D-Link®

DGS-3224SR
Stackable Ethernet Switch

Command Line Interface Reference Manual

October 2003
PN 6GS3224SRC01
Printed In Taiwan

RECYCLABLE

Trademarks

Copyright Statement

Table of Contents

Introduction 5

Using the Console CLI 10

Command Syntax 18

Basic Switch Commands 23

Switch Port Commands 44

Network Management Commands 49

Utility Commands 89

Network Monitoring Commands 93

Spanning Tree Commands 109

Layer 2 Forwarding Database Commands 120

Broadcast Storm Control Commands 131

ARP Commands 135

QOS Commands 139

Port Mirroring Commands 157

VLAN Commands 164

Link Aggregation Commands 174
IP Interface Commands 185
IGMP Snooping Commands 189
802.1X Commands 204
Access Control List (ACL) Commands 229
Traffic Segmentation Commands 244
Stacking Commands 248
Routing Table Commands 255
ARP Command 259
SNTP Commands 261
Port Security Commands 272
Jumbo Frame Commands 277
Technical Specifications 280

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:

- 115200 baud
- no parity
- 8 data bits
- 1 stop bit
- no flow control

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.

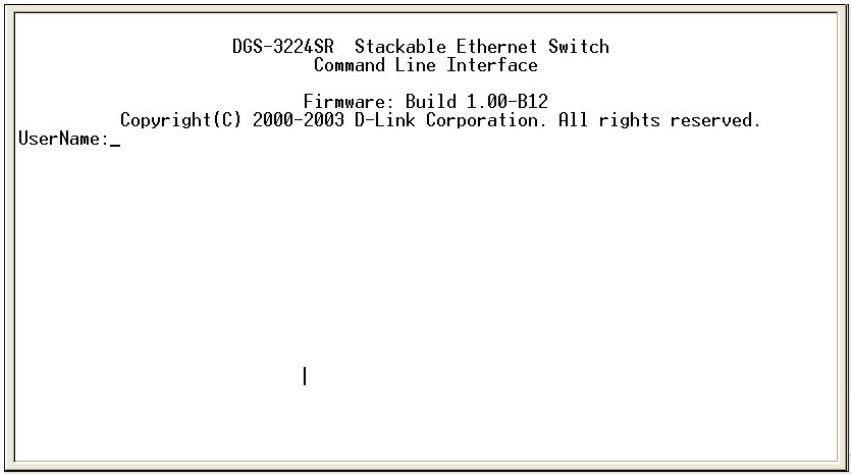

Figure 1-1. Initial Console screen.

There is no initial username or password. Just press the **Enter** key twice to display the CLI input cursor – **DGS-3224SR: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. This MAC address cannot be changed, and can be found from the initial boot console screen – shown below.

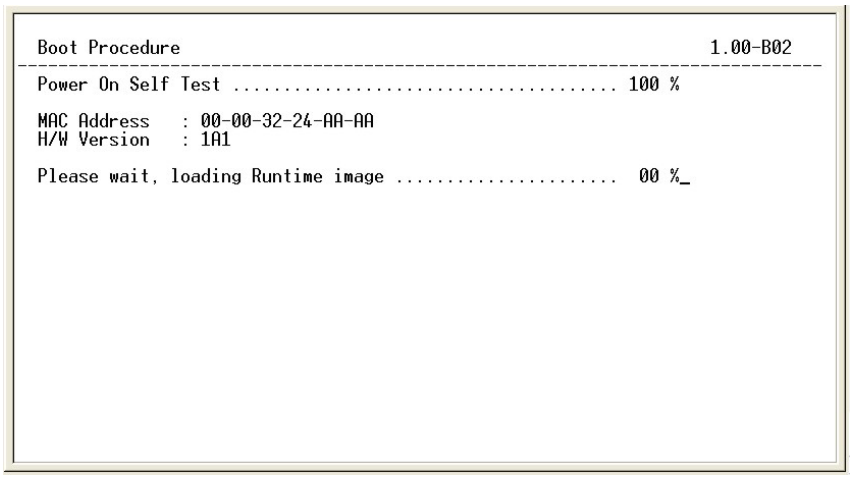

Figure 1-2. Boot Screen

The switch's MAC address can also 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-3224SR: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 **DGS3224SR: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.

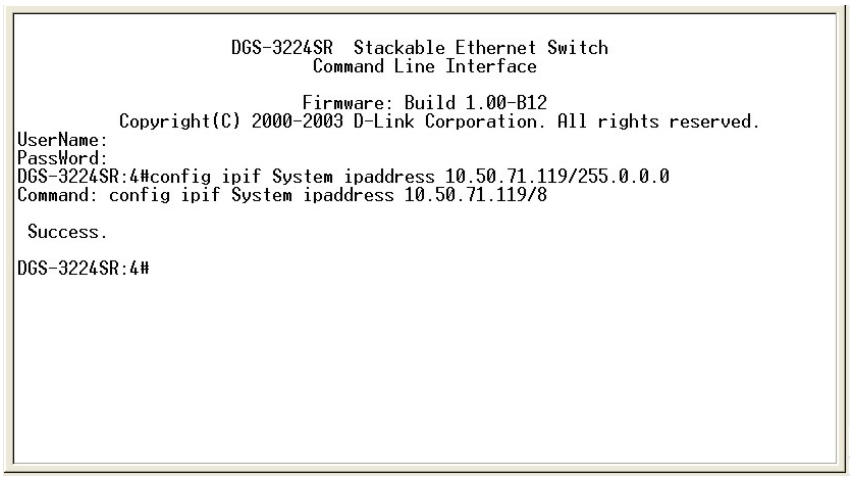

Figure 1-3. Assigning the Switch an IP Address

In the above example, the switch was assigned an IP address of 10.50.71.119 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-3224SR 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
- 115200 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:

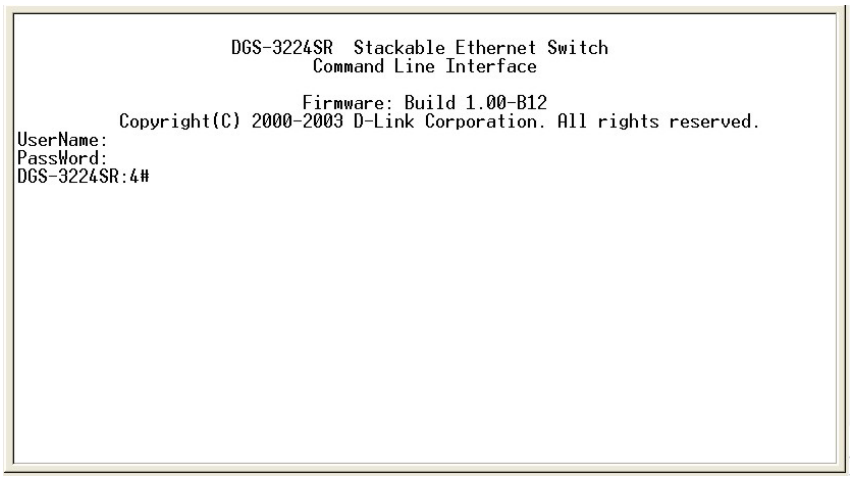

Figure 2-1. Initial Console Screen

Commands are entered at the command prompt, **DGS-3224SR: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.

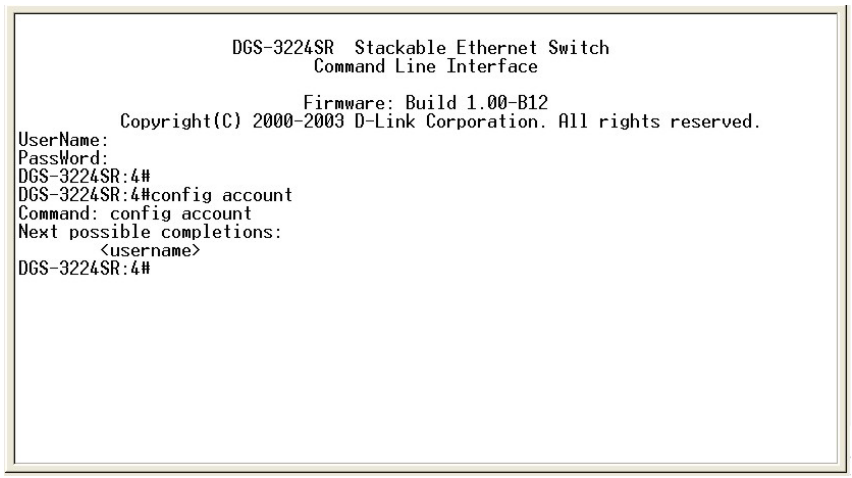

Figure 2-3. Example Command Parameter Help

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.

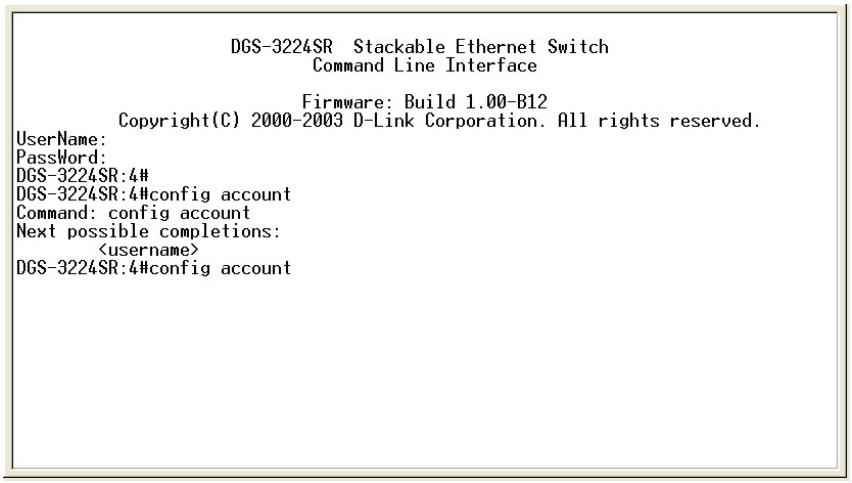

Figure 2-4. Using the Up Arrow to Re-enter a Command

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.

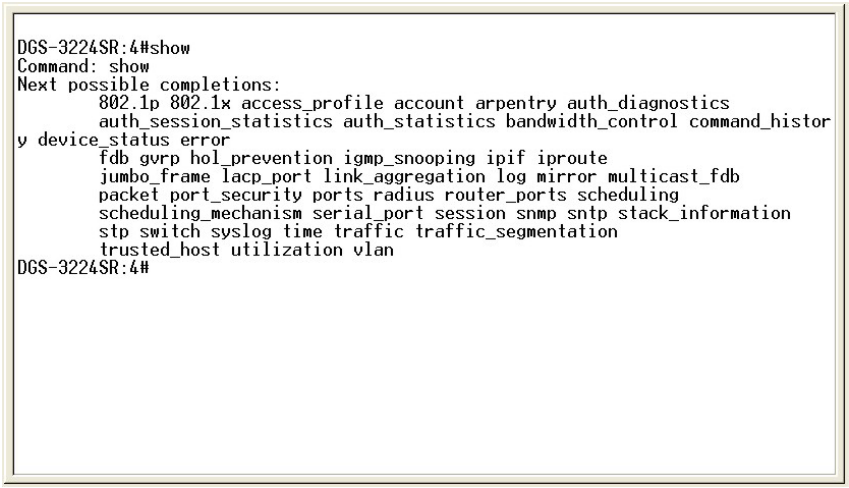

Figure 2-6. Next possible completions: Show Command

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	Enclose a variable or value that must be specified.
Syntax	**create ipif <ipif_name> vlan <vlan_name> ipaddress <network_address>**
Description	In the above syntax example, you must supply an IP interface name in the <ipif_name> space, a VLAN name in the <vlan_name> space, and the network address in the <network_address> space. Do not type the angle brackets.
Example Command	**create ipif Engineering vlan Design ipaddress 10.42.73.1/255.0.0.0**

[square brackets]	
Purpose	Encloses a required value or set of required arguments. One or more values or arguments can be specified.
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.
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.

| vertical bar	
Example Command	**show snmp community**

{braces}	
Purpose	Encloses an optional value or set of optional arguments.
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 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.

Line Editing Key Usage	
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.
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 115200 auto_logout(2) [never(0)|2_minutes(2)|5_minutes(5) |10_minutes(10)|15_minutes(15)]}(1)
enable clipaging	
disable clipaging	
enable telnet	{<tcp_port_number 1-65535>}
disable telnet	

Command	Parameters
enable web	{<tcp_port_number 1-65535>}
disable web	
save	
reboot	
reset	{config|system}
login	
logout	

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.
Parameters	Admin <username> User <username>
Restrictions	Only Administrator-level users can issue this command. Usernames can be between 1 and 15 characters.

create account

	Passwords can be between 0 and 15 characters.

Example Usage:

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

```
DGS-3224SR: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-3224SR:4#
```

config account

Purpose	Used to configure user accounts
Syntax	**config account <username>**
Description	The config account command configures a user account that has been created using the **create account** command.
Parameters	<username>
Restrictions	Only Administrator-level users can issue this command.

config account

	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-3224SR: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-3224SR:4#
```

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.

show account

Restrictions	none.

Example Usage:

To display the accounts that have been created:

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

Current Accounts:
  Username         Access Level
  ---------------  ------------
  System           user
  dlink            Admin
DGS-3224SR:4#
```

delete account

Purpose	Used to delete an existing user account
Syntax	**delete account <username>**
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-3224SR:4#delete account System
Command: delete account System

 Success.

DGS-3224SR: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
Restrictions	none.

Example Usage:

To display the way that the users logged in:

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

ID   Live Time      From        Level   Name
---  ------------   ----------  -----   ---------
8    0:17:16.2      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-3224SR:4#show switch
Command: show switch

Device Type        :DGS-3224SR Stackable 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 0.02.011
Hardware Version    : 0A1
Device S/N             :
```

```
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-3224SR:4#
```

show serial_port

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

Example Usage:

To display the serial port setting:

```
DGS-3224SR:4#show serial_port
Command: show serial_port
```

```
Baud Rate     : 115200
Data Bits     : 8
Parity Bits   : None
Stop Bits     : 1
Auto-Logout   : 10 mins
DGS-3224SR:4#
```

config serial_port

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

config serial_port

	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 auto logout:

```
DGS-3224SR:4#config serial_port auto_logout
10_minutes
Command: config serial_port auto_logout 10_minutes

 Success.

DGS-3224SR: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.

enable clipaging	
	The default setting is enabled.
Parameters	none.
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-3224SR:4#enable clipaging
Command: enable clipaging

 Success.

DGS-3224SR: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

disable clipaging	
	information.
Parameters	none.
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-3224SR:4#disable clipaging
Command: disable clipaging

 Success.

DGS-3224SR: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.

enable telnet	
Parameters	<tcp_port_number> – the TCP port number. TCP ports are numbered between 1 and 65535. The "well-known" TCP port for the Telnet protocol is 23.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To enable Telnet and configure port number:

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

 Success.

DGS-3224SR: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.

disable telnet

Restrictions	Only administrator-level users can issue this command.

Example Usage:

To disable the Telnet protocol on the switch:

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

 Success.

DGS-3224SR: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.

enable web	
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To enable HTTP and configure port number:

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

Success.

DGS-3224SR: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-3224SR:4#disable web
Command: disable web

 Success.

DGS-3224SR: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-3224SR:4#save
Command: save

  current box_id: 1  is AUTO
Do you want to save current box id from AUTO mode to
```

```
STATIC mode?(y/n)
```

reboot

Purpose	Used to restart the switch.
Syntax	**reboot**
Description	This command is used to restart the switch.
Parameters	none.
Restrictions	none.

Example Usage:

To restart the switch:

```
DGS-3224SR: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.

reset	
Syntax	**reset {config|system}**
Description	This command is used to restore the switch's configuration to the default settings assigned from the factory.
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, but maintain stack information:

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

Are you sure you want to proceed with system reset
```

```
except stack information?(y/n) y
 Success.

DGS-3224SR: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-3224SR:4#login
Command: login

UserName:
```

logout

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

Example Usage:

To terminate the current user's console session:

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

show device_status	
Purpose	Used to display the status of a device.
Syntax	**show device_status**
Description	This command displays the device status.
Parameters	None.
Restrictions	None.

Example Usage:

To terminate the current user's console session:

```
DGS-3224SR:#show device_status
Command:show device_status

ID   Internal Power   External power   Side Fan   Back Fan
---  --------------- ---------------- ---------- ----------
 1      Active          Fail          OK         OK
```

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] flow_control [enabled|disabled] learning [enabled|disabled] state [enabled|disabled]
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	**config ports [<portlist|all>] {speed(11) [auto(1)|10_half(2)|10_full(3)|100_half(4)| 100_full(8) [master(81) | slave(82)| 1000_full] flow_control [enabled|disabled] learning [enabled|disabled] state [enabled|disabled]}**
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 DGS3224SR is a stackable switch and each port is designated as belonging to a particular switch in the stack. For example, port 2 in switch 5 in a stack is listed as 2-5. A range of ports would be shown as 2-5, 3-6 (port 3 in switch 6), with the beginning and the end of the range of switches separated by a comma. 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

config ports	
	statically set to 1000 and cannot be set to slower speeds. [half|full] – Configures the specified range of ports as either full- or half-duplex. flowcontrol [enabled|disabled] – Enables or disables flow control for the specified range of ports. learning [enabled|disabled] – Enables or disables the MAC address learning on the specified range of ports. state [enabled|disabled] – 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-3224SR:4#config ports 1-3 speed 10_full learning enabled state enabled

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

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 DGS3224SR is a stackable switch and each port is designated as belonging to a particular switch in the stack. For example, port 2 in switch 5 in a stack is listed as 2:5. A range of ports would be shown as 2-5, 3-6 (port 3 in switch 6), with the beginning and the end of the range of switches separated by a comma.
Restrictions	none.

Example Usage:

To display the configuration of the ports 1-7 in switch 1:

```
DGS-3224SR:4#show ports 1-1,1-7

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_string32> view <view_name32> [readonly|readwrite]
delete snmp community	<community_string32>
enable rmon	
disable rmon	
config snmp system_contact	<sw_contact>
enable snmp traps	
disable snmp traps	
enable snmp authenticate_traps	
disable snmp authenticate_trap	

Command	Parameters
s	
show trusted_hosts	<ipaddr>
ping	<ipaddr> times <value> timeout <sec>
create snmp user	<SNMP_name 32> <groupname 32> {encrypted(1) [by_password(1) auth[md5(2) <auth_password 8-16> | sha(3) <auth_password 8-20>] priv [none(1) | des(2) <priv_password 8-16>] | by_key(2) auth [md5(2) <auth_key 32-32> | sha(3) <auth_key 40-40>] priv [none(1) | des(2) <priv_key 32-32>]]}
delete snmp user	<SNMP_name 32>
create snmp view	<view_name 32> [all | <oid>]
delete snmp view	<view_name 32> <oid> view_type[included(1 | excluded(2))
create snmp view	<view_view 32> [all | <oid>]
config snmp engineID	<snmp_engineID>
create snmp group	<groupname 32> [v1| v2c |v3 [noauth_nopriv | auth_nopriv | auth_priv]]{read_view <view_name32> |write|view <view_name32 | notify_view <view_name32> }
delete snmp group	<groupname 32>
create snmp host	<ipaddr> [v1 | v2c| v3 [noauth_nopriv | auth_nopriv | auth_priv]] <auth_string32>_
delete snmp host	<ipaddr>
show snmp engineID	

Command	Parameters
show snmp groups	
show snmp	[community | engineID | groups | host | traps | user | view]
show snmp user	
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 user

Purpose	Used to create a new SNMP user and adds the user to an SNMP group that is also created by this command.
Syntax	**create snmp user <SNMP_name32> <groupname 32>** {**encrypted(1) [by_password(1) auth[md5(2) <auth_password 8-16 > | sha(3) <auth_password 8-20 >]priv [none(1) | des(2) <priv_password 8-16>]| by_key(2) auth [md5(2) <auth_key 32-32>| sha(3) <auth_key 40-40>]priv [none(1) |des(2) <priv_key 32-32>]]**}
Description	The create snmp user command creates a new SNMP user and adds the user to an SNMP group that is also created by this command.
Parameters	<SNMP_name> – An alphanumeric name of up to 32 characters that will identify the new SNMP user. <groupname 32> – An alphanumeric name of up to 32 characters that will identify the SNMP group the new SNMP user will be associated with. encrypted – Specifies that the password will be in an encrypted format. by_password – Indicate input password for authentication and privacy. by_key – Indicate input key for authentication and privacy.

create snmp user	
	auth – Initiates an authentication level setting session. The options are MD5 and SHA. md5 – The HMAC-MD5-96 authentication level. sha – The HMAC-SHA-96 authentication level. <auth_password 8-16> – An alphanumeric sting of between 8 and 20 characters that will be used to authorize the agent to receive packets for the host. <priv_password 8-16> – An alphanumeric string of between 8 and 16 characters that will be used to encrypt the contents of messages the host sends to the agent. <auth_key> – An authentication key used by MD5 or SHA1, hex string type. <priv_key> – A privacy key used by DES, it is hex string type.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To create an SNMP user on the switch:

```
DGS-3224SR:4#create snmp user dlink default encrypted by_password
auth md5 auth_password none
Command: create snmp user dlink default encrypted by_password auth
md5 auth_password priv none
Success.
DGS-3224SR:4#
```

delete snmp user	
Purpose	Used to remove an SNMP user from an SNMP group and to delete the associated SNMP group.
Syntax	**delete snmp user <SNMP_name32>**
Description	The delete snmp user command removes an SNMP user from its SNMP group and then deletes the associated SNMP group.
Parameters	<SNMP_name> – An alphanumeric string of up to 32 characters that identifies the SNMP user that will be deleted.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To delete a previously entered SNMP user on the switch:

```
DGS-3224SR:4#delete snmp user dlink
Command: delete snmp user dlink

Success.

DGS-3224SR:4#
```

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

Example Usage:

To display the SNMP users currently configured on the switch:

```
DGS-3224SR:4#show snmp user
Command: show snmp user

Username                        Group Name       Ver   Auth     Priv
------------------------------  ---------------  ------- -------- ------------
initial                         initial          V3    None     None

Total Entries: 1

DGS-3224SR:4#
```

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

Example Usage:

To display the currently configured SNMP groups on the switch:

```
DGS-3224SR:4#show snmp groups
Command: show snmp groups

Vacm Access Table Settings

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

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

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

create snmp view

Purpose	Used to assign views to community strings to limit which MIB objects and SNMP manager can access.
Syntax	**create snmp view <view_name 32> <oid> view_type [included|excluded]**
Description	The create snmp view assigns views to community strings to limit which MIB objects an SNMP manager can access.
Parameters	<view_name 32> – An alphanumeric string of up to 32 characters that identifies the SNMP view that will be created. <oid> – The object ID that identifies an object tree (MIB tree) that will be included or excluded from access by an SNMP manager. included – Include this object in the list of objects that an SNMP manager can access. excluded – Exclude this object from the list of objects that an SNMP

create snmp view

	manager can access.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To create an SNMP view:

```
DGS-3224SR:4#create snmp view dlinkview 1.3.6 view_type
included
Command: create snmp view dlinkview 1.3.6 view_type included

 Success.

DGS-3224SR:4#
```

delete snmp view

Restrictions	Only administrator-level users can issue this command.

Example Usage:

To delete a previously configured SNMP view from the switch:

```
DGS-3224SR:4#delete snmp view dlinkview
Command: delete snmp view dlinkview

 Success.

DGS-3224SR:4#
```

show snmp view	
Purpose	Used to display an SNMP view previously created on the switch.
Syntax	**show snmp view {<view_name>}**
Description	The show snmp view command displays an SNMP view previously created on the switch.
Parameters	<view_name > – An alphanumeric string that identifies the SNMP view that will be displayed.
Restrictions	None.

Example Usage:

To show SNMP view:

```
UserName:
PassWord:
DGS-3224SR:4#show snmp view
Command: show snmp view

Vacm View Table Settings
View Name                    Subtree                          View Type

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

dlinkview                     1.3.6                         Included
restricted                    1.3.6.1.2.1.1                   Included
restricted                    1.3.6.1.2.1.11                  Included
restricted                    1.3.6.1.6.3.10.2.1                Included
restricted                    1.3.6.1.6.3.11.2.1                Included
```

```
restricted          1.3.6.1.6.3.15.1.1      Included
CommunityView       1                       Included
CommunityView       1.3.6.1.6.3             Excluded
CommunityView       1.3.6.1.6.3.1           Included

Total Entries: 9
DGS-3224SR:4#
```

create snmp community

Purpose	Used to create an SNMP community string to define the relationship between the SNMP manager and an agent. The community string acts like a password to permit access to the agent on the switch. One or more of the following characteristics can be associated with the community string: An Access List of IP addresses of SNMP managers that are permitted to use the community string to gain access to the switch's SNMP agent. An MIB view that defines the subset of all MIB objects that will be accessible to the SNMP community. Read|write or read-only level permission for the MIB objects accessible to the SNMP community.
Syntax	**create snmp community <community_string 32> view <view_name 32> [read_only|read_write]**

create snmp community

Description	The create snmp community command is used to create an SNMP community string and to assign access-limiting characteristics to this community string.
Parameters	<community_string 32> – An alphanumeric string of up to 32 characters that is used to identify members of an SNMP community. This string is used like a password to give remote SNMP managers access to MIB objects in the switch's SNMP agent. <view_name 32> – An alphanumeric string of up to 32 characters that is used to identify the group of MIB objects that a remote SNMP manager is allowed to access on the switch. read_only – Specifies that SNMP community members using the community string created with this command can only read the contents of the MIBs on the switch. read_write – Specifies that SNMP community members using the community string created with this command can read from and write to the contents of the MIBs on the switch.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To create the SNMP community string "dlink:"

```
DGS-3224SR:4#create snmp community dlink view
CommunityView read_write
Command: create snmp community dlink view CommunityView
read_write

 Success.

DGS-3224SR:4#
```

delete snmp community

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

Example Usage:

To delete the SNMP community string "dlink:"

```
DGS-3224SR:4#delete snmp community dlink
Command: delete snmp community dlink

Success.

DGS-3224SR:4#
```

show snmp community

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

Example Usage:

To display the currently entered SNMP community strings:

```
DGS-3224SR:4#show snmp community
Command: show snmp community

SNMP Community Table
Community Name              View Name                   Access
Right

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

private                     CommunityView               read_write
public                      CommunityView               read_only

Total Entries: 2
DGS-3224SR:4#
```

config snmp engineID

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

Example Usage:

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

```
DGS-3224SR:4#config snmp engineID 0035636666
Command: config snmp engineID 0035636666

Success.

DGS-3224SR:4#
```

show snmp engineID

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

Example Usage:

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

```
DGS-3224SR:4#show snmp engineID
Command: show snmp engineID
```

```
SNMP Engine ID : 0035636666
DGS-3224SR:4#
```

create snmp group

Purpose	Used to create a new SNMP group, or a table that maps SNMP users to SNMP views.
Syntax	**create snmp group <groupname> [v1|v2c|v3 noauth_nopriv|auth_nopriv|auth_priv]] {read_view <view_name>|notify_view <view_name>|notify_view <view_name>}**
Description	The create snmp group command creates a new SNMP group, or a table that maps SNMP users to SNMP views.
Parameters	<groupname> – An alphanumeric name that will identify the SNMP group the new SNMP user will be associated with. v1 – Specifies that SNMP version 1 will be used. The Simple Network Management Protocol (SNMP), version 1, is a network management protocol that provides a means to monitor and control network devices. v2c – Specifies that SNMP version 2c will be used. The SNMP v2c supports both centralized and distributed network management strategies. It includes

create snmp group

improvements in the Structure of Management Information (SMI) and adds some security features.

v3 – Specifies that the SNMP version 3 will be used. SNMP v3 provides secure access to devices through a combination of authentication and encrypting packets over the network. SNMP v3 adds:

- Message integrity – ensures that packets have not been tampered with in transit.
- Authentication – determines that an SNMP message is from a valid source.
- Encryption – scrambles the contents of messages to prevent it being seen by an unauthorized source.

noauth_nopriv – Specifies that there will be no authorization and no encryption of packets sent between the switch and a remote SNMP manager.

auth_nopriv – Specifies that authorization will be required, but there will be no encryption of packets sent between the switch and a remote SNMP manager.

auth_priv – Specifies that authorization will be required, and

create snmp group	
	that packets sent between the swtich and a remote SNMP manger will be encrypted. read_view – Specifies that the SNMP group being created can request SNMP messages. <view_name> – An alphanumeric string that is used to identify the group of MIB objects that a remote SNMP manager is allowed to access on the switch. notify_view – Specifies that the SNMP group being created can recieve SNMP trap messages generated by the switch's SNMP agent.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To create an SNMP group named "D-Link_group":

```
DGS-3224SR:4#creat snmp group D-Link_group v3 auth_priv
read_view CommunityView

write_view CommunityView notify_view CommunityView
Command: create snmp group D-Link_group v3 auth_priv
read_view CommunityView wri
te_view CommunityView notify_view CommunityView

 Success.
```

```
DGS-3224SR:4#
```

delete snmp group

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

Example Usage:

To delete the SNMP group named "D-Link_group":

```
DGS-3224SR:4#delete snmp group D-Link_group
Command: delete snmp group D-Link_group

Success.

DGS-3224SR:4#
```

create snmp host

Purpose	Used to create a recipient of SNMP traps generated by the switch's SNMP agent.

create snmp host	
	generated by the switch's SNMP agent.
Syntax	**create snmp host <ipaddr> [v1|v2c|v3 [noauth_nopriv|auth_nopriv|auth_priv] <auth_string 32>]**
Description	The create snmp host command creates a recipient of SNMP traps generated by the switch's SNMP agent.
Parameters	<ipaddr> – The IP address of the remote management station that will serve as the SNMP host for the switch. v1 – Specifies that SNMP version 1 will be used. The Simple Network Management Protocol (SNMP), version 1, is a network management protocol that provides a means to monitor and control network devices. v2c – Specifies that SNMP version 2c will be used. The SNMP v2c supports both centralized and distributed network management strategies. It includes improvements in the Structure of Management Information (SMI) and adds some security features. v3 – Specifies that the SNMP version 3 will be used. SNMP v3 provides secure access to devices through a combination of authentication and encrypting packets over the network. SNMP v3 adds: • Message integrity – ensures that

create snmp host

packets have not been tampered with in transit.

- Authentication – determines that an SNMP message is from a valid source.
- Encryption – scrambles the contents of messages to prevent it being seen by an unauthorized source.

noauth_nopriv – Specifies that there will be no authorization and no encryption of packets sent between the switch and a remote SNMP manager.

auth_nopriv – Specifies that authorization will be required, but there will be no encryption of packets sent between the switch and a remote SNMP manager.

auth_priv – Specifies that authorization will be required, and that packets sent between the swtich and a remote SNMP manger will be encrypted.

<auth_sting 32> – An alphanumeric string used to authorize a remote SNMP manager to access the switch's SNMP agent.

Restrictions	Only administrator-level users can issue this command.

Example Usage:

To create an SNMP host to receive SNMP messages:

```
DGS-3224SR:4#create snmp host 10.59.19.2 v3 noauth_nopriv
initial
Command: create snmp host 10.59.19.2 v3 noauth_nopriv initial

 Success.

DGS-3224SR:4#
```

delete snmp host

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

Example Usage:

To delete an SNMP host entry:

```
DGS-3224SR:4#delete snmp host 10.52.19.2
Command: delete snmp host 10.52.19.2

Success.

DGS-3224SR:4#
```

show snmp host

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

Example Usage:

To display the currently configured SNMP hosts on the switch:

```
DGS-3224SR:4#show snmp host
Command: show snmp host
```

```
SNMP Host Table
Host IP Address  SNMP Version     Community Name / SNMPv3
User Name
---------------  ---------------  --------------------------------
10.59.19.2       V3 noauthnopriv  initial

Total Entries: 1
DGS-3224SR:4#
```

show snmp traps

Purpose	Used to display the status of SNMP traps and authentication traps
Syntax	**show snmp traps**
Description	The show snmp traps command is used to show traps state.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To display the current state of traps on the switch:

```
DGS-3224SR:4#show snmp traps
Command: show snmp traps

SNMP Trap         : Enabled
Authenticate Traps : Enabled
DGS-3224SR:4#
```

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 "dgs3224srcliman":

.

```
DGS-3224SR:4#config snmp system_name
dgs3224srcliman
Command: config snmp system_name dgs3224srcliman

 Success.

DGS-3224SR:4#
```

config snmp system_location	
Purpose	Used to enter a description of the location of the switch.
Syntax	**config snmp system_location <sw_location>**
Description	This command is used to enter a description of the location of the switch. A maximum of 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 "factory":

.

```
DGS-3224SR:4#config snmp system_location factory
Command: config snmp system_location factory

 Success.
```

```
DGS-3224SR:4#
```

config snmp system_contac :	
Purpose	Used to enter the name of a contact person who is responsible for the switch.
Syntax	**config snmp system_contact <sw_contact>**
Description	This command is used to enter the name and|or other information to identify a contact person who is responsible for the switch. A maximum of 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 "igor":

.

```
DGS-3224SR:4#config snmp system_contact igor
Command: config snmp system_contact igor

 Success.

DGS-3224SR: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 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-3224SR:4#enable rmon
Command: enable rmon

 Success.

DGS-3224SR:4#
```

disable rmon	
Purpose	Used to disable RMON on the switch.
Syntax	**disable rmon**

disable rmon

Description	This command is used, in conjunction with the **enable rmon** command above, to enable and disable remote monitoring (RMON) on the switch.
Parameters	none.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To disable RMON:

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

 Success.

DGS-3224SR:4#
```

show snmp

Purpose	Used to display the SNMP configuration entered on the switch.
Syntax	**show snmp [community | engineID | groups | host | traps | user | view]**
Description	This command will display the current SNMP configuration on the switch.

show snmp

Parameters	community – Displays all of the communities configured on the switch. A community string is an alpha-numeric string used to authenticate management stations wanting access to the switch's SNMP agent. engineID -
Restrictions	None.

Example Usage:

To display SNMP configurations:

```
DGS-3224SR:4#show snmp
Command: show snmp

System Name          : DGS3224TGR
System Location      : Taiwan
System Contact       : dlink
SNMP Trap            : Enabled
Authenticate Traps   : Enabled



Community String                    Rights
-------------------------------------------- ---------------
System                                Read|Write
public                                Read-Only
```

```
Develop                          Read-Only
private                          Read|Write

 Total Entries: 4

IP Address      Community String
---------------  ------------------------------------------------------------
10.1.1.1         Develop

 Total Entries: 1

DGS-3224SR: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.
Restrictions	none.

Example Usage:

To display the list of trusted hosts:

```
DGS-3224SR:4#show trusted_host
```

```
Command: show trusted_host


Management Stations

IP Addrress
---------------

Total Entries: 0

DGS-3224SR: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-3224SR:4#enable snmp traps
Command: enable snmp traps

 Success.
```

```
DGS-3224SR:4#
```

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

Example Usage:

To prevent SNMP traps from being sent from the switch:

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

 Success.

DGS-3224SR: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-3224SR:4#enable snmp authenticate_traps
Command: enable snmp authenticate_traps

Success.

DGS-3224SR: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-3224SR:4#disable snmp authenticate_traps
Command: disable snmp authenticate_traps

 Success.

DGS-3224SR: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 "10.52.19.2" for 4 times:

```
DGS-3224SR:4#ping 10.52.19.2 times 4
Command: ping 10.52.19.2 times 4

Request timed out.
Reply from 10.52.19.2, time<10ms
Reply from 10.52.19.2, time<10ms
Reply from 10.52.19.2, time<10ms
 Ping Statistics for 10.52.19.2
 Packets: Sent =4, Received =3, Lost =1

DGS-3224SR:4#
```

7

UTILITY COMMANDS

The Utility (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_filename64> {unit [all | <unitid>]} | configuration <ipaddr> <path_filename64> {increment}
upload	configuration log <ipaddr> <path_filename64>

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

download

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. unit [all|<unitid>] – All specifies all units (switches), <unitid> is the unit id of the switch that will receive the download. 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

download	
	parameters will remain unchanged.
Restrictions	The TFTP server must be on the same IP subnet as the switch. Only administrator-level users can issue this command.

Example Usage:

```
DGS-3224SR: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-3224SR: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

upload	
	TFTP server. log – Specifies that the switch history log will be uploaded to the TFTP server. <ipaddr> – The IP address of the TFTP server. The TFTP server must be on the same IP subnet as the switch. <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-3224SR: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-3224SR: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>] { severity [informational | warning | all] | facility [local0 | local1 | local2 | local3 | local4 | local5 |local6 | local7] | |udp_port <udp_port_numer> |

Command	Parameters
	ipaddress <ipaddr> | state [enable | disable]}
Create syslog	**{host(1) [all|<index 1-4>] { severity [informational | warning | all] | facility [local0 | local1 | local2 | local3 | local4 | local5 |local6 | local7] | |udp_port <udp_port_numer> | ipaddress <ipaddr> | state [enable | disable]}**
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 DGS3224SR is a stackable switch and each port is designated as belonging to a particular switch in the stack. For example,

show packet ports

	port 2 in switch 5 in a stack is listed as 2-5. A range of ports would be shown as 2-5, 3-6 (port 3 in switch 6), with the beginning and the end of the range of switches separated by a comma.
Restrictions	none.

Example Usage:

To display the packets analysis for port 7:

```
Port number : 1:1
Frame Size    Frame Counts  Frames/sec    Frame Type   Total  Total/sec
------------  ------------  ----------    ----------   ---------  ---------
64            554569        53            RX Bytes     217736772  10678
65-127        253434        30            RX Frames    1010191    100
128-255       58687         15
256-511       54386         1             TX Bytes     199735     0
512-1023      14721         0             TX Frames    2221       0
1024-1518     76600         1

Unicast RX    284475        16
Multicast RX  137061        6
Broadcast RX  588655        78
```

show error ports

Purpose	Used to display the error statistics for a range of ports.

show error 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 highest port number of the range. The DGS3224SR is a stackable switch and each port is designated as belonging to a particular switch in the stack. For example, port 2 in switch 5 in a stack is listed as 2-5. A range of ports would be shown as 2-5, 3-6 (port 3 in switch 6), with the beginning and the end of the range of switches separated by a comma.
Restrictions	none.

Example Usage:

To display the errors of the port 3:

```
DGS-3224SR:4#show error ports 1
Command: show error ports 1:1

 Port number : 1:1
          RX Frames                    TX Frames
```

```
                ---------                    ---------
CRC Error       60              Excessive Deferral    0
Undersize       0               CRC Error             0
Oversize        0               Late Collision        0
Fragment        0               Excessive Collision   0
Jabber          15              Single Collision      0
Drop Pkts       234952          Collision             0
```

show utilization

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

```
Port    TX/sec     RX/sec   Util    Port    TX/sec     RX/sec   Util
-----  ---------- ---------- ----    -----  ---------- ---------- ----
1:1    0          37         1       1:22   0          0          0
1:2    0          0          0       1:23   0          0          0
1:3    0          0          0       1:24   0          0          0
1:4    0          0          0
1:5    36         0          1
```

```
1:6    0        0        0
1:7    0        0        0
1:8    0        0        0
1:9    0        0        0
1:10   0        0        0
1:11   0        0        0
1:12   0        0        0
1:13   0        0        0
1:14   0        0        0
1:15   0        0        0
1:16   0        0        0
1:17   0        0        0
1:18   0        0        0
1:19   0        0        0
1:20   0        0        0
1:21   0        0        0
 CTRL+C ESC q Quit SPACE n Next Page p Previous Page r
Refresh
```

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 DGS3224SR is a stackable switch and

clear counters	
	each port is designated as belonging to a particular switch in the stack. For example, port 2 in switch 5 in a stack is listed as 2-5. A range of ports would be shown as 2-5, 3-6 (port 3 in switch 6), with the beginning and the end of the range of switches separated by a comma.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To clear the counters:

```
DGS-3224SR:4#clear counters ports 7-9
Command: clear counters ports 1:7-1:9

 Success.

DGS-3224SR: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.

clear log	
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To clear the log information:

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

 Success.

DGS-3224SR:4#
```

show log	
Purpose	Used to display the switch history 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-3224SR:4# show log

46   2003-10-11 12:26:10 Unit 1, Console session timed out (Username:
Anonymous

                  )
45   2003-10-11 12:14:31 Port 1:5 link up, 100Mbps FULL duplex
44   2003-10-11 12:14:31 Port 1:1 link up, 100Mbps FULL duplex
43   2003-10-11 12:14:29 Port 1:5 link down
42   2003-10-11 12:14:29 Port 1:1 link down
41   2003-10-11 12:12:14 Port 1:5 link up, 100Mbps FULL duplex
40   2003-10-11 12:12:14 Port 1:1 link up, 100Mbps FULL duplex
39   2003-10-11 12:12:12 Port 1:5 link down
38   2003-10-11 12:12:12 Port 1:1 link down
37   2003-10-11 12:12:02 Unit 1, Successful login through Console (Username: An

                  onymous)
36   2003-10-11 12:00:13 Unit 1, Console session timed out (Username:
Anonymous

                  )
35   2003-10-11 12:00:13 Unit 1, Console session timed out (Username:
Anonymous

                  )
34   2003-10-11 11:38:15 Unit 1, Successful login through Console (Username: An

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

DGS-3224SR:4#
```

enable syslog

Purpose	Used to enable syslog sending message.
Syntax	**Enable syslog**
Description	This command will clear enable syslog sending.

enable syslog

	sending.
Parameters	none.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To enable syslog:

```
DGS-3224SR:4#enable syslog
Command: enable syslog

 Success.

DGS-3224SR:4#
```

disable syslog

Purpose	Used to disable syslog sending message.
Syntax	**disable syslog**
Description	This command will disable syslog sending.
Parameters	none.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To enable syslog:

```
DGS-3224SR:4#disable syslog
```

```
Command: disable syslog

Success.

DGS-3224SR:4#
```

show syslog

Purpose	Used to display the syslog protocol global state.
Syntax	**show syslog**
Description	This command will display the syslog protocol global state.
Parameters	none.
Restrictions	none

Example Usage:

To display the syslog proocol global state:

```
DGS-3224SR:4#show syslog
Command: show syslog

Syslog Global State: Disabled

DGS-3224SR:4#
```

config syslog host

config syslog host

Purpose	Used to configure the syslog host parameters.
Syntax	**Config syslog host [all |<index>] {severity [informational | warning | all] | facility | local0 | local1 |local2 | local3 | local4 | local5 | local6 | local7] | udpport <udp_port_number> | ipaddress <ipaddr> | state [enable | disable]}**
Description	This command configures the syslog host parameters.
Parameters	Host – host index or all hosts Severity – three levels are supported: Informational: informational messages Warning: warning conditions All: any condition local0 to local7 – these are user-defined facilities udp_port – udp port number ipaddr – IP address of the host state – enables or disables reception of event-notification messages
Restrictions	Only administrator-level users can use this command.

DGS-3224SR:4#config syslog host all severity all facility local0

```
Command: config syslog host all severity all facility
local0

 Success.

DGS-3224SR:4#
```

create syslog host

Purpose	Used to create a new syslog host.
Syntax	**create syslog host <index 1-4>] {severity [informational | warning | all} | facility [local0 | local1 |local2 | local3 | local4 | local5 | local6 | local7] | udpport <udp_port_number> | ipaddress <ipaddr> | state [enable | disable]}**
Description	This command creates a new syslog host.
Parameters	Host – host index or all hosts Severity – three levels are supported: Informational: informational messages Warning: warning conditions All: any condition local0 to local7 – these are user-defined facilities udp_port – udp port number ipaddr – IP address of the host state – enables or disables reception of event-notification messages

create syslog host

Restrictions	Only administrator-level users can use this command.

```
DGS-3224SR:4#create syslog host 1 severity all facility
local0
Command: create syslog host 1 severity all facility local0

 Success.

DGS-3224SR:4#
 Success.

DGS-3224SR:4#
```

delete syslog host

Purpose	Used to delete syslog host(s).
Syntax	**Delete syslog host [index 1-4 | all]**
Description	This command deletes a new syslog host.
Parameters	Host – host index or all hosts
Restrictions	Only administrator-level users can use this command.

```
DGS-3224SR:4#delete syslog host 1
Command: delete syslog host 1

 Success.

DGS-3224SR:4#
```

show syslog host

Purpose	Used to display syslog host configurations.
Syntax	**show syslog host** {**<index 1-4>**}
Description	This command displays the syslog host configurations.
Parameters	host index If no parameter is specified, all hosts will be displayed.
Restrictions	None..

```
DGS-3224SR:4#show syslog host
Command: show syslog host

 Syslog Global State: Disabled
```

```
 Host Id  Host IP Address     Severiry     Facility  UDP port
Status
 -------  ---------------  --------------  --------  --------  --------

 Total Entries : 0

DGS-3224SR: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	Parameter
config stp	maxage <value6-40>| hellotime <value1-10>| forwarddelay <value4-30>| priority <value0-61440>| version [rstp | stp]| txholdcount <value1-10>| fbpdu [enabled|disabled] }(1)
config stp ports	<portlist> {cost [auto | <value1-200000000> |priority <value0-240>| 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 setup STP on the switch.
Syntax	config stp {maxage <value6-40>|hellotime <value1-10>|forwarddelay <value4-30>|priority <value0-61440>|version [rstp | stp] | defaultpathcost [8021t | 8021d] | txholdcount <value1-10> |fbpdu [enable|disable]}(1)
Description	This command is used to set up the Spanning Tree Protocol (STP) for the entire switch.
Parameters	maxage <value6-40> – 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 <value1-10> – The time interval between transmission of configuration messages by the root device. The default is 2 seconds. forwarddelay <value4-30> – The maximum amount of time (in seconds) that the root device will wait before changing states. The default is 15 seconds. priority <value1-61440> – A numerical value that is used in determining the root device, root port, and designated port. The device with the highest priority becomes the root device. The lower the numerical

config stp	
	value, the higher the priority. The default is 32,768. Range is 0 to 61440, in steps of 4096. 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. version - The version of Spanning Tree Protocol the bridge is currently running. Default is Rapid Spanning Tree Protocol (rstp). txholdcount - Used by the Port Transmit state to limit the maximum transmission rate. Default is 3.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To set maxage to 18 and hellotime to 4:

```
DGS-3224SR:4#config stp maxage 10 hellotime 4
Command: config stp maxage 10 hellotime 4

 Success.

DGS-3224SR:4#
```

config stp ports

Purpose	Used to setup STP on the port level.
Syntax	**config stp ports <portlist> {cost [auto |<value1-20000000>|priority <value0-240>|migrate [yes | no] | edge [true | false] | p2p [true | false | auto] | state [enable|disable]}(1)**
Description	This command is used to create and configure STP for a group of ports.
Parameters	<portlist> – specifies a range of ports to be configured. The port list is specified by listing the beginning port number and the highest port number of the range. The DGS3224SR is a stackable switch and each port is designated as belonging to a particular switch in the stack. For example, port 2 in switch 5 in a stack is listed as 2-5. A range of ports would be shown as 2-5, 3-6 (port 3 in switch 6), with the beginning and the end of the range of switches separated by a comma. state [enable|disable] – Allows STP to be enabled or disabled for the ports specified in the port list. The default is disabled. cost <value> – 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

config stp ports	
	2,000,000. priority <value> – A numeric value between 0 and 240, in steps of 16, 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 – when operating in RSTP mode, the "yes" parameter forces the port to transmit RSTP BPDUs. edge – *true* indicates the port is assumed to be an edge port; *false* indicates a non-edge port. p2p – *true* indicates the port should be treated as a point-to-point link; *false* indicates the port should be treated as having a shared media connection; *auto* indicates that th eport is considered to have a p2p link if it si an aggregator and all of its members are aggregatable, or if the MAC entity is configured for full duplex operation. state – allows STP to be enabled or disabled for the specified ports Default is enable.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To set the path cost 19, the priority 16, and the state enabled of the ports 1-5:

```
DGS-3224SR:4#config stp ports 1:1-1:5 cost 19 priority
16 state enabled
Command: config stp ports 1:1-1:5 cost 19 priority 16
state enabled

 Success.

DGS-3224SR: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-3224SR:4#enable stp
Command: enable stp

 Success.
```

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

 Success.

DGS-3224SR:4#
```

show stp

Purpose	Used to display the switch's current STP configuration.

show stp	
Syntax	**show stp**
Description	This command displays the switch's current STP configuration.
Parameters	none
Restrictions	none.

Example Usage:

Status 1: STP enabled

```
STP Status       : Enabled
Max Age          : 10
Hello Time       : 4
Forward Delay    : 15
Priority         : 32768
Default Path Cost : 802.1T
STP Version      : RSTP
TX Hold Count    : 3
Forwarding BPDU  : Enabled


Designated Root Bridge: 00-00-00-52-33-E3
Root Priority       : 32768
Cost to Root        : 0
Root Port           : None
Last Topology Change  : 25sec
Topology Changes Count: 1
Protocol Specification: 3
Max Age             : 10
Hello Time          : 4
Forward Delay       : 15
```

```
  Hold Time          : 3
  CTRL+C ESC q Quit SPACE n Next Page p Previous
Page r Refresh
```

Status 2: STP Disabled

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

STP Status       : Disabled
Max Age          : 10
Hello Time       : 4
Forward Delay    : 15
Priority         : 32768
Default Path Cost : 802.1T
STP Version      : RSTP
TX Hold Count    : 3
Forwarding BPDU  : Enabled

DGS-3224SR: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.
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.

show stp ports

	The DGS3224SR is a stackable switch and each port is designated as belonging to a particular switch in the stack. For example, port 2 in switch 5 in a stack is listed as 2-5. A range of ports would be shown as 2-5, 3-6 (port 3 in switch 6), with the beginning and the end of the range of switches separated by a comma.
Restrictions	None

Example Usage:

To display STP state of port 1-9:

```
DGS-3224sR:4#show stp ports 1-9


 Port  Connection        State Cost     Pri Edge P2P Status     Role
 ----- ------------------ --- ---------- ---- --- --- ---------- ----------
 1:1   100M/Full/None     Yes  19       16   No   Yes  Forwarding
Designated
 1:2   Link Down         Yes  19       16   No   Yes  Disabled   Disabled
 1:3   Link Down         Yes  19       16   No   Yes  Disabled   Disabled
 1:4   Link Down         Yes  19       16   No   Yes  Disabled   Disabled
 1:5   100M/Full/None     Yes  19       16   No   Yes  Forwarding
Designated
 1:6   Link Down         Yes *20000     128  No   Yes  Disabled
Disabled
 1:7   Link Down         Yes *20000     128  No   Yes  Disabled
Disabled
 1:8   Link Down         Yes *20000     128  No   Yes  Disabled
```

```
Disabled
 1:9   Link Down          Yes *20000     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>
clear fdb	[vlan <vlan_name32> | port <port>| all]
show multicast_fdb	[vlan <vlan_name> mac_address <macaddr>]
show fdb	{port <port> | vlan <vlan_name> | mac_address <macaddr> | static | aging_time}

Command	Parameters
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_name32> <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.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To create an unicast MAC forwarding:

```
DGS-3224SR:4#create fdb default 00-00-00-00-01-02 port
5
Command: create fdb default 00-00-00-00-01-02 port 1:5

 Success.

DGS-3224SR:4#
```

create multicast_fdb

Purpose	Used to create a static entry to the multicast MAC address forwarding table (database)
Syntax	**create multicast_fdb [<vlan_name32> <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 added to the forwarding table.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To create multicast MAC forwarding:

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

 Success.

DGS-3224SR: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 added to the forwarding table. [add|delete] – Add or delete the following <portlist> to forwarding database. <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.

config multicast_fdb

	The DGS3224SR is a stackable switch and each port is designated as belonging to a particular switch in the stack. For example, port 2 in switch 5 in a stack is listed as 2-5. A range of ports would be shown as 2:5, 3:6 (port 3 in switch 6), with the beginning and the end of the range of switches separated by a comma.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To add multicast MAC forwarding:

```
DGS-3224SR: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 
1:1-1:5

Success.

DGS-3224SR:4#
```

config fdb aging_time

Purpose	Used to the switch's MAC address aging time.
Syntax	**Config fdb aging_time <sec 10-1000000>**
Description	This command is used to set the age-out timer for the switch's dynamic unicast MAC

config fdb aging_time

	address forwarding tables.
Parameters	aging_time – the time, in seconds, that a dynamically learned MAC address will remain in the MAC address forwarding table, without being accessed, before being dropped from the database. Range: 10-1000000 seconds.
Restrictions	Only administrator-level users can issue this command.

```
DGS-3224SR:4#config fdb aging_time 300
Command: config fdb aging_time 300

Success.

DGS-3224SR:4#
```

delete fdb

Purpose	Used to delete an entry to the switch's forwarding database for both unicast and multicast.

delete fdb	
Syntax	**delete fdb <vlan_name32> <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. Maximum length is 32 characters. <macaddr> – The MAC address that will be deleted to the forwarding table.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To delete a permanent FDB entry:

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

 Success.

DGS-3224SR:4#
```

clear fdb	
Purpose	Used to clear the switch's forwarding database of all dynamically learned MAC

clear fdb	
	addresses.
Syntax	**clear fdb [vlan <vlan_name32>|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-3224SR:4#clear fdb all
Command: clear fdb all

 Success.

DGS-3224SR:4#
```

show multicast_fdb

Purpose	Used to display the contents of the switch's multicast forwarding database.
Syntax	**show multicast_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-3224SR:4#show multicast_fdb
Command: show multicast_fdb


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


Total Entries: 1
```

```
DGS-3224SR:4#
```

show fdb

Purpose	Used to display the current unicast MAC address forwarding database.
Syntax	**show fdb {port <port>|vlan <vlan_name32>|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-3224SR:4#show fdb
Command: show fdb


 Unicast MAC Address Ageing Time  = 300

 VID   VLAN Name       MAC Address       Port    Type
 ----  ---------------  -----------------  ------  -----------------
 1     default          00-00-00-00-00-04  1:1     Dynamic
 1     default          00-00-00-00-00-0D  1:1     Dynamic
 1     default          00-00-00-00-00-19  1:1     Dynamic
 1     default          00-00-00-52-33-E3  CPU     Self
 1     default          00-00-5A-53-05-A0  1:1     Dynamic
 1     default          00-00-5E-00-01-01  1:1     Dynamic
 1     default          00-00-74-60-72-2D  1:1     Dynamic
 1     default          00-00-81-48-75-00  1:1     Dynamic
 1     default          00-00-81-9A-99-4F  1:1     Dynamic
 1     default          00-00-81-9A-F2-F4  1:1     Dynamic
 1      default            00-00-00-00-01-02     5       Permanent
 1      default            00-50-BA-6B-2A-29   9       Dynamic


DGS-3224SR: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_grouplist> | all] {broadcast [enabled|disabled] | multicast [enabled|disabled] | dlf [enabled|disabled] | threshold <value 0-255>}
show traffic control	group_list <storm_grouplist>

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_grouplist>|all] {broadcast [enable|disable]|multicast [enable|disable]|dlf [enable|disable]|threshold <value>}**
Description	This command is used to configure broadcast/multicast/dlf storm control.
Parameters	<storm_grouplist> – Used to specify a broadcast storm control group with the syntax: unit_id. all – Specifies all broadcast storm control groups on the switch. broadcast [enabled|disabled] – Enables or disables broadcast storm control. multicast [enabled|disabled] – Enables or disables multicast storm control. dlf [enabled|disabled] – 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-3224SR:4#config traffic control all broadcast
enable multicast enable dlf enable threshold 255
Command: config traffic control all broadcast enable
multicast enable dlf enable
 threshold 255

 Success.

DGS-3224SR:4#
```

show traffic control

Purpose	Used to display current traffic control settings.
Syntax	**show traffic control {group_list<storm_grouplist>}**
Description	This command displays the current storm traffic control configuration on the switch.
Parameters	group_list <storm_grouplist> – Used to specify a broadcast storm control group with the syntax: unit_id:group_id.

show traffic control

Restrictions none.

Example Usage:

To display traffic control setting:

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

Traffic Control

                                  Broadcast  Multicast  Destination
Module  Group [ports]  Threshold  Storm      Storm      Lookup Fail
------  -------------  ---------  ---------  ---------  -----------
1       1              255        Enabled    Enabled    Enabled
1       2              255        Enabled    Enabled    Enabled
1       3              255        Enabled    Enabled    Enabled
1       4              255        Enabled    Enabled    Enabled
1       5              255        Enabled    Enabled    Enabled
1       6              255        Enabled    Enabled    Enabled
1       7              255        Enabled    Enabled    Enabled
1       8              255        Enabled    Enabled    Enabled
1       9              255        Enabled    Enabled    Enabled
1       10             255        Enabled    Enabled    Enabled
1       11             255        Enabled    Enabled    Enabled
1       12             255        Enabled    Enabled    Enabled
1       13             255        Enabled    Enabled    Enabled
1       14             255        Enabled    Enabled    Enabled
1       15             255        Enabled    Enabled    Enabled
1       16             255        Enabled    Enabled    Enabled
```

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 <value 0-65535>
show arpentry	{ipif(1) <ipif_name 12> | ipaddress(2) <ipaddr> | static(3)}

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 <value 0-65535>**
Description	This command sets the maximum amount of time, in minutes, that a ARP entry can

config arp_aging	
	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 <value 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-3224SR:4#config arp_aging time 30
Command: config arp_aging time 30

 Success.

DGS-3224SR: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

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-3224SR:4#show arpentry
Command: show arpentry


 ARP Aging Time : 30

Interface     IP Address      MAC Address       Type
------------  --------------  ----------------  --------------
System        10.0.0.0        FF-FF-FF-FF-FF-FF  Local/Broadcast
System        10.0.0.139       00-40-05-D3-20-76  Dynamic
System        10.0.1.100       00-50-BA-F4-96-9A  Dynamic
System        10.0.25.1        00-D0-59-A9-2A-C4  Dynamic
System        10.0.51.1        00-80-C8-4C-69-FB  Dynamic
System        10.0.58.4        00-0C-6E-43-13-AE  Dynamic
System        10.1.1.1        00-E0-98-74-F2-CA  Dynamic
System        10.1.1.170       00-50-BA-70-E4-7A  Dynamic
System        10.1.1.252       00-01-30-BC-FD-30  Dynamic
```

```
System      10.1.23.1      00-50-BA-0A-D5-B4  Dynamic
System      10.1.49.9      00-08-02-0A-6F-D8  Dynamic
System      10.1.53.1      00-50-BA-0A-F5-21  Dynamic
System      10.2.26.1      00-80-C8-F7-93-73  Dynamic
System      10.2.27.250     00-50-BA-DA-01-58  Dynamic
System      10.2.33.1      00-50-BA-14-D8-A5  Dynamic
System      10.2.33.201     00-80-C8-CD-25-3A  Dynamic
System      10.2.33.202     00-80-C8-CD-25-39  Dynamic

 Total Entries = 20

DGS-3224SR: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 bandwidth_control	[<portlist>] {rx_rate [no_limit | <value 1-1000>] | tx_rate {no_limit | <value 1-1000>]}
show bandwidth_control	{<portlist>}
config scheduling	<class_id 0-6>{max_packet <value 1-15>}
config scheduling_mechanism	[strict|weight_fair]
show scheduling	
show scheduling_mechanism	
config 802.1p user_priority	<priority 0-7> <class_id 0-6>
show 802.1p user_priority	

Command	Parameters
config 802.1p default_priority	[<portlist>|all] <priority 0-7>
show 802.1p default_priority	<portlist>
disable hol_prevention	
enable hol_prevention	
show hol_prevention	

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

config bandwidth_control

Purpose	Used to configure the port bandwidth control.
Syntax	**config bandwidth_control <portlist> {rx_rate [no_limit | <value 1-1000>] | tx_rate {no_limit | <value 1-1000>]}**
Description	This command configures the port bandwidth control.
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 DGS3224SR is a stackable switch and each port is designated as belonging to a particular switch in the stack. For example, port 2 in switch 5 in a stack is listed as 2-5. A range of ports would be shown as 2-5, 3-6

config bandwidth_control

	(port 3 in switch 6), with the beginning and the end of the range of switches separated by a comma. Rx_rate – specifies the limitation of receive-data rate Tx_rate – specifies the limitation of the transmit-data rate
Restrictions	Only administrator-level users can issue this command. For Gigabit ports, the tx_rate and/or rx_rate must be a multiple of 8.

Example Usage:

To configure scheduling:

```
DGS-3224SR:4#config bandwidth_control 1-10 tx_rate 16
Command: config bandwidth_control 1:1-1:10 tx_rate 16

 Success.

DGS-3224SR:4#
```

show bandwidth_control

Purpose	Used to display the port bandwidth control table.
Syntax	**show bandwidth_control**

show bandwidth_control

Description	This command sdisplays the port bandwidth configurations.
Parameters	<portlist> - specifies the range of ports
Restrictions	none.

Example Usage:

To display port bandwidth control table:

```
DGS-3224SR:4#show bandwidth_control 1-10
Command: show bandwidth_control 1:1-1:10

Bandwidth Control Table

Port   RX Rate (Mbit/sec)        TX_RATE (Mbit/sec)
-----  ----------------------  ----------------------
1:1   no_limit                16
1:2   no_limit                16
1:3   no_limit                16
1:4   no_limit                16
1:5   no_limit                16
1:6   no_limit                16
1:7   no_limit                16
1:8   no_limit                16
1:9   no_limit                16
1:10  no_limit                 16

DGS-3224SR:4#
```

config scheduling

Purpose	Used to configure the traffic scheduling mechanism for each COS queue.
Syntax	**config scheduling <class_id 0-n> {max_packet <value 0-15>**
Description	The switch contains n + 1 hardware priority queues. Incoming packets must be mapped to one of these n + 1 queues. This command is used to specify the rotation by which these n + 1 hardware priority queues are emptied. The switch's default (if the config scheduling command is not used, or if the config scheduling command is entered with both max_packet and max_latency parameters set to zero) is to empty the n + 1 hardware priority queues in order – from the highest priority queue (hardware queue n) to the lowest priority queue (hardware queue 0). Each hardware queue will transmit all of the packets in its buffer before allowing the next lower priority queue to transmit its packets. When the lowest hardware priority queue has finished transmitting all of its packets, the highest hardware priority queue can again transmit any packets it may have received.
Parameters	<class_id> – This specifies which of the n + 1 hardware priority queues the config scheduling command will apply to. The hardware priority queues are identified by number – from 0 to n – with the 0 queue

config scheduling

	being the lowest priority. (The max value of n is 6, and class_id 7 is reserved for internal control packet use.) max_packet – specifies the weights for weighted fari queueing. Max_packet is the maximum number of packets the hardware priority queue will be allowed to transmit before allowing the next lowest priority queue to transmit its packets. A value between 0 and 15 can be used.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To configure the traffic scheduling mechanism for each COS queue:

```
DGS-3224SR:4#config scheduling 1 max_packet 10
Command: config scheduling 1 max_packet 10

Success.
```

show scheduling

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

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-3224SR:4#show scheduling
Command: show scheduling


QOS Output Scheduling

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

DGS-3224SR:4#
```

config scheduling_mechanis n	
Purpose	Used to configure the traffic scheduling mechanism for each COS queue.
Syntax	**config scheduling_mechanism [strict(1)| weight_fair(2)]**
Description	This command is use to specify how the switch handles 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-3224SR:4#config scheduling_mechanism strict
Command: config scheduling_mechanism strict

 Success.

DGS-3224SR: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-3224SR:4#show scheduling_mechanism
Command: show scheduling_mechanism

QOS scheduling_mechanism
CLASS ID  Mechanism
--------  -----------
Class-0   strict
Class-1   strict
Class-2   strict
Class-3   strict
Class-4   strict
Class-5   strict
Class-6   strict
Class-7   strict
```

```
DGS-3224SR: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.
Syntax	**config 802.1p user_priority <priority 0-6> <class_id 0-n>**
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 four 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

config 802.1p user_priority

	7 6 High This mapping scheme is based upon recommendations contained in IEEE 802.1D (page 40). 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). <class_id> – The number of the switch's hardware priority queue. The switch has n+1 hardware priority queues available. They are numbered between 0 (the lowest priority) and n (the highest priority).
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To configure 802.1p user priority:

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

 Success.

DGS-3224SR:4#
```

show 802.1p user_priority

Purpose	Used to display the current 802.1p user 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 current 802.1p user priority:

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


QOS Class of Traffic

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

```
DGS-3224SR:4#
```

config 802.1p default_priority

Purpose	Used to configure the 802.1p default priority settings on the switch. If an untagged packet is received by the switch, the priority configured with this command will be written to the packet's priority field.
Syntax	**config 802.1p default_priority [<portlist>|all] <priority 0-7>**
Description	This command allows 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 portlist is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the portlist range are separated by a hyphen. For example, 1:3 would specify switch number 1, port 3; 2:4 specifies switch number 2, port 4. Thus, 1:3-2:4 specifies all of the ports between switch 1,

config 802.1p default_priority	
	port 3 and switch 2, 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.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To configure 802.1p default priority:

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

 Success.

DGS-3224SR:4#
```

show 802.1p default_priority	
Purpose	Used to display the current default priority settings on the switch.
Syntax	**show 802.1p default_priority** {**<portlist>**}

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-3224SR:4# show 802.1p default_priority
Command: show 802.1p default_priority

 Port   Priority
 -----  --------
 1:1    5
 1:2    5
 1:3    5
 1:4    5
 1:5    5
 1:6    5
 1:7    5
 1:8    5
 1:9    5
 1:10   5
 1:11   5
 1:12   5
 1:13   5
 1:14   5
 1:15   5
 1:16   5
 1:17   5
```

```
1:18   5
1:19   5
1:20   5
```

enable hol_prevention

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

Example Usage:

To enable HOL prevention:

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

 Success.

DGS-3224SR:4#
```

disable hol_prevention

Purpose	Used to disable HOL prevention.

disable hol_prevention

Syntax	**disable hol_prevention**
Description	The disable hol_prevention command disables Head of Line prevention.
Parameters	none.
Restrictions	You must have administrator privileges.

Example Usage:

To disable HOL prevention:

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

 Success.

DGS-3224SR: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-3224SR:4#show hol_prevention
Command: show hol_prevention

Device HOL Prevention State Disabled

DGS-3224SR: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. rx – Allows the mirroring of only packets received (flowing into) the port or ports in the port list. The portlist is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the portlist range are separated by a hyphen. For example, 1:3 would specify switch number 1, port 3; 2:4 specifies switch number 2, port 4. Thus, 1:3-2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4, in numerical order. rx – Allows the mirroring of only packets received by (flowing into) the port or ports on the portlist.

config mirror port	
	tx – Allows the mirroring of only packets sent by (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 add the mirroring ports:

```
DGS-3224SR:4#config mirror port 1:6 add source ports 1:1-1:5
both
Command: config mirror port 1:6 add source ports 1:1-1:5 both

Success.

DGS-3224SR:4#
```

config mirror delete	
Purpose	Used to delete a port mirroring configuration|
Syntax	**config mirror port <port> delete source ports <portlist> [rx|tx|both]**
Description	This command is used to delete a previously entered port mirroring

config mirror delete	
	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 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-3224SR:4#config mirror port 1:5 delete source
ports 1:2-1:3 both
Command: config mirror port 1:5 delete source ports
1:2-1:3 both

Success.
```

```
DGS-3224SR:4#
```

enable mirror

Purpose	Used to enable a previously entered port mirroring configuration.
Syntax	**enable mirror**
Description	This command, combined with the **disable mirror** command below, allows 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	none.

Example Usage:

To enable mirroring configurations:

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

 Success.

DGS-3224SR:4#
```

disable mirror

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 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-3224SR:4#disable mirror
Command: disable mirror

 Success.

DGS-3224SR:4#
```

show mirror

Purpose	Used to show the current port mirroring configuration on the switch.

show mirror

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-3224SR:4#
DGS-3224SR:4#show mirror
Command: show mirror

Current Settings
Mirror Status: Disabled
Target Port  : 1:6
Mirrored Port
        RX: 1:1-1:5
        TX: 1:1-1:5
DGS-3224SR:4#
```

15

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> {tag <vlanid1-4094> | advertisement}
delete vlan	<vlan_name>
config vlan	<vlan_name> add [tagged|untagged|forbidden] | delete] <portlist> | advertisement [enabled | disabled]
config gvrp	[<portlist> | all {state [enabled|disabled] | ingress_checking [enabled|disabled]}
enable gvrp	
disable gvrp	
show vlan	{<vlan_name>}
show gvrp	{<portlist>}

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

create vlan	
Purpose	Used to create a VLAN on the switch.
Syntax	**create vlan <vlan_name> {tag <vlanid>|advertisement}**
Description	This command allows you to create a VLAN on the switch.
Parameters	<vlan_name> – The name of the VLAN to be created. <vlanid> – The VLAN ID of the VLAN to be created. Range is 1-4094. advertisement – Specifies the VLAN as able to join GVRP. If this parameter is not set, the switch cannot be configured to have forbidden ports.
Restrictions	Each VLAN name can be up to 32 characters. If the VLAN is not given a tag, it is a port-based VLAN. Only administrator-level users can issue this command.

Example Usage:

To create a VLAN v1, tag 2:

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

 Success.
```

```
DGS-3224SR:4#
```

delete vlan

Purpose	Used to delete a previously configured VLAN on the switch.
Syntax	**delete vlan <vlan_name>**
Description	This command will delete a previously configured VLAN on the switch.
Parameters	<vlan_name> – The VLAN name of the VLAN you want to delete.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To remove a vlan v1:

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

 Success.

DGS-3224SR:4#
```

config gvrp

Purpose	Used to configure GVRP on the switch.
Syntax	**config gvrp [<portlist>|all] [state [enable|disable]] [ingress_checking [enable|disable]]**
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.
Parameters	<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. rx – Allows the mirroring of only packets received (flowing into) the port or ports in the port list. The portlist is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the portlist range are separated by a hyphen. For example, 1:3 would specify switch number 1, port 3; 2:4 specifies switch number 2, port 4. Thus, 1:3-2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4, in numerical order. all – Specifies all of the ports on the switch.

config gvrp	
	state [enabled|disabled] – Enables or disables GVRP for the ports specified in the port list. ingress_checking [enabled|disabled] – Enables or disables ingress checking for the specified port list.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To sets the ingress checking status and the GVRP status:

```
DGS-3224SR:4#config gvrp 1:1-1:5 state enabled
Command: config gvrp 1:1-1:5 state enabled

 Success.

DGS-3224SR:4#
```

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

enable 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-3224SR:4#enable gvrp
Command: enable gvrp

 Success.

DGS-3224SR: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 on the switch – without changing the GVRP configuration for each port on the switch.
Parameters	none.

disable gvrp

Restrictions	Only administrator-level users can issue this command.

Example Usage:

To disable the Generic VLAN Registration Protocol (GVRP):

DGS-3224SR:4#disable gvrp
Command: disable gvrp

Success.

DGS-3224SR:4#

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

 Success.

DGS-3224SR:4#
```

show vlan

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

show vlan	
	each port that is a member of the VLAN.
Parameters	<vlan_name> – 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-3224SR:4#show vlan
Command: show vlan

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

VID           : 4094     VLAN Name      : george
VLAN TYPE     : static   Advertisement  : Disabled
Member ports  :
  Static ports  :
Untagged ports  :
Forbidden ports :


Total Entries : 2

DGS-3224SR:4#
```

show gvrp	
Purpose	Used to display the GVRP status for a port list on the switch.
Syntax	**show gvrp** {**<portlist>**}
Description	This command displays the
Parameters	<portlist> – The portlist is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the portlist range are separated by a hyphen. For example, 1:3 would specify switch number 1, port 3; 2:4 specifies switch number 2, port 4. Thus, 1:3-2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4, in numerical order.
Restrictions	none.

Example Usage:

To display 802.1Q port setting:

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

```
Global GVRP : Disabled

 Port   PVID     GVRP      Ingress Checking
 -----  --------  --------  --------------------
 1:1    1       Enabled       Enabled
 1:2    1       Enabled       Enabled
 1:3    1       Enabled       Enabled
 1:4    1       Enabled       Enabled
 1:5    1       Enabled       Enabled
 1:6    1       Enabled       Enabled
 1:7    1       Enabled       Enabled
 1:8    1       Enabled       Enabled
 1:9    1       Enabled       Enabled
 1:10   1       Enabled       Enabled
 1:11   1       Enabled       Enabled
 1:12   1       Enabled       Enabled
 1:13   1       Enabled       Enabled
 1:14   1       Enabled       Enabled
 1:15   1       Enabled       Enabled
 1:16   1       Enabled       Enabled
 1:17   1       Enabled       Enabled
 1:18   1       Enabled       Enabled
DGS-3224SR:4#
```

16

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> {type [lacp | static]}
delete link_aggregation	group_id <value>
config link_aggregation	group_id <value> {master_port <port> | ports <portlist> | state [enabled|disabled]
config link_aggregation algorithm	[mac_source | mac_destination | mac_source_dest | ip_source | ip_destination | ip_source_dest
show link_aggregation	{group_id <value> | algorithm}
Config lacp_port	<portlist> mode(1) [active(3) | passive(4)
Show lacp_port	{<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>**
Description	This command will create a link aggregation group.
Parameters	<value> – Specifies the group id. The switch allows up to 32 link aggregation groups to be configured. The group number identifies each of the groups.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To create link aggregation group:

```
DGS-3224SR:4#create link_aggregation group_id 1 type
lacp
Command: create link_aggregation group_id 1 type lacp

 Success.

DGS-3224SR:4#
```

delete link_aggregation group_id	
Purpose	Used to delete a previously configured link aggregation group.

delete link_aggregation group_id	
Syntax	**delete link_aggregation group_id <value>**
Description	This command is used to delete a previously configured link aggregation group.
Parameters	<value> – Specifies the group id. The switch allows up to 32 link aggregation groups to be configured. The group number identifies each of the groups.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To delete link aggregation group:

```
DGS-3224SR:4#delete link_aggregation group_id 1
Command: delete link_aggregation group_id 1

 Success.

DGS-3224SR:4#
```

config link_aggregation	
Purpose	Used to configure a previously created link aggregation group.
Syntax	**config link_aggregation group_id <value> {master_port <port>|ports <portlist>|**

config link_aggregation	
	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> – 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> – The portlist is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the portlist range are separated by a hyphen. For example, 1:3 would specify switch number 1, port 3; 2:4 specifies switch number 2, port 4. Thus, 1:3-2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4, in numerical order. state [enabled|disabled] – Allows you to enable or disable the specified link

config link_aggregation	
	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 10:

```
DGS-3224SR:4#config link_aggregation group_id 1 master_port 1:10 ports 1:5-1:10


Command: config link_aggregation group_id 1 master_port 1:10 ports 1:5-1:10

Success.

DGS-3224SR: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]**

config link_aggregation algorithm	
Description	This command configures to part of the packet examined by the switch when selecting the egress port for transmitting load-sharing data. This feature is only available using the address-based load-sharing algorithm.
Parameters	mac_source – Indicates that the switch should examine the MAC source address. mac_destination – Indicates that the switch should 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-3224SR:4#config link_aggregation algorithm
mac_source_dest
Command: config link_aggregation algorithm
mac_source_dest

 Success.

DGS-3224SR:4#
```

show link_aggregation

Purpose	Used to display the current link aggregation configuration on the switch.
Syntax	**show link_aggregation** {**group_id <value>**|**algorithm**}
Description	This command will display the current link aggregation configuration of the switch.
Parameters	<value> – Specifies the group id. The switch allows up to 32 link aggregation groups to be configured. The group number identifies each of the groups. 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-3224SR:4#show link_aggregation
Command: show link_aggregation

Link Aggregation Algorithm = MAC-source-dest
Group ID      : 1
Type          : LACP
Master Port   : 1:10
Member Port   : 1:5-1:10
Active Port   :
Status        : Disabled
Flooding Port : X

DGS-3224SR:4#
```

config lacp_port

Purpose	Used to apply the Link Aggregation Control Protocol (LACP) to a port or group of ports..
Syntax	**Config lacp_port <portlist> mode(1) [active(3) | passive(4)]**
Description	This command will apply LACP to a port or group of ports.
Parameters	<portlist> – The portlist is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the portlist range are separated by a

config lacp_port	
	hyphen. For example, 1:3 would specify switch number 1, port 3; 2:4 specifies switch number 2, port 4. Thus, 1:3-2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4, in numerical order. Mode: either active or passive mode
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To config LACP for port 1:5 as active:

```
DGS-3224SR:4#
DGS-3224SR:4#config lacp_port 1:5 mode active
Command: config lacp_port 1:5 mode active

 Success.

DGS-3224SR:4#
```

show lacp_port	
Purpose	Used to display the Link Aggregation Control Protocol (LACP) status.

show lacp_port	
	Control Protocol (LACP) status.
Syntax	**show lacp_port** {**<portlist>**}
Description	This command will show LACP status of a port or group of ports
Parameters	<portlist> – The portlist is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the portlist range are separated by a hyphen. For example, 1:3 would specify switch number 1, port 3; 2:4 specifies switch number 2, port 4. Thus, 1:3-2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4, in numerical order. Mode: either active or passive mode
Restrictions	None.

Example Usage:

To display LACP for port 1:5:

```
DGS-3224SR:4#show lacp_port 1:5
Command: show lacp_port 1:5
```

```
Port     Activity

-----    --------
1:5      Active
DGS-3224SR:4#
```

17

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	[{ipaddress <network_address> | vlan <vlan_name> | state [enabled|disabled]} | bootp | dhcp]
show ipif	<ipif_name>

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

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

config ipif System

config ipif System

Purpose	Used to configure the System IP interface.
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 [enabled|disabled] – 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-3224SR:4#config ipif System ipaddress 10.52.19.2/8
vlan george state enabled


Command: config ipif System ipaddress 10.52.19.2/8
vlan george state enabled

 Success.

DGS-3224SR: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.
Restrictions	none.

Example Usage:

To display IP interface settings:

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

 IP Interface Settings

 Interface Name : System
 IP Address     : 10.52.19.2      (MANUAL)
 Subnet Mask    : 255.0.0.0
 VLAN Name      : george
 Admin. State   : Enabled
 Link Status    : Link DOWN
 Member Ports   :

Total Entries : 1

DGS-3224SR:4#
```

18

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_name32> | all] {host_timeout <sec> | router_timeout <sec> | leave_timer <sec> state [enabled|disabled]}
config igmp_snooping querier	[<vlan_name> | all] {query_interval <sec> | max_response_time <sec> | robustness_variable <value> | last_member_query_interval <sec>| state [enabled|disabled]
config router_ports	<vlan_name> [add|delete] <portlist>
enable igmp snopping	forward_mcrouter_only
show igmp snooping	vlan <vlan_name>
show router ports	vlan {<vlan_ name>} {static | dynamic |

Command	Parameters
	forbidden}
show igmp_snooping group	{vlan <vlan_name 32>}
config router_ports_forbidden	<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 configure IGMP snooping on the switch.
Syntax	**config igmp_snooping [<vlan_name>|all] {host_timeout <sec>|router_timeout <sec>|leave_timer <sec>|state [enabled|disabled]}**
Description	This command allows you to configure IGMP snooping on the switch|
Parameters	<vlan_name> – The name of the VLAN for which IGMP snooping is to be configured. host_timeout <sec> – 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. Maximum

config igmp_snooping	
	value is 16711450. route_timeout <sec> – Specifies the maximum amount of time a route will can be a member of a multicast group without the switch receiving query. The default is 260 seconds. Maximum value is 16711450. leave_timer <sec> – Leave timer. The default is 2 seconds. Maximum value is 16711450. state [enabled|disabled] – 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-3224SR:4#config igmp_snooping default
host_timeout 250 state enabled
Command: config igmp_snooping default host_timeout
250 state enabled

 Success.

DGS-3224SR:4#
```

config igmp_snooping querier

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>|all] {query_interval <sec>|max_response_time <sec>|robustness_variable <value>|last_member_query_interval <sec>|state [enable|disable]}**
Description	This command configures IGMP snooping querier.
Parameters	<vlan_name> – The name of the VLAN for which IGMP snooping querier is to be configured. query_interval <sec> – Specifies the amount of time in seconds between general query transmissions. The default setting is 125 seconds. Maximum value is 65535. max_response_time <sec> – Specifies the maximum time in seconds to wait for reports from members. The default setting is 10 seconds. Maximum value is 25. robustness_variable <value> – Provides fine-tuning to allow for expected packet loss on a subnet. The value of the robustness variable is used in calculating

config igmp_snooping queri :r	
	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. Maximum value is 255. last_member_query_interval <sec> – The maximum amount of time between group-

config igmp_snooping querier	
	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. Maximum value is 25. state [enabled|disabled] – 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 the igmp snooping querier:

```
UserName:
PassWord:
DGS-3224SR:4#config igmp_snooping querier default
query_interval 125 state enabled
Command: config igmp_snooping querier default
query_interval 125 state enabled

 Success.

DGS-3224SR:4#
```

config router_ports	
Purpose	Used to configure ports as router ports.

config router_ports

Syntax	**config router_ports <vlan_name> [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> – The name of the VLAN on which the router port resides. Maximum 32 characters. <portlist> – Specifies a range of ports which will be configured as router ports. The portlist is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the portlist range are separated by a hyphen. For example, 1:3 would specify switch number 1, port 3; 2:4 specifies switch number 2, port 4. Thus, 1:3-2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4, in numerical
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To set up static router ports:

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

 Success.

DGS-3224SR:4#
```

config router_ports_forbidden

Purpose	Used to configure ports as forbidden ports.
Syntax	**config router_ports_forbidden <vlan_name 32> [add | delete] <portlist>**
Description	This command allows you to designate a range of ports as being forbidden ports.
Parameters	<vlan_name> – The name of the VLAN on which the router port resides. Maximum 32 characters. <portlist> – Specifies a range of ports which will be configured as router ports. The portlist is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the portlist range are separated by a hyphen. For example, 1:3 would specify switch number 1, port 3; 2:4 specifies switch number 2, port 4. Thus, 1:3-2:4 specifies all of the ports

config router_ports_forbidd(n	
	between switch 1, port 3 and switch 2, port 4, in numerical
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To configure ports 1-5 as forbidden ports:

```
DGS-3224SR:4#config router_ports_forbidden default
add 1:1-1:5
Command: config router_ports_forbidden default add
1:1-1:5

 Success.
```

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 multicast traffic to any IP router.

enable igmp_snooping	
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-3224SR:4#enable igmp_snooping
Command: enable igmp_snooping

 Success.

DGS-3224SR: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

disable igmp_snooping	
	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-3224SR:4#disable igmp_snooping
Command: disable igmp_snooping

 Success.
DGS-3224SR:4#
```

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

show igmp_snooping

Restrictions none.

Example Usage:

To show IGMP snooping:

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

IGMP Snooping Global State : Enabled
Multicast router Only      : Disabled

VLAN  Name                 : default
Query Interval             : 125
Max Response Time          : 10
Robustness Value           : 2
Last Member Query Interval : 1
Host Timeout               : 250
Route Timeout              : 260
Leave Timer                : 2
Querier State              : Enabled
Querier Router Behavior    : Non-Querier
State                      : Enabled


VLAN  Name                 : george
Query Interval             : 125
Max Response Time          : 10
Robustness Value           : 2
Last Member Query Interval : 1
Host Timeout               : 260

DGS-3224SR: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>}**
Description	This command will display the current IGMP snooping group configuration on the swtich.
Parameters	<vlan_name> – The name of the VLAN for which you want to view IGMP snooping group configuration information.
Restrictions	none.

Example Usage:

To show IGMP snooping group:

```
DGS-3224SR: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        : 5
Port Member    : 1:1

VLAN Name      : default
Multicast group: 224.0.0.9
MAC address    : 01-00-5E-00-00-09
```

```
Reports       : 9
Port Member   : 1:1

VLAN Name     : default
Multicast group: 224.0.0.18
MAC address   : 01-00-5E-00-00-12
Reports       : 4
Port Member   : 1:1

VLAN Name     : default
Multicast group: 224.0.0.251
MAC address   : 01-00-5E-00-00-FB
Reports       : 4

DGS-3224SR:4#
```

show router_ports

Purpose	Used to display the currently configured router ports on the switch.
Syntax	**show router_ports** {**vlan <vlan_name>**} {**static|dynamic | forbidden**}
Description	This command will display the router ports currently configured on the switch.
Parameters	<vlan_name> – 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. Forbidden – Displays router ports

show router_ports	
	configured as forbidden ports.
Restrictions	none.

Example Usage:

To display the router ports:

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

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

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

Total Entries: 2
DGS-3224SR:4#
```

19

802.1X COMMANDS

The DGS-3224SR 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	[loca(1)|radius_eap(4)]
config 802.1x capability	ports [<portlist>|all] [authenticator | none]
show 802.1x auth_protocol	[auth_state | auth_configuration] {ports <portlist>}
config 802.1x auth_parameter	ports [<portlist>|all] [default {direction [both|in] | port_control [force_unauth|auto|force_auth] | quiet_period <sec 0-65535> | tx_period <sec 1-65535> | supp_timeout <sec 1-65535> | server_timeout <sec 1-65535> | max_req <value 1-10> | reauth_period <sec 1-65535> | enable_reauth [enabled|disabled]}]

Command	Parameters
config 802.1x capability	Ports [<portlist> | all] [authenticator | none]
config 802.1x auth_mode	[port_based | mac_based]
config 802.1x init	[port_based ports [<portlist>|all]
config 802.1x reauth	[port_based ports [<portlist>|all]
config radius add	<server_index 1-3> <server_ip> key <passwd 32> [default | {auth_port <udp_port_number> | acct_port <udp_port_number>}]
config radius delete	<server_index 1-3>
config radius	<server_index 1-3> {ipaddress <server_ip> | key <passwd 32> | auth_port <udp_port_number> | acct_port <udp_port_number>
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

Purpose	Used to enable the 802.1x server on the switch.

enable 802.1x	
	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-3224SR:4#enable 802.1x
Command: enable 802.1x

Success.

DGS-3224SR: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 Access control server application on the

disable 802.1x	
	switch.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To disable 802.1x on the switch:

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

Success.

DGS-3224SR: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.
Restrictions	Only administrator-level users can issue this command.

config 802.1x auth_protoco	
	this command.

Example Usage:

To configure 802.1x authentication protocol:

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

Success.

DGS-3224SR: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 portlist is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the portlist range are separated by a hyphen. For example, 1:3 would specify switch number 1, port 3; 2:4 specifies switch number 2, port 4.

config 802.1x capability	
	Thus, 1:3-2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4, in numerical order. all – Specifies all of the ports on the switch. 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-3224SR:4#config 802.1x capability ports 1:1-1:10 
authenticator
Command: config 802.1x capability ports 1:1-1:10 authenticator

Success.

DGS-3224SR: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**

config 802.1x auth_parameter	
	[<portlist>|all] [default|{direction [both|in]|port_control [force_unauth|auto|force_auth]| quiet_period <sec 0-65535>| tx_period <sec 1-65535> | supp_timeout <sec 1-65535> | server_timeout <sec 1-65535> | max_req <value 1-10>|reauth_period <sec 1-65535>|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 portlist is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the portlist range are separated by a hyphen. For example, 1:3 would specify switch number 1, port 3; 2:4 specifies switch number 2, port 4. Thus, 1:3-2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4, in numerical order. all – Specifies all of the ports on the switch. default – Returns all of the ports in the specified range to their 802.1x default settings. direction [both|in] – Determines whether a

config 802.1x auth_parameter	
	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. 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.

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

Example Usage:

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

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

Success.

DGS-3224SR:4#
```

config 802.1x init	
Purpose	Used to initialize the 802.1x functions on a range of ports.
Syntax	**config 802.1x init port_based 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 portlist is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range

config 802.1x init	
	(also separated by a colon) are specified. The beginning and end of the portlist range are separated by a hyphen. For example, 1:3 would specify switch number 1, port 3; 2:4 specifies switch number 2, port 4. Thus, 1:3-2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4, in numerical order. all – Specifies all of the ports on the switch.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

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

```
Command: config 802.1x init port_based ports 1:1-1:15

Success.

DGS-3224SR:4#
```

config 802.1x reauth	
Purpose	Used to configure the 802.1x re-authentication feature of the switch.
Syntax	**config 802.1x reauth port_based ports [<portlist>|all]**
Description	The config 802.1x reauth command is used to enable the 802.1x re-authentication feature on the switch.

config 802.1x reauth	
Parameters	<portlist> – Specifies a range of ports. The portlist is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the portlist range are separated by a hyphen. For example, 1:3 would specify switch number 1, port 3; 2:4 specifies switch number 2, port 4. Thus, 1:3-2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4, in numerical order. all – Specifies all of the ports on the switch.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To configure 802.1x reauthentication for ports 1-15:

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

Success.

DGS-3224SR:4#
```

config radius add	
Purpose	Used to configure the settings the switch will use to communicate with a Radius

config radius add

	will use to communicate with a Radius server.
Syntax	**config radius add <server_index 1-3> <server_ip> key <passwd 32> [default|{auth_port <udp_port_number>| acct_port <udp_port_number>}]**
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 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> – The UDP port number for authentication requests. The default is 1812. acct_port <udp_port_number> – The UDP

config radius add	
	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-3224SR: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-3224SR:4#
```

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

config radius delete

this command.

Example Usage:

To delete previously configured Radius server communication settings:

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

 Success.

DGS-3224SR: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>|acct_port <udp_port_number>}**
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.

config radius	
	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> – The UDP port number for authentication requests. The default is 1812. acct_port <udp_port_number> – 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-3224SR: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-3224SR:4#
```

show radius	
Purpose	Used to display the current Radius configurations on the switch.

show 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-3224SR:4#show radius
Command: show radius

Idx IP Address      Auth- Acct- Status       Key
                    Port  Port
                    No.   No.
--- --------------- ----- ----- ------------ --------------------------------
1   10.48.74.121    1812  1813  Active       dlink

Total Entries : 1
DGS-3224SR: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

show 802.1x user	
	display the current configuration of the 802.1x Port-based Network Access Control server application on the switch.
Parameters	None.
Restrictions	None.

Example Usage:

To show the 802.1x user:

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

Current Accounts:
Username        Password
---------------  ---------------
george          Go
lise            lise

Total Entries:2

DGS-3224SR: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 many as 15 alphanumeric characters.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To create an 802.1x user:

```
DGS-3224SR:4#create 802.1x user jill
Command: create 802.1x user jill

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

DGS-3224SR: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-3224SR:4#delete 802.1x user jill
Command: delete 802.1x user jill

Success.
```

```
DGS-3224SR: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 portlist is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the portlist range are separated by a hyphen. For example, 1:3 would specify switch number 1, port 3; 2:4 specifies switch number 2, port 4. Thus, 1:3-2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4, in numerical order.
Restrictions	None.

Example Usage:

To display authentication statistics:

```
DGS-3224SR:4#show auth_statistics ports 1
Command: show auth_statistics

Port number : 1:1
```

```
Port number : 1:1

EapolFramesRx                0
EapolFramesTx                244
EapolStartFramesRx           0
EapolReqIdFramesTx           163
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 portlist is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range

show auth_diagnostics	
	(also separated by a colon) are specified. The beginning and end of the portlist range are separated by a hyphen. For example, 1:3 would specify switch number 1, port 3; 2:4 specifies switch number 2, port 4. Thus, 1:3-2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4, in numerical order.
Restrictions	None.

Example Usage:

To display authentication diagnostics statistics:

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

Port number : 1:1

 EntersConnecting                250
 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>}**
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 portlist is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the portlist range are separated by a hyphen. For example, 1:3 would specify switch number 1, port 3; 2:4 specifies switch number 2, port 4. Thus, 1:3-2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4, in numerical order.
Restrictions	None.

Example Usage:

To display authentication session statistics:

```
DGS-3224SR:4# show auth_session_statistics ports 1
Command: show auth_session_statistics port 1:1


Port number : 1:1

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-3224SR:4# show radius auth_client
Command: show radius auth_client

radiusAuthClient ==>
radiusAuthClientInvalidServerAddresses   0
radiusAuthClientIdentifier              D-Link

radiusAuthServerEntry ==>
radiusAuthServerIndex :1

radiusAuthServerAddress                 10.48.74.121
radiusAuthClientServerPortNumber        1812
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.

show radius acct_client	
Parameters	None.
Restrictions	Only administrator-level users can issue this command. ???

Example Usage:

To display the Radius account client statistics:

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

radiusAcctClient ==>
 radiusAcctClientInvalidServerAddresses   0
 radiusAcctClientIdentifier              D-Link

 radiusAuthServerEntry ==>
 radiusAccServerIndex : 1

 radiusAccServerAddress                10.48.74.121
 radiusAccClientServerPortNumber        1813
 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
```

20

ACCESS CONTROL LIST (ACL) COMMANDS

The DGS-3224SR 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 | [icmp {type | code} | igmp {type} | tcp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | udp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xfff>} | 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 1-50> [ethernet {vlan <vlan_name 32> | source_mac <macaddr> | destination_mac <macaddr> | 802.1p <value 0-7> | ethernet type <hex 0x0-0xfff>}

Command	Parameters
	| ip {vlan <vlan_name 32> | source_ip <ipaddr> | destination_ip <ipaddr> | dscp <value0-63> | icmp {type <value 0-255> | code <value 0-255>} | igmp {type <value 0-255>} **| tcp {src_port <value 0-65535> | dst_port <value 0-65535>} | udp {src_port <value 0-65535> | dst_port <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 1-50>]**

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 eight (8) 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	**[ethernet {vlan | source_mac <macmask> | destination_mac <macmask> | 802.1p | ethernet_type}| ip {vlan | source_ip_mask <netmask> | destination_ip_mask <netmask> | dscp | [icmp {type | code} | igmp {type} | tcp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | 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>}**
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.

create access_profile

	Masks can be entered that will be combined with the values the switch finds in the specified frame header fields. Specific values for the rules are entered using the config access_profile command, below.
Parameters	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.

create access_profile

destination_ip_mask <netmask> – Specifies an IP address mask for the destination IP address.

dscp – Specifies that the switch will examine the DiffServ Code Point (DSCP) field in each frame's header.

icmp – Specifies that the switch will examine the Internet Control Message Protocol (ICMP) field in each frame's header.

type – Specifies that the switch will examine each frame's ICMP Type field.

code – Specifies that the switch will examine each frame's ICMP Code field.

igmp – Specifies that the switch will examine each frame's Internet Group Management Protocol (IGMP) field.

type – Specifies that the switch will examine each frame's IGMP Type field.

tcp – Specifies that the switch will examine each frames Transport Control Protocol (TCP) field.

src_port_mask <hex 0x0-0xffff> – Specifies a TCP port mask for the source port.

dst_port_mask <hex 0x0-0xffff> – Specifies a TCP port mask for the destination port.

udp – Specifies that the switch will examine each frame's Universal Datagram Protocol (UDP) field.

create access_profile	
	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 1-8> – 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 access list rules:

```
Command: create access_profile ethernet vlan source_mac 00-
00-00-00-00-01 destin
ation_mac 00-00-00-00-00-02 802.1p ethernet_type permit
profile_id 8
```

```
Success.

DGS-3224SR:4#
```

delete access_profile

Purpose	Used to delete a previously created access profile.
Syntax	**delete access_profile [profile_id <value 1-8>]**
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-3224SR:4#delete access_profile profile_id 8
Command: delete access_profile profile_id 8

Success.

DGS-3224SR: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	**profile_id <value 1-8> [add access_id <value 1-50> [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 <value0-63> | icmp {type <value 0-255> | code <value 0-255>} | igmp {type <value 0-255>}| tcp {src_port <value 0-65535> | dst_port <value 0-65535>} | udp {src_port <value 0-65535> | dst_port <value 0-65535>} | protocol_id <value 0-255> {user_define <hex 0x0-0xffffffff>}]}] {priority <value 0-7>**
Description	The config access_profile command is used to configure an access profile on the switch

config access_profile

	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 1-8> –
	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.
	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.

config access_profile

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 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.

config access_profile

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 field in each packet and if this field contains the value entered here, apply the following rules.

user_define <hex 0x0-0xffffff> – Specifies a mask to be combined with the value found in the frame header using a logical AND operaiton.

priority <value 0-7> – Specifies that the

config access_profile	
	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 access list entry:

```
DGS-3224SR:4#config access_profile profile_id 8 add access_id
1 ethernet vlan de
        config access_profile profile_id 8 add access_id 1
ethernet vlan de
fault ethernet_type 0x800
Command: config access_profile profile_id 8 add access_id 1
```

```
ethernet vlan defaul
t ethernet_type 0x800

 Success.

DGS-3224SR: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	Only administrator-level users can issue this command.

Example Usage:

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

```
Access Profile  ID:8                    Mode : Permit
                                    TYPE : Ethernet
================================================================
=
```

```
MASK Option  VLAN        Source MAC        Destination MAC   802.1p  Eth

                    00-00-00-00-00-01  00-00-00-00-00-02

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

 Access ID

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

 1           default      00-00-00-00-00-00  00-00-00-00-00-00  0       0x800

==============================================================
=


Total Entries: 1

DGS-3224SR:4#
```

21

TRAFFIC SEGMENTATION COMMANDS

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

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

config traffic_segmentation

Purpose	Used to configure the traffixc segmentation.
Syntax	**config traffic_segmentation <portlist> forward_list [all | null | <portlist>]**
Description	This command configures traffic segmentation.
Parameters	<portlist> - Specifies a range of ports. The portlist is specified by listing the lowest

config traffic_segmentation	
	switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the portlist range are separated by a hyphen. For example, 1:3 would specify switch number 1, port 3; 2:4 specifies switch number 2, port 4. Thus, 1:3-2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4, in numerical order. forward_list – specifies a range of port forwarding domain. all – includes entire range ofports null – specifies a range of port forwarding domain as null.
Restrictions	Administrator privileges are needed to issue this command.

Usage Example:

To configure traffic segmentation:

```
DGS-3224SR:4#config traffic_segmentation 1:1-1:10 forward_list
all
Command: config traffic_segmentation 1:1-1:10 forward_list all

 Success.

DGS-3224SR:4#
```

show traffic_segmentation	
Purpose	Used to display the current traffic segmentation table.
Syntax	**show traffic_segmentation**
Description	This command will display the current traffic segmentation table.
Parameters	<portlist> - Specifies a range of ports. The portlist is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the portlist range are separated by a hyphen. For example, 1:3 would specify switch number 1, port 3; 2:4 specifies switch number 2, port 4. Thus, 1:3-2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4, in numerical order.
Restrictions	none.

Usage Example:

To display the traffic segmentation table:

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

Traffic Segmentation Table
```

```
Port  Forward Portlist
----  --------------------------------------------------
1:1    1:1-1:24
1:2    1:1-1:24
1:3    1:1-1:24

DGS-3224SR:4#
```

22

STACKING COMMANDS

Command	Parameters
config box_priority	current_box_id <value 1-12> priority <value1-16>
config box_id	current_box_id <value1-12> new_box_id [auto|1|2|3|4|5|6|7|8|9|10|11|12]
config box_type	current_box_id <value1-12> type [DGS-3224SR | DES-3352SR | BOX_NOTEXIST]
config all_boxes_id	[static_mode | auto_mode]
show stack_information	

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

config box_priority

Purpose	Used to configure box priority, which determines which box becomes master. Lower numbers have higher priority..
Syntax	**current_box_id <value 1-12> priority <value1-16>**
Description	This command configures box (switch) priority.

config box_priority	
	priority.
Parameters	current_box_id – identifies the switch being configured. Range is 1-12. priority – assigns a priority value to the box, with lower numbers having higher priority. Range is 1-16.
Restrictions	Administrator privileges are needed to issue this command.

Usage Example:

To configure box priority:

```
DGS-3224SR:4#config box_priority current_box_id 1 priority 1
Command: config box_priority current_box_id 1 priority 1

Success.

DGS-3224SR:4#
```

config box_id	
Purpose	Used to configure box ID. Users can use this command to reassign box Ids.
Syntax	**current_box_id <value1-12> new_box_id [auto|1|2|3|4|5|6|7|8|9|10|11|12]**
Description	This command will assign box Ids to switches in a stack.

config box_id	
Parameters	current_box_id – identifies the switch being configured. Range is 1-12. new_box_id – the new Id being assigned to the box. Range is 1-12. auto – allows the box ID to be assigned automatically.
Restrictions	Administrator privileges are needed to issue this command.

Usage Example:

To change a box ID:

```
DGS-3224SR:4#config box_id current_box_id 1 new_box_id 2
Command: config box_id current_box_id 1 new_box_id 2

Success.

DGS-32S24R:4#
```

config box_type	
Purpose	Used to configure box type.
Syntax	**current_box_id <value1-12> type [DGS-3224SR | DES-3352SR |**

config box_type	
	BOX_NOTEXIST]
Description	This command will pre-assign the box type of switches in a stack.
Parameters	current_box_id – identifies the switch being configured. Range is 1-12. DGS-3224SR – DES-3352SR – BOX_NOTEXIST – identifies a switch which may be added to the stack in future. A box_type may be assigned to this box, in effect to pre-configure it as it is added to the stack. If box_type is not assigned, box is identified as BOX_NOTEXIST and box type will be identified automatically.
Restrictions	Administrator privileges are needed to issue this command.

Usage Example:

To configure box type:

```
DGS-3224SR:4#config box_type current_box_id 3 type
BOX_NOTEXIST
Command: config box_type current_box_id 3 type
BOX_NOTEXIST

 Success.

DGS-3224SR:4#
```

config all_boxes_id	
Purpose	Used to configure box IDs for switches in a stack.
Syntax	**[static_mode | auto_mode]**
Description	This command will determine the mode of assigning box IDs.
Parameters	static_mode – user assigns box IDs auto_mode – box Ids are assigned automatically
Restrictions	Administrator privileges are needed to issue this command.

Usage Example:

To configure box type:

```
DGS-3224SR:4#config all_boxes_id auto_mode
Command: config all_boxes_id auto_mode

 Success.

DGS-3224SR:4#
```

show stack_information

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

Usage Example:

To display stack information:

```
DGS-3224SR:4#show stack_information
Command: show stack_information

 Box User              Prio- Prom     Runtime   H/W
 ID  Set  Type       Exist rity  version  version   version
 --- ---- ----------- ----- ----- -------- -------- --------
  1 AUTO DGS-3224SR  exist     1 1.00-B03 1.00-B14      2A1
  2    - USR-NOT-CFG no
  3    - USR-NOT-CFG no
  4    - USR-NOT-CFG no
  5    - USR-NOT-CFG no
  6    - USR-NOT-CFG no
  7    - USR-NOT-CFG no
  8    - USR-NOT-CFG no
  9    - USR-NOT-CFG no
 10    - USR-NOT-CFG no
 11    - USR-NOT-CFG no
 12    - USR-NOT-CFG no
```

```
 ---------------------------------------------------------------------
Topology    :DUPLEX_CHAIN
My Box ID   :1
Current state:MASTER
Box Count   :1

DGS-3224SR:4#
```

23

ROUTING TABLE COMMANDS

Command	Parameters
create iproute default	<ipaddr> {metric 1-65535}
delete iproute default	
show iproute	

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

create iproute default

Purpose	Used to create a default IP route entry.
Syntax	**Create iproute default <ipaddr> {metric 1-65535}**
Description	This command creates a default IP route entry.
Parameters	default – creates a default IP route entry.

create iproute default	
	<ipaddr> – The IP address for the next hop router. <metric 1-65535> – The default setting is 1.
Restrictions	Administrator privileges are needed to issue this command.

Usage Example:

To create an IP route for the routing table:

```
DGS-3224SR:4#create iproute default 10.52.19.2
Command: create iproute default 10.52.19.2

Success.

DGS-3224SR:4#
```

delete iproute default	
Purpose	Used to delete an IP route entry from the switch's IP routing table.
Syntax	**delete iproute default**
Description	This command will delete an existing entry from the switch's IP routing table.
Parameters	default – deletes a default IP route entry.

delete iproute default	
Restrictions	Only administrator-level users can issue this command.

Usage Example:

To delete the default IP route from the switch's routing table:

```
DGS-3224SR:4#delete iproute default
Command: delete iproute default

Success.

DGS-3224SR:4#
```

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

show iproute

Restrictions None.

Usage Example:

To display the switch's routing table:

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


Routing Table

IP Address/Netmask Gateway       Interface    Hops     Protocol
------------------ ------------- ------------ -------- --------
10.0.0.0/8         0.0.0.0       System       1        Local

Total Entries : 1

DGS-3224SR:4#
```

24

ARP COMMAND

show arpentry	
Purpose	Used to display the ARP table.
Syntax	**show arpentry {ipif <ipif_name12> | ipaddress <ipaddr> | static}**
Description	This command will display the Address Resolution Protocol (ARP) table.
Parameters	ipif_name – the name of the IP interface that the end node or station for which the ARP entry was made, resides on. <ipaddr> - the IP address of the end node or station static – displays the static entries to the ARP table
Restrictions	None.

Usage Example:

To display the ARP table for a specific IP address:

```
DGS-3224SR:4#show arpentry ipaddress 10.52.19.2
Command: show arpentry ipaddress 10.52.19.2


 ARP Aging Time : 20

Interface     IP Address      MAC Address       Type
------------  --------------  ----------------  --------------
System        10.52.19.2      00-00-00-52-33-E3  Local

Total Entries: 1

DGS-3224SR:4#
```

25

SNTP COMMANDS

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

Command	Parameters
config sntp	{primary <ipaddr> | secondary <ipaddr> | poll-interval <int 30-99999>}
enable sntp	
disable sntp	
show sntp	
config time	<date ddmthyyyy> <time hh:mm:ss>
config time_zone	{operator [+|-] | hour <gmt_hour 0-13> | min <minute 0-59>}

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

config sntp

config sntp	
Purpose	Used to configure SNTP on the switch.
Syntax	**config sntp** {**primary <ipaddr> | secondary <ipaddr> | poll-interval <int30-99999>**}
Description	This command is used to configure SNTP on the switch.
Parameters	primary – This is the primary server the SNTP information will be taken from. <ipaddr> – The IP address of the primary server. secondary – This is the secondary server the SNTP information will be taken from in the event the primary server is unavailable. <ipaddr> – The IP address for the secondary server. poll-interval – This is the time the SNTP information will be polled. <int 30-99999> – The polling interval ranges from 30 to 99,999 seconds.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To configure SNTP for the primary server for a switch:

```
DGS-3224SR:4#config sntp primary 10.52.19.7
Command: config sntp primary 10.52.19.7

Success.

DGS-3224SR:4#
```

enable sntp

Purpose	Used to enable SNTP on the switch.
Syntax	**enable sntp**
Description	This command enables SNTP on a switch.
Parameters	none.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To enable SNTP on the switch:

```
DGS-3224SR:4#enable sntp
Command: enable sntp

Success.
```

```
DGS-3224SR:4#
```

disable sntp

Purpose	Used to disable SNTP on the switch.
Syntax	**disable sntp**
Description	This command will disable SNTP on the switch.
Parameters	None.
Restrictions	None.

Example Usage:

To disable SNTP on the switch:

```
DGS-3224SR:4#disable sntp
Command: disable sntp

Success.

DGS-3224SR:4#
```

show sntp	
Purpose	Used to show SNTP on the switch.
Syntax	**show sntp**
Description	This command will show SNTP on the switch.
Parameters	None.
Restrictions	None.

Example Usage:

To show SNTP on the switch:

```
DGS-3224SR:4#show sntp
Command: show sntp

   Current Time Scource  : System Clock
   SNTP : Enabled
   SNTP Primary Server   : 10.52.19.7
   SNTP Secondary Server : 0.0.0.0
   SNTP poll interval : 720 sec
DGS-3224SR:4#
```

config time	
Purpose	Used to configure the clock on the switch.
Syntax	**config time <date ddmthyyyy> <time hh:mm:ss>**
Description	This command will set the time on the switch.
Parameters	<date ddmthyyyy> - the date as day, month and year, no spaces <time hh:mm:ss> - the time as hours, minutes and seconds, separated by colons.
Restrictions	Administrator privileges are needed to issue this command.

Example Usage:

To set the time on the switch:

```
DGS-3224SR:4#config time 10oct2003 16:21:30
Command: config time 10oct2003 16:21:30

 Success.

DGS-3224SR:4#
```

config time_zone	
Purpose	Used to configure the time zone on the switch.
Syntax	**config time_zone** {**operator [+|-] hour < gmt_hour 0-13> | min <minute 0-59>**}
Description	This command will set the time zone for the switch.
Parameters	operator – signals addition or subtraction to follow + - add - - subtract gmt_hour – number of hours to or from Greenwich Mean Time (GMT) min – number of minutes
Restrictions	Administrator privileges are needed to issue this command.

Example Usage:

To set the time zone on the switch for Taipei:

```
DGS-3224SR:4#config time_zone operator + hour 8 min 0
Command: config time_zone operator + hour 8 min 0

 Success.

DGS-3224SR:4#
```

config dst

Purpose	Used to configure Daylight Saving Time (DST) on the switch.
Syntax	**config dst** {**disable | repeating** {**s_week <start_week 1-4, last> | s_day <start_day sun-sat> | s_mth <start_mth 1-12> | s_time <start_time hh:mm> | e_week <end_week 1-4, last> | e_day <end_day sun-sat> | e_mth <end_mth 1-12> | e_time <end_time hh:mm> | offset [30|60|90|120]**} | **annual** {**s_date <start_date 1-31> | s_mth <start_mth 1-12> | s_time <start_time hh:mm> | e_date <end_date 1-31> | e_mth <end_mth 1-12> | e_time <end_time hh:mm> | offset [30|60|90|120]**

config dst

Description	This command will enable and configure Daylight Saving Time (DST) settings for the switch.
Parameters	disable – DST is not used in many parts of the world repeating – set these parameters when DST starts on a particular time of year, for example the third Sunday of the fourth month, and ends on the fourth Monday of the tenth month. annual – set these parameters when DST starts and ends on a certain calendar date, for example March 23 to October 10. offset – the amount of time, in minutes, that Daylight Saving Time will be offset from Standard Time.
Restrictions	Administrator privileges are needed to issue this command.

Example Usage:

To set annual DST for Toronto:

```
Command: config dst annual s_date 23 s_mth 3 s_time 00:01
e_date 10 e_mth 10 e_t
ime 00:01 offset 60

 Success.

DGS-3224SR:4#
```

show time

Purpose	Used to display the time, time zone, and DST settings on the switch.
Syntax	**show time**
Description	This command will display the time on the switch.
Parameters	None.
Restrictions	None.

Example Usage:

To display the time on the switch:

```
DGS-3224SR:4#show time
Command: show time

    Current Time Scource  : System Clock
    Boot Time    : 11 Oct 2003  09:30:19
    Current Time : 11 Oct 2003  11:25:28
    Time zone    : GMT +00:00
    Daylight Saving Time  : Disabled
       Offset in minutes : 60
       Repeating    From : Apr 1st  Sun 00:00
                    To   : Oct last Sun 00:00
       Annual       From : 29 Apr 00:00
                    To   : 12 Oct 00:00
DGS-3224SR:4#
```

26

PORT SECURITY COMMANDS

Command	Parameters
config port_security	ports [<portlist> | all] {admin_state [enabled |disabled] | max-learing_addr <max_lock_no> | lock_address_mode [DeleteOnTimeout | DeleteOnReset]}
show port_security	

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

config port_security

Purpose Used to configure port security settings.

config port_security

Syntax	**config port_security ports [<portlist>| all] {admin_state [enable | disable] | max_learning_addr <max_lock_no 0-10> |lock_address_mode [DeleteOnTimeout|DeleteOnReset]}**
Description	This command allows for the configuration of the port security feature. Only the ports listed in the <portlist> are effected.
Parameters	<portlist> – Specifies a range of ports to be configured. The portlist is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the portlist range are separated by a hyphen. For example, 1:3 would specify switch number 1, port 3; 2:4 specifies switch number 2, port 4. Thus, 1:3-2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4, in numerical order. all – configure port security for all ports on the switch. admin_state [enabled|disaled] – enable or disable port security for the listed ports. max_learning_addr <1-10> - use this to limit the number of MAC addresses dynamically listed in the FDB for the ports. lock_address_mode[DeleteOnTimout|DeleteOnReset] – delete FDB dynamic entries for the ports on timeout of the FDB (see Forwarding Database

config port_security	
	Commands). Specify DeleteOnReset to delete all FDB entries, including static entries upon system reset or rebooting.
Restrictions	Only administrator-level users can issue this command.

Usage Example:

To display all of the commands in the CLI:

```
DGS-3224SR:4#config port_security ports 1:5-1:6 admin_state
enabled max_learning
_addr 5 lock_address_mode DeleteOnTimeout
Command: config port_security ports 1:5-1:6 admin_state enabled
max_learning_add
r 5 lock_address_mode DeleteOnTimeout

 Success.

DGS-3224SR:4#
```

show port_security	
Purpose	Used to display the current port security configuration.
Syntax	{**ports <portlist>**}
Description	This command is used to display port security information of the switch ports. The information displayed includes port security admin state, maximum number of

show port_security	
	learning address and lock mode.
Parameters	<portlist> – Specifies a range of ports to be configured. The portlist is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the portlist range are separated by a hyphen. For example, 1:3 would specify switch number 1, port 3; 2:4 specifies switch number 2, port 4. Thus, 1:3-2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4, in numerical order.
Restrictions	none.

Usage Example:

To display the port security configuration:

```
DGS-3224SR:4#show port_security ports 1-5
Command: show port_security ports 1:1-1:5
 Port#   Admin State  Max. Learning Addr.  Lock Address Mode
 -----   -----------  -------------------  -----------------
 1:1     Disabled          1               DeleteOnReset
 1:2     Disabled          1               DeleteOnReset
 1:3     Disabled          1               DeleteOnReset
 1:4     Disabled          1               DeleteOnReset
 1:5     Enabled           5               DeleteOnTimeout
DGS-3224SR:4#
```

27

JUMBO FRAME COMMANDS

enable jumbo_frame	
Purpose	Used to enable jumbo frame.
Syntax	**enable jumbo_frame**
Description	This command configures the jumbo frame setting as enabled.
Parameters	None.
Restrictions	None.

Usage Example:

To enable jumbo frame:

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

 Success.

DGS-3224SR:4#
```

disable jumbo_frame	
Purpose	Used to disable jumbo frame.
Syntax	**disable jumbo_frame**
Description	This command configures the jumbo frame setting as disabled.
Parameters	None.
Restrictions	None.

Usage Example:

To disable jumbo frame:

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

Success.

DGS-3224SR:4#
```

show jumbo_frame	
Purpose	Used to display jumbo frame setting.
Syntax	**show jumbo_frame**
Description	This command displays the jumbo frame setting.

show jumbo_frame	
	setting.
Parameters	None.
Restrictions	None.

Usage Example:

To disable jumbo frame:

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

 Off.

DGS-3224SR: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:	Half-duplex	Full-duplex
Ethernet	10 Mbps	20Mbps
Fast Ethernet	100Mbps	200Mbps
Gigabit Ethernet	n/a	2000Mbps
Topology:	Star, Ring	

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 Mini-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 207(D) x 44mm(H), 19 inch

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. 1,488,000 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.