1

method list name: list1
entry[0], method= 602, srv_group name=group1
entry[1], method= 1102, srv_group name=local
entry[2], method=     0, srv_group name=
entry[3], method=     0, srv_group name=

DGS-3224TGR:4#
```

delete authentication login

delete authentication login

Purpose	Used to delete a login authentication method.
Syntax	**delete authentication login [default| method_list_name <method_list_name>]**
Description	This command deletes an authentication method from the database.
Parameters	<method_list_name> – The list name you want to delete.
Restrictions	Only administrator-level users can issue this command.

Usage Example:

To delete authentication login:

```
DGS-3224TGR:4# delete authentication login method_list_name
list1
Command: delete authentication login method_list_name list1

Success.

DGS-3224TGR:4#
```

config login_authentication

Purpose	Used to set authentication methods of login applications.

config login_authentication

Syntax	**config login_authentication {console[default|method_list_name <method_list_name>]|telnet[default|method_list_name <method_list_name>]|all[default|method_list_name <method_list_name>]}**
Description	Set Authentication methods of login applications.
Parameters	<method_list_name> – The list name you want to configure.
Restrictions	Only administrator-level users can issue this command.

Usage Example:

To configure login authentication method:

```
DGS-3224TGR:4#config login_authentication console
method_list_name list1
Command: config login_authentication console method_list_name
 list1

Success.

DGS-3224TGR:4#
```

show login_authentication

Purpose	Used to show the authentication method list database.

show login_authentication	
	list database.
Syntax	**show login_authentication**
Description	This shows the authentication method when logging in.
Parameters	None.
Restrictions	None.

Usage Example:

To display the authentication method at login:

```
DGS-3224TGR:4#show login_authentication
Command: show login_authentication

CONSOLE    :list1 .
TELNET     :default .

The amount of time for login input is 100 seconds!
The maximum attempts for Login authentication is 5 !

DGS-3224TGR:4#
```

enable authentication_policy	
Purpose	Used to enable the AAA module to authentication at login.
Syntax	**enable authentication_policy**

enable authentication_policy	
Description	This command enables the AAA module.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Usage Example:

To enable authentication policy:

```
DGS-3224TGR:4#enable authentication_policy
Command: enable authentication_policy

Success.

DGS-3224TGR:4#
```

disable authentication_policy	
Purpose	Used to disable the AAA module at login.
Syntax	**disable authentication_policy**
Description	This command disables the AAA module.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Usage Example:

To disable authentication policy:

```
DGS-3224TGR:4# disable authentication_policy
Command: disable authentication_policy

Success.

DGS-3224TGR:4#
```

show authentication_policy

Purpose	Used to show if the AAA module is enabled.
Syntax	**show authentication_policy**
Description	This command shows the status of the AAA module.
Parameters	None.
Restrictions	None.

Usage Example:

To display the AAA module status:

```
DGS-3224TGR:4# show authentication_policy
Command: show authentication_policy

AAA is disabled!

DGS-3224TGR:4#
```

create authentication server_group	
Purpose	Used to create a new authentication server group.
Syntax	**create authentication server_group <string 15>**
Description	This command creates a new server group.
Parameters	<string 15> – The name of the newly created group. It must be 15 characters or less.
Restrictions	Only administrator-level users can issue this command.

Usage Example:

To create an authentication server group:

```
DGS-3224TGR:4#create authentication server_group group1
Command: create authentication server_group group1

Success.

DGS-3224TGR:4#
```

config authentication server_group	
Purpose	Used to configuration an authentication server group.
Syntax	**config authentication server_group <string 15> [add | delete] server_host**

config authentication server_group	
	<server_ip> protocol [tacacs|xtacacs]
Description	This command adds or deletes a server host to or from a server group.
Parameters	<string 15> – The name of 15 characters or less of the group to be configured. <server_ip> – The IP address of the host to be added or deleted to or from the group.
Restrictions	Only administrator-level users can issue this command.

Usage Example:

To configure an authentication server group:

```
DGS-3224TGR:4# config authentication server_group group1 add
server_host 172.18.211.26 protocol tacacs
Command: config authentication server_group group1 add
 server_host 172.18.211.26 protocol tacacs

Success.

DGS-3224TGR:4#
```

delete authentication server_group	
Purpose	Used to delete an AAA server group from the group list.
Syntax	**delete authentication server_group <string 15>**

delete authentication server_group	
	<string 15>
Description	This command deletes a server group from the group list.
Parameters	<string 15> – The group name you want to delete. It must be 15 characters or less.
Restrictions	Only administrator-level users can issue this command.

Usage Example:

To delete an authentication server group:

```
DGS-3224TGR:4# delete authentication server_group group1
Command: delete authentication server_group group1

Success.

DGS-3224TGR:4#
```

show authentication server_group	
Purpose	Used to show an existing server group.
Syntax	**show authentication server_group {<string 15>}**
Description	This command shows the server group in the group list.
Parameters	<string 15> – This optional parameter indicates the group you want to see. If this

show authentication server_group	
	indicates the group you want to see. If this is not set, the switch will show all the server groups.
Restrictions	None.

Usage Example:

To show authenticated server groups:

```
DGS-3224TGR:4#show authentication server_group group1
Command: show authentication server_group group1

Group:  group1
      IP Addresss                Protocol
   ----------------------      ----------------
      172.18.211.26             TACACS
      172.18.211.26             XTACACS

DGS-3224TGR:4#
```

create authentication server_host	
Purpose	Used to create an AAA server host.
Syntax	**create authentication server_host <server_ip> protocol [tacacs|xtacacs]**
Description	This command create an authentication login server host.
Parameters	<server_ip> – The host's IP address.

create authentication serve :_host	
Restrictions	Only administrator-level users can issue this command.

Usage Example:

To create an authentication server host:

```
DGS-3224TGR:4# create authentication server_host 172.18.211.28
protocol tacacs
Command: create authentication server_host 172.18.211.28
 protocol tacacs

Success.

DGS-3224TGR:4#
```

config authentication serve :_host	
Purpose	Used to configure an AAA server host.
Syntax	**config authentication server_host <server_ip> protocol [tacacs|xtacacs] {port <int 1-65535> | key <key_string 254> | timeout <int 1-255> | retransmi <int 1-255>}**
Description	This command creates an authentication login server host.
Parameters	<server_ip> – The host's IP address. <int 1-65535> – The port on which the server waitS for the request packet. The

config authentication serve ' _host	
	default is 49. <key_string 254> – Used to encrypt. <int 1-255> – The maximum time to wait for the response. The default is 5 seconds. <int 1-255> – The maximum retransmit time of the request packet. The default is 2 times.
Restrictions	Only administrator-level users can issue this command.

Usage Example:

To configure an authentication server host:

```
DGS-3224TGR:4# config authentication server_host  172.18.211.28
protocol tacacs port 49 timeout 3 retransmit 2
Command: config authentication server_host  172.18.211.28
 protocol tacacs port 49 timeout 3 retransmit 2

Success.

DGS-3224TGR:4#
```

delete authentication serve ' _host	
Purpose	Used to delete an AAA server host from the list.
Syntax	**delete authentication server_host <server_ip> proto [tacacs|xtacacs]**

delete authentication server_host	
	<server_ip> proto [tacacs)|xtacacs]
Description	This command delete a existing authentication server host from the host list.
Parameters	<server_ip> – The IP address of the server host you want to remove.
Restrictions	Only administrator-level users can issue this command.

Usage Example:

To delete an authentication server host:

```
DGS-3224TGR:4# delete authentication server_host 172.18.211.28
proto tacacs
Command: delete authentication server_host 172.18.211.28 proto
 tacacs

Success.

DGS-3224TGR:4#
```

show authentication server_host	
Purpose	Used to show the server host in the host list.
Syntax	**show authentication server host**
Description	This command shows the authentication server host in the list.

show authentication server_ host	
	server host in the list.
Parameters	None.
Restrictions	None.

Usage Example:

To show authenticated server hosts:

```
DGS-3224TGR:4# show authentication server host
Command: show authentication server host

IP Addresss      Protocol    Port   timeout     retransmit    key
-----------------  ----------  -------  -----------  ---------------  -----
172.18.211.26    TACACS    49       2            2
172.18.211.26    XTACACS   49       3            2

DGS-3224TGR:4#
```

config login_ uthentication response_timeout	
Purpose	Used to set the maximum time at input.
Syntax	**config login_authentication response_timeout <int 1-255>**
Description	This command sets the maximum time when waiting for the input.
Parameters	<int 1-255> – The maximum time value to wait, in seconds.

config login_authentication response_timeout	
Restrictions	Only administrator-level users can issue this command.

Usage Example:

To configure the login authentication response timeout:

```
DGS-3224TGR:4# config login_authentication response_timeout 20
Command: config login_authentication response_timeout 20

Success.

DGS-3224TGR:4#
```

config login_authentication attempt	
Purpose	Used to set the login attempt times.
Syntax	**config login_authentication response_timeout <int 1-255>**
Description	This command sets the maximum attempt times at login.
Parameters	<int 1-255> – The maximum time for attempts, in seconds.

config login_authentication attempt	
Restrictions	Only administrator-level users can issue this command.

Usage Example:

To configure login authentication attempts:

```
DGS-3224TGR:4# config login_authentication response_timeout 3
Command: config login_authentication response_timeout 3

Success.

DGS-3224TGR:4#
```

25

TRAFFIC SEGMENTATION COMMANDS

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

Command	Parameters
config traffic_segmentation	<portlist> forward_list [null | <portlist>]
show traffic_segmentation	{<portlist>}

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

config traffic_segmentation

Purpose	Used to configure the traffic segmentation.

config traffic_segmentation	
Syntax	**config traffic_segmentation <portlist> forward_list [null | <portlist>]**
Description	This command configures traffic segmentation.
Parameters	<portlist> – Specifes a range of ports to be configured. forward_list – Specifies a range of ports in the forwarding domain. The choices are: portlist, which specifes a range of ports to be configured and null, which specifies the range of ports in the forwarding domain is null.
Restrictions	Only administrator-level users can issue this command. The forwarding domain is restricted to Bridge Traffic only.

Usage Example:

To configure traffic segmentation:

```
DGS-3224TGR:4# config traffic_segmentation 1-3 forward_list 11-15
Command: config traffic_segmentation 1-3 forward_list 11-15

Success.

DGS-3224TGR:4#
```

show traffic_segmentation

Purpose	Used to display the current traffic segmentation table.
Syntax	**show traffic_segmentation {<portlist>}**
Description	This command displays the current traffic segmentation table.
Parameters	<portlist> – Specifes a range of ports to be displayed. If no parameter is specified, the system will display all current traffic segmentation tables.
Restrictions	None.

Usage Example:

To display the traffic segmentation table:

```
DGS-3224TGR:4# show traffic_segmentation 1-3
Command: show traffic_segmentation 1-3

Traffic Segmentation Table

Port        Forward  Portlist
--------    ------------------------------------------------------------------------------
1           11-15
2           11-15
3           11-15

DGS-3224TGR:4#
```

26

COMMAND HISTORY LIST

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

Command	Parameters
?	
show command_history	
dir	
config command_history	<value>

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

?	
Purpose	Used to display all commands in the Command Line Interface (CLI).
Syntax	?

?	
Description	This command will display all of the commands available through the Command Line Interface (CLI).
Parameters	None.
Restrictions	None.

Usage Example:

To display all of the commands in the CLI:

```
DGS-3224TGR:4#?
Command: ?

..
?
clear
clear arptable
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_parameter ports
config 802.1x auth_protocol
config 802.1x capability ports
config 802.1x init ports
config 802.1x reauth ports
config access_profile profile_id
config account
config arp_aging time
config authentication login
```

```
config authentication server_group
config authentication server_host
config bandwidth_control
CTRL+C ESC q Quit SPACE n Next Page Enter Next Entry a All
```

show command_history

Purpose	Used to display the command history.
Syntax	**show command_history**
Description	This command will display the command history.
Parameters	None.
Restrictions	None.

Usage Example:

To display the command history:

```
DGS-3224TGR:4#show command_history
Command: show command_history

?
? show
show vlan
config router_ports vlan2 add 1:1-1:10
config router_ports vlan2 add
config router_ports vlan2
config router_ports
show vlan
create vlan vlan2 tag 3
create vlan vlan2 tag 2
```

```
show router_ports
show router ports
login
DGS-3224TGR:4#
```

dir	
Purpose	Used to display all commands.
Syntax	**dir**
Description	This command will display all commands.
Parameters	None.
Restrictions	None.

Usage Example:

To display all of the commands:

```
DGS-3224TGR:4#dir
Command: dir

..
?
clear
clear arptable
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_parameter ports
config 802.1x auth_protocol
config 802.1x capability ports
config 802.1x init ports
config 802.1x reauth ports
config access_profile profile_id
config account
config arp_aging time
config authentication login
config authentication server_group
config authentication server_host
config bandwidth_control
CTRL+C ESC q Quit SPACE n Next Page Enter Next Entry a All
```

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> – This value represents the number of commands to be displayed.
Restrictions	None.

Usage Example:

To configure the command history:

```
DGS-3224TGR:4#config command_history 20
```

```
Command: config command_history 20

Success.

DGS-3224TGR:4#
```

A

TECHNICAL SPECIFICATIONS

	General	
Standards:	IEEE 802.3 10BASE-T Ethernet IEEE 802.3u 100BASE-TX Fast Ethernet IEEE 802.3z 1000BASE-SX Gigabit Ethernet IEEE 802.1 P/Q VLAN IEEE 802.3x Full-duplex Flow Control ANSI/IEEE 802.3 Nway auto-negotiation	
Protocols:	CSMA/CD	
Data Transfer Rates: Ethernet Fast Ethernet Gigabit Ethernet	Half-duplex 10 Mbps 100Mbps n/a	Full-duplex 20Mbps 200Mbps 2000Mbps
Topology:	Star	

General	
Network Cables: 10BASE-T:	2-pair UTP Cat. 3,4,5 (100 m) EIA/TIA- 568 100-ohm STP (100 m)
100BASE-TX:	2-pair UTP Cat. 5 (100 m) EIA/TIA-568 100-ohm STP (100 m)
Fiber Optic:	IEC 793-2:1992 Type A1a – 50/125um multimode Type A1b - 62.5/125um multimode Both types use MTRJ or SC optical connector
Number of Ports:	24 x 10/100/1000 Mbps NWay ports 4 GBIC combo ports

Physical and Envi onmental	
AC Inputs:	100 - 240 VAC, 50/60 Hz (internal universal power supply)
Power Consumption:	60 watts maximum
DC Fans:	4 built-in 40 x 40 x 10 mm fans 1 built-in 60 x 60 x 18 mm 5400 RPM fan blower
Operating Temperature:	0 to 40 degrees Celsius
Storage Temperature:	-25 to 55 degrees Celsius
Humidity:	Operating: 5% to 95% RH non-condensing
Dimensions:	441(W) x 309(D) x 44mm(H), 19-inch rack-mount width, 1U height

Physical and Environmental	
	rack-mount width 1U height
Weight:	4 kg
EMI:	FCC Class A, CE Mark Class A, BSMI Class A, C-Tick Class A
Safety:	CSA International

Performance	
Transmission Method:	Store-and-forward
RAM Buffer:	2 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 16K MAC address
Priority Queues:	8 Priority Queues per port
Forwarding Table Age Time:	Max age:10–1000000 seconds. Default = 300.