D-Link®

DGS-3312SR

Release 3.5

12-Port Gigabit Layer 3 Stackable Switch

Command Line Interface Reference Manual

Third Edition
(Oct 2005)

Version 0.35

Printed In China

RECYCLABLE

Information in this document is subject to change without notice.

© 2005 D-Link Computer Corporation. All rights reserved.

Reproduction in any manner whatsoever without the written permission of D-Link Computer Corporation is strictly forbidden.

Trademarks used in this text: D-Link and the D-LINK logo are trademarks of D-Link Computer Corporation; Microsoft and Windows are registered trademarks of Microsoft Corporation.

Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. D-Link Computer Corporation disclaims any proprietary interest in trademarks and trade names other than its own.

October 2005 P/N DGS3312SR.A3

Table of Contents

Introduction 1
Using the Console CLI 4
Command Syntax 10
Basic Switch Commands 12
Switch Port Commands 24
Port Security Commands 27
Network Management (SNMP) Commands 31
Switch Utility Commands 52
Network Monitoring Commands 56
Multiple Spanning Tree Protocol (MSTP) Commands 69
Forwarding Database Commands 82
Broadcast Storm Control Commands 89
QoS Commands 91
Port Mirroring Commands 99
VLAN Commands 104
Link Aggregation Commands 111
IP Commands (Including IP Multinetting) 117
IGMP Commands 122
IGMP Snooping Commands 125
MAC Notification Commands 133
Access Authentication Control Commands 137
SSH Commands 161
SSL Commands 169
802.1X Commands 174
Access Control List (ACL) Commands 186
Traffic Segmentation Commands 195
Stacking Commands 197
D-Link Single IP Management Commands 200
Time and SNTP Commands 210
ARP Commands 216
VRRP Commands 220
Routing Table Commands 227
Route Redistribution Commands 231
BOOTP Relay Commands 237
DNS Relay Commands 241

RIP Commands 245
DVMRP Commands 248
PIM Commands 253
IP Multicasting Commands 257
MD5 Configuration Commands 259
OSPF Configuration Commands 262
Command History List 282
Technical Specifications 284
VCCI Warning 286

1

INTRODUCTION

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

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

Accessing the Switch via the Serial Port

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

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

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

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

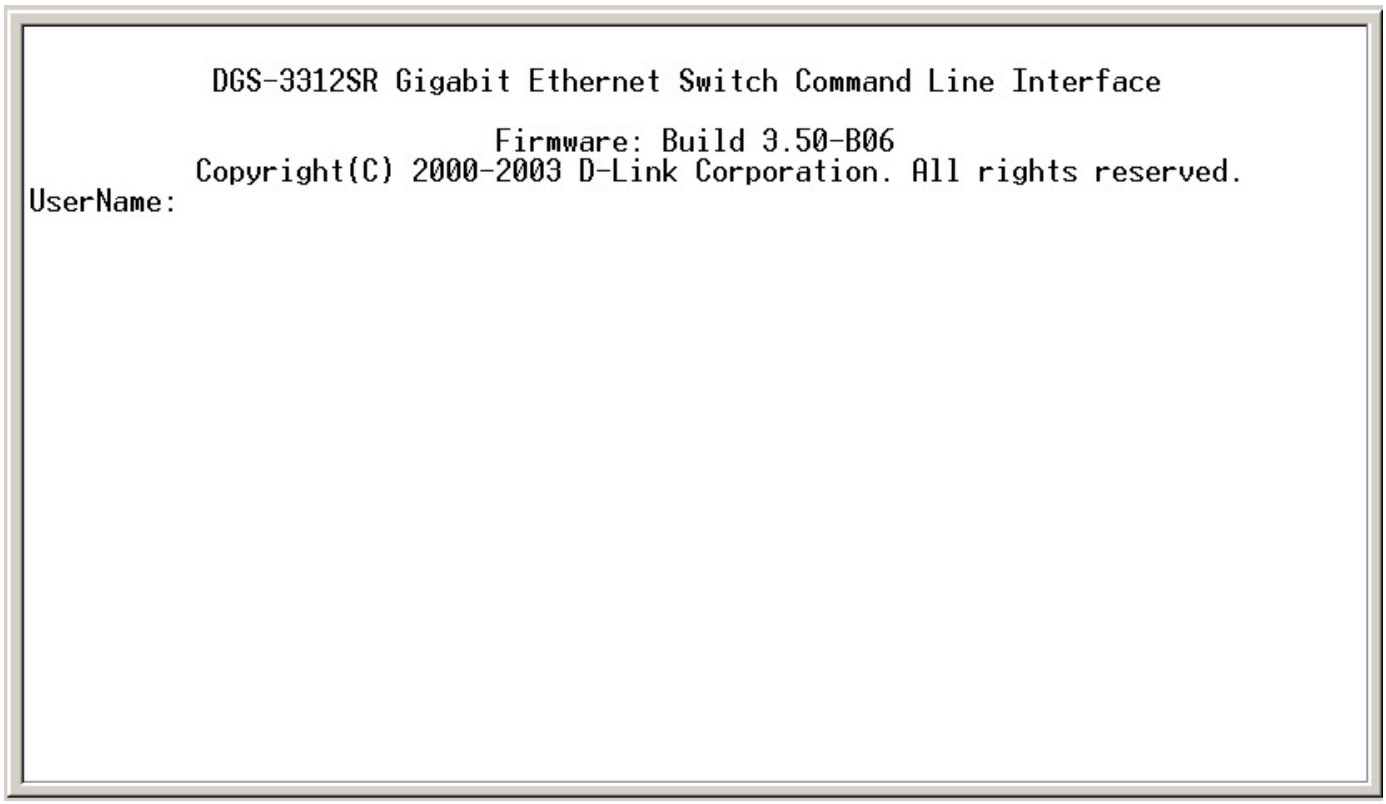

Figure 1-1. Initial CLI screen

There is no initial username or password. Just press the **Enter** key twice to display the CLI input cursor – **DGS-3312SR: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, TFTP). The switch's default IP address is 10.90.90.90. You can change the default Switch IP address to meet the specification of your networking address scheme.

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

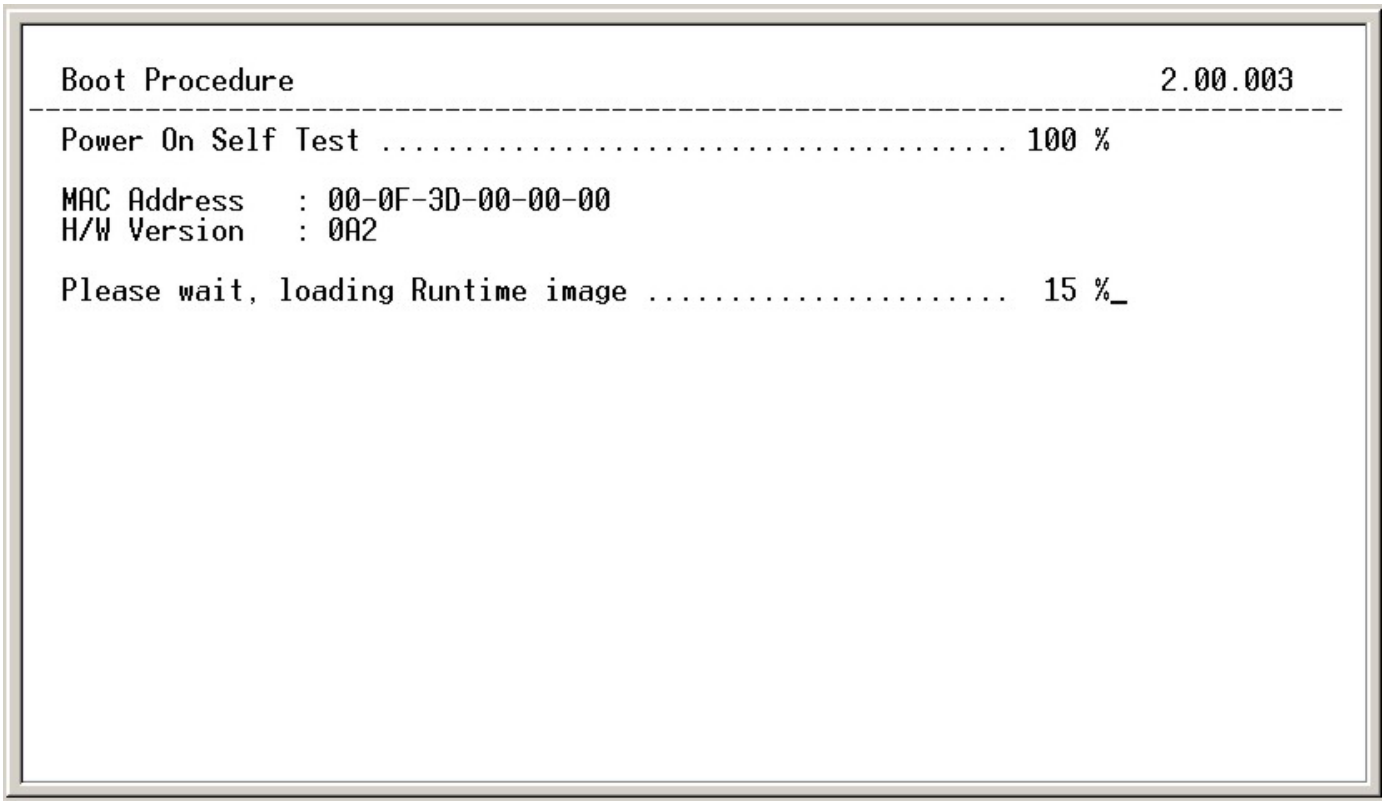

Figure 1-2. Boot Screen

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

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

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

1. Starting at the command line prompt, enter the commands **config ipif System ipaddress xxx.xxx.xxx.xxx/yyy.yyy.yyy.yyy**. Where the **x**'s represent the IP address to be assigned to the IP interface named **System** and the **y**'s represent the corresponding subnet mask.

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

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

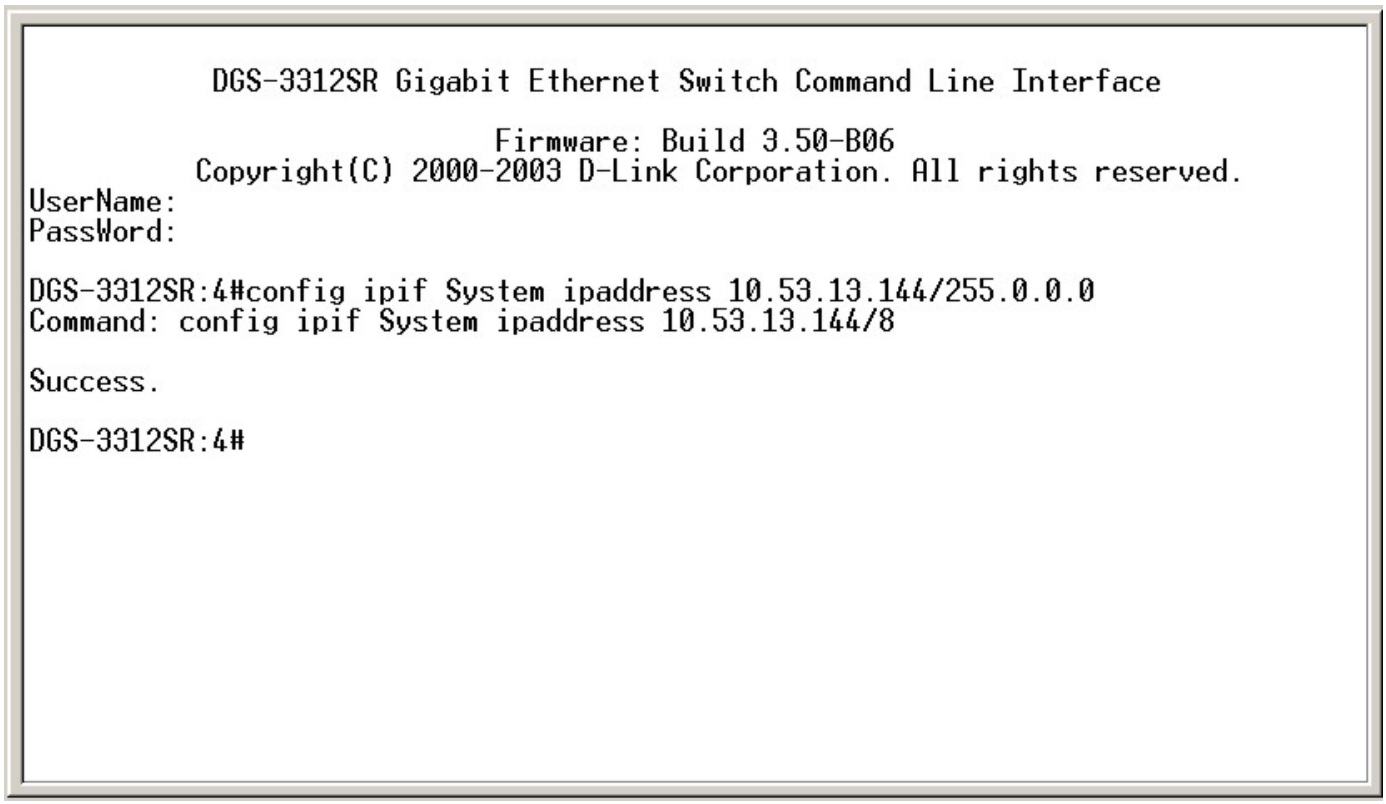

Figure 1-3. Assigning an IP Address

In the above example, the switch was assigned an IP address of 10.53.13.144/8 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-3312SR supports a console management interface that allows the user to connect to the switch's management agent via a serial port and a terminal or a computer running a terminal emulation program. The console can also be used over the network using the TCP/IP Telnet protocol. The console program can be used to configure the switch to use an SNMP-based network management software over the network.

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

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

Connecting to the Switch

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

- **VT-100 compatible**
- **9600 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:

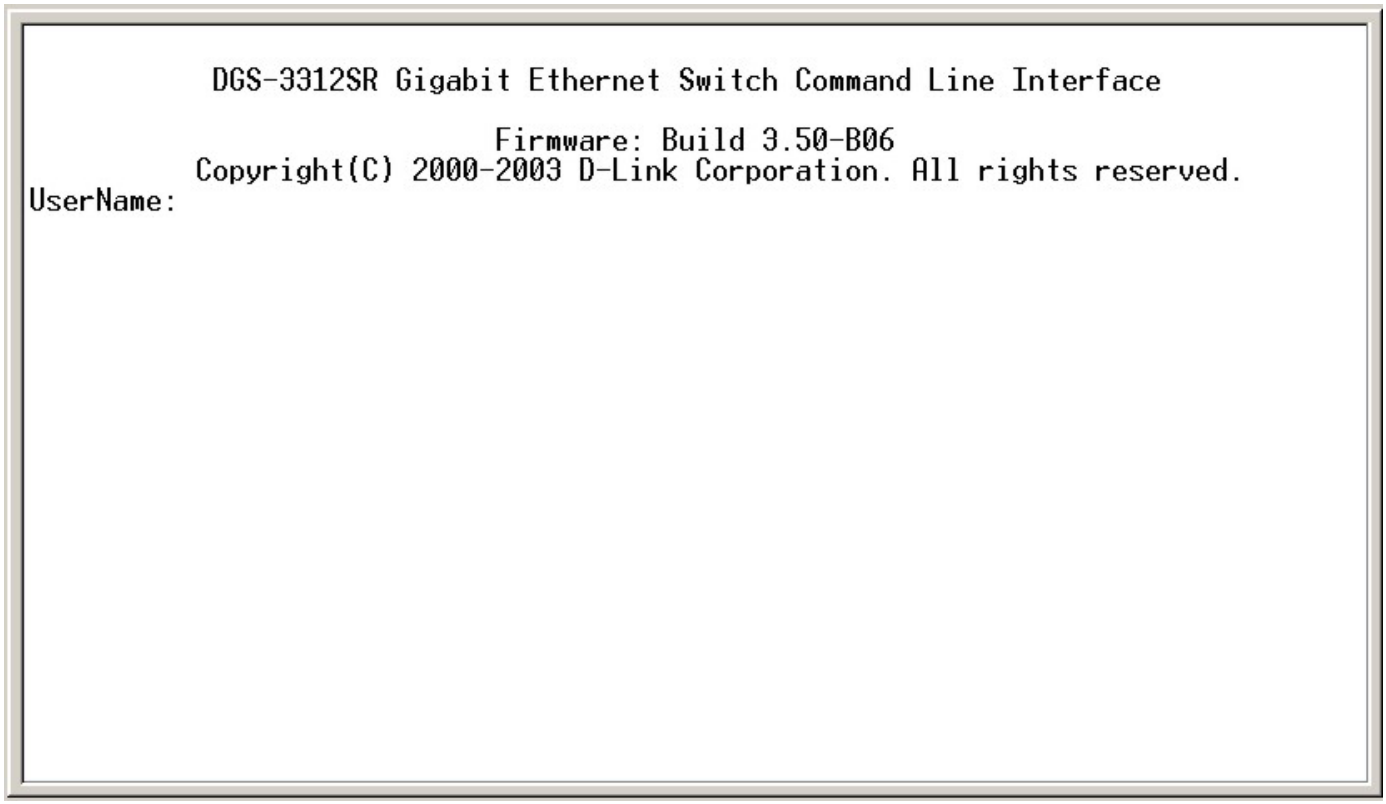

Figure 2-1. Initial Console Screen

Commands are entered at the command prompt, **DGS-3312SR: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.

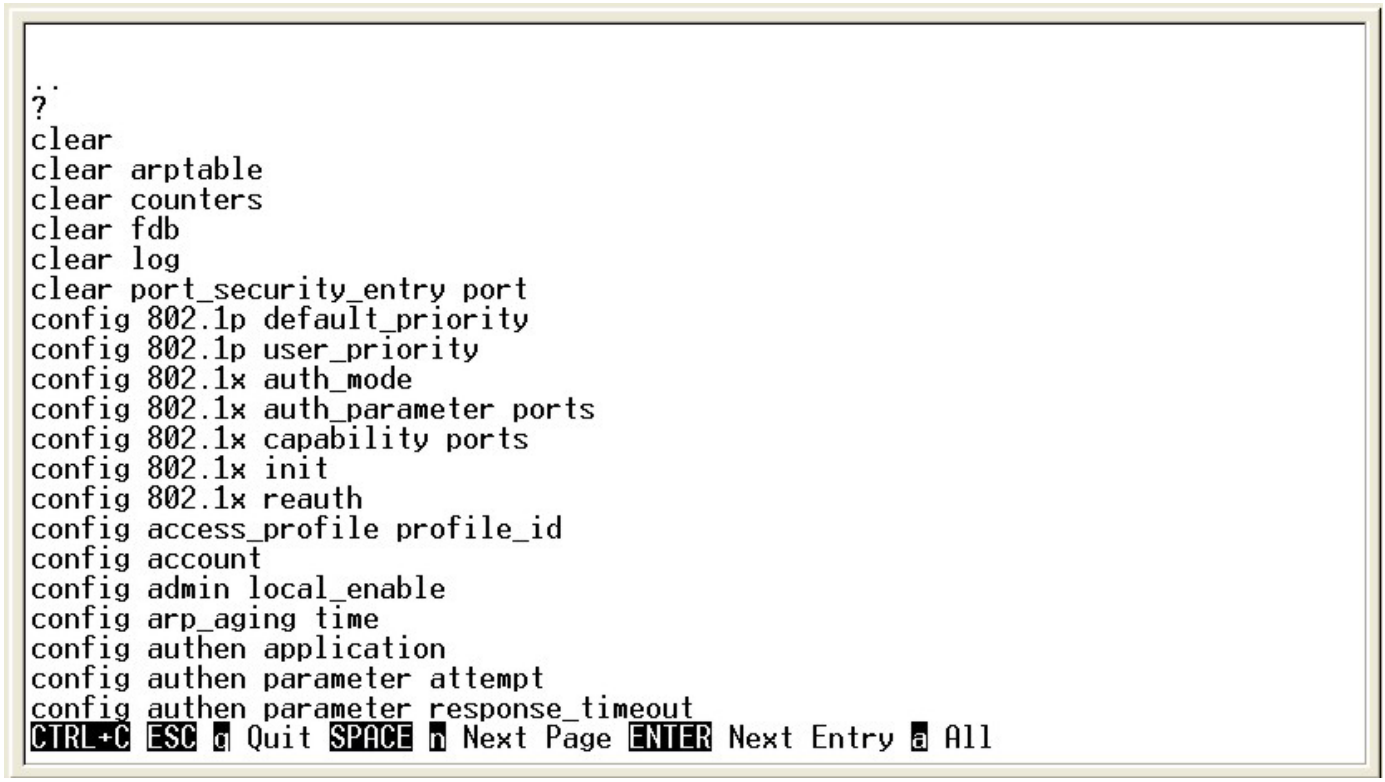

Figure 2-2. The ? Command

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

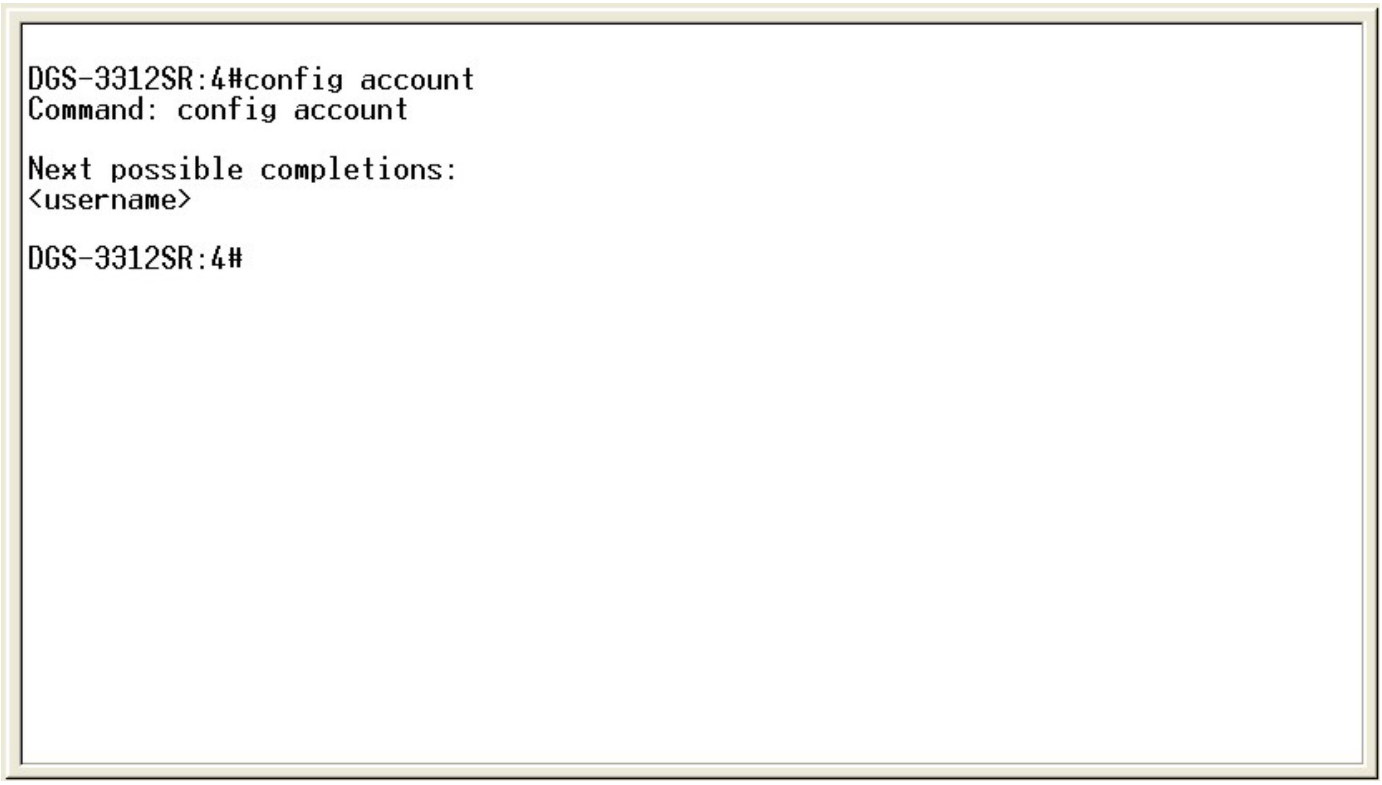

Figure 2-3. Example Command Parameter Help

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.

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

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

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.

```
DGS-3312SR:4#the

Available commands:
..                  ?                   clear               config
create              delete              dir                 disable
download            enable              login               logout
ping                reboot              reconfig            reset
save                show                traceroute          upload

DGS-3312SR:4#
```

Figure 2-5. The Next Available Commands Prompt

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

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

```
DGS-3312SR:4#show
Command: show

Next possible completions:
802.1p              802.1x              access_profile      account
arpentry            authen              authen_enable       authen_login
authen_policy       bandwidth_control   bootp_relay         certificate
command_history     config              dnsr                dvmrp
error               fdb                 gvrp                igmp
igmp_snooping       ipfdb               ipif                ipmc
iproute             lacp_port           link_aggregation    log
mac_notification    md5                 mirror              multicast
multicast_fdb       ospf                packet              pim
port_security       ports               radius              rip
route               router_ports        scheduling_mechanism
serial_port         session             sim                 snmp
sntp                ssh                 ssl                 stacking
stp                 switch              syslog              time
traffic             traffic_segmentation                    trusted_host
utilization         vlan                vrrp

DGS-3312SR:4#
```

Figure 2-6. Next possible completions: Show Command

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

3

COMMAND SYNTAX

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

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

<angle brackets>	
Purpose	Encloses a variable or value that must be specified.
Syntax	**create ipif <ipif_name> vlan <vlan_name 32> 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 32>* space, and the network address in the *<network_address>* space. Do not type the angle brackets.
Example Command	**create ipif Engineering vlan Design ipaddress 10.24.22.5/255.0.0.0**

[square brackets]	
Purpose	Encloses a required value or set of required arguments. One value or argument 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 | detail]**
Description	In the above syntax example, you must specify either **community,** or **detail**. Do not type the backslash.
Example Command	**show snmp community**

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

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

Line Editing Key Usage	
Delete	Deletes the character under the cursor and then shifts the remaining characters in the line to the left.
Backspace	Deletes the character to the left of the cursor and shifts the remaining characters in the line to the left.
Left Arrow	Moves the cursor to the left.
Right Arrow	Moves the cursor to the right.
Up Arrow	Repeat the previously entered command. Each time the up arrow is pressed, the command previous to that displayed appears. This way it is possible to review the command history for the current session. Use the down arrow to progress sequentially forward through the command history list.
Down Arrow	The down arrow will display the next command in the command history entered in the current session. This displays each command sequentially as it was entered. Use the up arrow to review previous commands.
Tab	Shifts the cursor to the next field to the left.

Multiple Page Display Control Keys	
Space	Displays the next page.
CTRL+c	Stops the display of remaining pages when multiple pages are to be displayed.
ESC	Stops the display of remaining pages when multiple pages are to be displayed.
n	Displays the next page.
p	Displays the previous page.
q	Stops the display of remaining pages when multiple pages are to be displayed.
r	Refreshes the pages currently displayed.
a	Displays the remaining pages without pausing between pages.
Enter	Displays the next line or table entry.

4

BASIC SWITCH COMMANDS

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

Command	Parameters
create account	[admin | user] <username 15>
config account	<username 15>
show account	
delete account	<username 15>
show session	
show switch	
show config	[current_config | config_in_NVRAM]
show serial_port	
config serial_port	{baud_rate [9600 | 19200 | 38400 | 115200] auto_logout [never | 2_minutes | 5_minutes | 10_minutes | 15_minutes]}
enable clipaging	
disable clipaging	
enable telnet	<tcp_port_number 1-65535>
disable telnet	
enable web	<tcp_port_number 1-65535>
disable web	
save	
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 8 user accounts can be created.
Parameters	*admin <username>* *user <username>*
Restrictions	Only Administrator-level users can issue this command.

create account	
	Usernames can be between 1 and 15 characters.
	Passwords can be between 0 and 15 characters.

Example usage:

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

```
DGS-3312SR: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-3312SR: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.
	Usernames can be between 1 and 15 characters.
	Passwords can be between 0 and 15 characters.

Example usage:

To configure the user password of “dlink” account:

```
DGS-3312SR: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-3312SR:4#
```

show account	
Purpose	Used to display user accounts
Syntax	**show account**
Description	Displays all user accounts created on the switch. Up to 8 user accounts can exist on the switch at one time.
Parameters	None.
Restrictions	None.

Example usage:

To display the accounts created:

```
DGS-3312SR:4#show account
Command: show account

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

DGS-3312SR: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-3312SR:4#delete account System
Command: delete account System

 Success.

DGS-3312SR:4#
```

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-3312SR:4#show switch
Command: show switch

Device Type          : DGS-3312SR Gigabit-Ethernet Switch
Module 1 Type        : Empty
Module 2 Type        : Empty
Unit ID              : 15
MAC Address          : DA-10-21-00-00-01
IP Address           : 10.41.44.22 (Manual)
VLAN Name            : default
Subnet Mask          : 255.0.0.0
Default Gateway      : 0.0.0.0
Boot PROM Version    : Build 2.00.003
Firmware Version     : Build 3.50-B06
Hardware Version     : 2A1
Device S/N           :
System Name          : DGS-3312SR_#3
System Location      : 7th_flr_east_cabinet
System Contact       : Julius_Erving_212-555-6666
Spanning Tree        : Disabled
GVRP                 : Disabled
IGMP Snooping        : Disabled
TELNET               : Enabled (TCP 23)
WEB                  : Enabled (TCP 80)
RMON                 : Disabled
RIP                  : Disabled
DVMRP                : Disabled
PIM-DM               : Disabled
OSPF                 : Disabled

DGS-3312SR:4#
```

show config	
Purpose	Used to display the configuration of the switch.
Syntax	**show config [current_config | config_in_NVRAM]**
Description	This command displays either the current configuration of the switch, or the configuration stored in the switch's NVRAM.
Parameters	current_config – displays the switch's current configuration. If you have entered a configuration command, but have not saved the configuration in the switch's Non-Volatile RAM (NVRAM), this configuration will differ from the one saved in the switch's NVRAM. config_in_NVRAM – displays the switch's configuration saved in the switch's NVRAM. Any configuration commands that have been entered, but not saved in the switch's NVRAM will not be shown.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To display the switch's configuration information:

```
DGS-3312SR:4#show config current_config
Command: show current_config

# BASIC

config serial_port baud_rate 9600 auto_logout 10_minutes
enable telnet 23
enable web 80

# STORM

config traffic control 15:1-15:2 broadcast disable multicast disable dlf disable
threshold 128

# GM

config sim candidate
disable sim
config sim dp_interval 30
config sim hold_time 100

# SYSLOG

disable syslog

#QOS

config scheduling_mechanism round_robin
config scheduling_mechanism round_robin
config scheduling_mechanism round_robin
config scheduling_mechanism round_robin
config scheduling_mechanism round_robin
config scheduling_mechanism round_robin
config scheduling_mechanism round_robin
config scheduling_mechanism round_robin
config 802.1p user_priority 0 2
```

```
config 802.1p user_priority 1 0
config 802.1p user_priority 2 1
config 802.1p user_priority 3 3
config 802.1p user_priority 4 4
config 802.1p user_priority 5 5
config 802.1p user_priority 6 6
config 802.1p user_priority 7 7
config 802.1p default_priority 15:1-15:12 0
config bandwidth_control 15:1 rx_r
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

show serial_port

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

Example usage:

To display the serial port setting:

```
DGS-3312SR:4#show serial_port
Command: show serial_port

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

DGS-3312SR:4#
```

config serial_port

Purpose	Used to configure the serial port.
Syntax	**config serial_port {baud_rate [9600 | 19200 | 38400 | 115200] | auto_logout [never | 2_minutes | 5_minutes | 10_minutes | 15_minutes]}**
Description	This command is used to configure the serial port's baud rate and auto logout settings.
Parameters	*baud_rate [9600 | 19200 | 38400 | 115200]* – The serial bit rate used to communicate with the management host. *auto logout* – This parameter will set the time that the switch will wait before logging out automatically, if left idle. The choices that accompany this parameter are:

config serial_port	
	▪ *never* – No time limit on the length of time the console can be open with no user input. ▪ *2_minutes* – The console will log out the current user if there is no user input for 2 minutes. ▪ *5_minutes* – The console will log out the current user if there is no user input for 5 minutes. ▪ *10_minutes* – The console will log out the current user if there is no user input for 10 minutes. ▪ *15_minutes* – The console will log out the current user if there is no user input for 15 minutes.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure baud rate:

```
DGS-3312SR:4#config serial_port baud_rate 9600
Command: config serial_port baud_rate 9600

Success.

DGS-3312SR: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 which causes the console screen to rapidly scroll through several pages. This command will cause the console to pause at the end of each page. The default setting is enabled.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

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

```
DGS-3312SR:4#enable clipaging
Command: enable clipaging

Success.

DGS-3312SR:4#
```

disable clipaging	
Purpose	Used to disable the pausing of the console screen scrolling at the end of each page when the show command displays more than one screen of information.
Syntax	**disable clipaging**
Description	This command is used to disable the pausing of the console screen at the end of each page when the show command would display more than one screen of information.
Parameters	None.
Restrictions	Only administrator-level 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-3312SR:4#disable clipaging
Command: disable clipaging

Success.

DGS-3312SR:4#
```

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

Example usage:

To enable Telnet and configure port number:

```
DGS-3312SR:4#enable telnet 23
Command: enable telnet 23

Success.

DGS-3312SR:4#
```

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

Example usage:

To disable the Telnet protocol on the switch:

```
DGS-3312SR:4#disable telnet
Command: disable telnet

Success.

DGS-3312SR:4#
```

enable web	
Purpose	Used to enable the HTTP-based management software on the switch.
Syntax	**enable web <tcp_port_number 1-65535>**
Description	This command is used to enable the Web-based management software on the switch. The user can specify the TCP port number the switch will use to listen for Telnet requests.
Parameters	*<tcp_port_number 1-65535>* – The TCP port number. TCP ports are numbered between 1 and 65535. The “well-known” port for the Web-based management software is 80.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To enable HTTP and configure port number:

```
DGS-3312SR:4#enable web 80
Command: enable web 80

Success.

DGS-3312SR: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-3312SR:4#disable web
Command: disable web

Success.

DGS-3312SR: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	Entering just the **save** command will save the switch configuration to NV-Ram
Restrictions	Only administrator-level users can issue this command.

Example usage:

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

```
DGS-3312SR:4#save
Command: save

Saving all configurations to NV-RAM…  Done

DGS-3312SR:4#
```

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

Example usage:

To restart the switch:

```
DGS-3312SR:4#reboot
Command: reboot
Are you sure want to proceed with the system reboot? (y/n)
Please wait, the switch is rebooting...
```

reset	
Purpose	Used to reset the switch to the factory default settings.
Syntax	**reset {[config | system]}**
Description	This command is used to restore the switch's configuration to the default settings assigned from the factory.
Parameters	*config* – If the keyword 'config' is specified, all of the factory default settings are restored on the switch including the IP address, user accounts, and the switch history log. The switch will not save or reboot. *system* – If the keyword 'system' is specified all of the factory default settings are restored on the switch. The switch will save and reboot after the settings are changed to default. Rebooting will clear all entries in the Forwarding Data Base. If no parameter is specified, the switch's current IP address, user accounts, and the switch history log are not changed. All other parameters are restored to the factory default settings. The switch will not save or reboot.
Restrictions	Only administrator-level users can issue this command.

Example usage:

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

```
DGS-3312SR:4#reset config
Command: reset config

Success.

DGS-3312SR: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-3312SR:4#login
Command: login

UserName:
```

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

Example usage:

To terminate the current user's console session:

```
DGS-3312SR:4#logout
```

5

SWITCH PORT COMMANDS

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

Command	Parameters
config ports	[<portlist | all> {speed [auto | 10_half | 10_full | 100_half | 100_full | 1000_full {[master | slave]}} | flow_control [enable | disable] | learning [enable | disable] | state [enable | disable] description <desc 32> | clear]}
show ports	{<portlist>} {description}

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

NOTE: As a stand-alone switch or as a master switch in a switch stack, the switch number will be referred to as 15 for all configurations, graphs and tables.

config ports

Purpose	Used to configure the Switch's Ethernet port settings.
Syntax	**[<portlist | all> {speed [auto | 10_half | 10_full | 100_half | 100_full | 1000_full{[master | slave]}} | flow_control [enable | disable] | learning [enable | disable] state [enable | disable] description <desc 32> | clear]}**
Description	This command allows for the configuration of the switch's Ethernet ports. Only the ports listed in the *<portlist>* will be affected.
Parameters	*<portlist>* – Specifies a range of ports to be configured. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3-2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. *all* – Configure all ports on the switch. *auto* – Enables auto-negotiation for the specified range of ports. *[10 | 100 | 1000]* – Configures the speed in Mbps for the specified range of ports. *[half | full]* – Configures the specified range of ports as either full- or half-duplex. *{[master | slave}]* – Configures the specified range of ports as either master or slave ports.

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

Example usage:

To configure the speed of port 3 to be 10 Mbps, full duplex, learning and state enable:

```
DGS-3312SR:4#config ports 1:1-1:3 speed 10_full learning enable state enable
Command: config ports 1:1-1:3 speed 10_full learning enable state enable

Success.

DGS-3312SR:4#
```

show ports	
Purpose	Used to display the current configuration of a range of ports.
Syntax	**show ports {<portlist>} {description}**
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 lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3-2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. *description* – Enter this parameter to view the description of the port previously set in the **config ports** command.
Restrictions	None.

Example usage:

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

```
DGS-3312SR:4#show ports
Command show ports:

Port    Port       Settings                 Connection               Address
        State      Speed/Duplex/FlowCtrl    Speed/Duplex/FlowCtrl    Learning
------  --------   ---------------------    ---------------------    --------
15:1    Enabled    Auto/Enabled             Link Down                Enabled
15:2    Enabled    Auto/Enabled             Link Down                Enabled
15:3    Enabled    Auto/Enabled             Link Down                Enabled
15:4    Enabled    Auto/Enabled             Link Down                Enabled
15:5    Enabled    Auto/Enabled             Link Down                Enabled
15:6    Enabled    Auto/Enabled             Link Down                Enabled
15:7    Enabled    Auto/Enabled             Link Down                Enabled
15:8    Enabled    Auto/Enabled             Link Down                Enabled
15:9    Enabled    Auto/Enabled             Link Down                Enabled
15:10   Enabled    Auto/Enabled             100M/Full/802.3x         Enabled
15:11   Enabled    Auto/Enabled             Link Down                Enabled
15:12   Enabled    Auto/Enabled             Link Down                Enabled

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

Example usage:

To view port 1:1 with description

```
DGS-3312SR:4# show ports 15:1 description
Command: show ports 15:1 description

Port    Port       Settings                 Connection               Address
        State      Speed/Duplex/FlowCtrl    Speed/Duplex/FlowCtrl    Learning
------  --------   ---------------------    ---------------------    --------
1:1     Enabled    Auto/Enabled             Link Down                Enabled
        Desc: Darren's

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

6

PORT SECURITY COMMANDS

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

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

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

NOTE: As a stand-alone switch or as a master switch in a switch stack, the switch number will be referred to as 15 for all configurations, graphs and tables.

config port_security ports

Purpose	Used to configure port security settings.
Syntax	**config [<portlist> | all] {admin_state [enable | disable] | max_learning_addr <max_lock_no 0-10> | lock_address_mode [Permanent | DeleteOnTimeout | DeleteOnReset]}**
Description	This command allows for the configuration of the port security feature. Only the ports listed in the <portlist> are affected.
Parameters	*<portlist>* – Specifies a range of ports to be configured. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3-2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. *all* – Configure port security for all ports on the switch. *admin_state [enable* | *disable]* – Enables or disables port security for the listed ports. *max_learning_addr <max_lock_no 0-10>* - Use this to limit the number of MAC addresses dynamically listed in the FDB for the ports.

config port_security ports	
	lock_address_mode [Permanent | DeleteOnTimeout | DeleteOnReset] – Delete FDB dynamic entries for the ports on timeout of the FDB (see Forwarding Database Commands). Specify DeleteOnReset to delete all FDB entries, including static entries upon system reset or rebooting. Entering the *Permanent* parameter will permanently set the MAC address in the switch's memory until deleted by the user.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure the port security:

DGS-3312SR:4#config port_security ports 1:1-1:5 admin_state enable max_learning_addr 5 lock_address_mode DeleteOnReset

Command: config port_security ports 1:1-1:5 admin_state enable max_learning_addr 5 lock_address_mode DeleteOnReset

Success

DGS-3312SR:4#

show port_security	
Purpose	Used to display the current port security configuration.
Syntax	**show port_security {ports <portlist>}**
Description	This command is used to display port security information of the switch ports. The information displayed includes port security admin state, maximum number of learning address and lock mode.
Parameters	*<portlist>* – Specifies a range of ports to be viewed. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3-2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order.
Restrictions	None.

Example usage:

To display the port security configuration:

```
DGS-3312SR:4#show port_security ports
Command: show port_security ports

Port#   Admin State   Max. Learning Addr.   Lock Address Mode
----    -----------   -------------------   -----------------
15:1    Disabled      1                     DeleteOnReset
15:2    Disabled      1                     DeleteOnReset
15:3    Disabled      1                     DeleteOnReset
15:4    Disabled      1                     DeleteOnReset
15:5    Disabled      1                     DeleteOnReset
15:6    Disabled      1                     DeleteOnReset
15:7    Enabled       10                    DeleteOnReset
15:8    Disabled      1                     DeleteOnReset
15:9    Disabled      1                     DeleteOnReset
15:10   Disabled      1                     DeleteOnReset
15:11   Disabled      1                     DeleteOnReset
15:12   Disabled      1                     DeleteOnReset

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

delete port_security_entry_vlan_name

Purpose	Used to delete an entry from the switch's port security settings.
Syntax	**delete port_security_entry_vlan_name <vlan_name 32> mac_address <macaddr> port <port>**
Description	This command is used to remove an entry from the port security entries learned by the switch and entered into the forwarding database.
Parameters	<vlan_name 32> - Enter the corresponding vlan of the entry the user wishes to delete. mac_address <macaddr> - Enter the corresponding MAC address of the entry the user wishes to delete. port <port> - Enter the corresponding port of the entry to delete. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3-2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To delete an entry from the port security list:

```
DGS-3312SR:4#delete port_security_entry_vlan_name default
mac_address 00-0C-6E-73-2B-C9 port 1:1
Command: delete port_security_entry_vlan_name default
mac_address 00-0C-6E-73-2B-C9 port 1:1

Success

DGS-3312SR:4#
```

clear port_security_entry port	
Purpose	Used to clear MAC address entries learned from a specified port for the port security function.
Syntax	**clear port_security_entry port <portlist>**
Description	This command is used to clear MAC address entries which were learned by the switch by a specified port. This command only relates to the port security function.
Parameters	*<portlist>* – Specifies a port or port range the user wishes to clear. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3-2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To clear a port security entry by port:

```
DGS-3312SR:4# clear port_security_entry port 6
Command: clear port_security_entry port 6

Success.

DGS-3312SR:4#
```

7

NETWORK MANAGEMENT (SNMP) COMMANDS

The DGS-3312SR supports the Simple Network Management Protocol (SNMP) versions 1, 2c, and 3. You can specify which version of the SNMP you want to use to monitor and control the switch. The three versions of SNMP vary in the level of security provided between the management station and the network device. The following table lists the security features of the three SNMP versions:

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

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

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

Command	Parameters
create snmp user	create snmp user <username 32> <groupname 32> {encrypted [by_password auth [md5 <auth_password 8-16> | sha <auth_password 8-20 >] priv [none | des <priv_password 8-16>] | by_key auth [md5 <auth_key 32-32> | sha <auth_key 40-40>] priv [none | des <priv_key 32-32>]]}
delete snmp user	<username 32>
show snmp user	
create snmp view	<view_name 32> <oid> view_type [included | excluded]
delete snmp view	<view_name 32> [all | oid]
show snmp view	<view_name 32>
create snmp community	<community_string 32> view <view_name 32> [read_only | read_write]
delete snmp community	<community_string 32>
show snmp community	<community_string 32>
config snmp engineID	<snmp_engineID>
show snmp engineID	

Command	Parameters
create snmp group	<groupname 32> {v1 | v2c |v3 [noauth_nopriv | auth_nopriv | auth_priv]} {read_view <view_name 32> | write_view <view_name 32> | notify_view <view_name 32>}
delete snmp group	<groupname 32>
show snmp groups	
create snmp host	<ipaddr> {v1 | v2c | v3 [noauth_nopriv | auth_nopriv | auth_priv]} <auth_string 32>
delete snmp host	<ipaddr>
show snmp host	<ipaddr>
create trusted_host	<ipaddr>
delete trusted_host	<ipaddr>
show trusted_host	<ipaddr>
enable snmp traps	
enable snmp authenticate_traps	
disable snmp traps	
disable snmp authenticate_traps	
config snmp system contact	<sw_contact>
config snmp system location	<sw_location>
config snmp system name	<sw_name>
enable rmon	
disable rmon	

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

create snmp user

Purpose	Used to create a new SNMP user and adds the user to an SNMP group that is also created by this command.
Syntax	**create snmp user <username 32> <groupname 32> {encrypted [by_password auth [md5 <auth_password 8-16> | sha <auth_password 8-20>] priv [none | des <priv_password 8-16>] | by_key auth [md5 <auth_key 32-32>| sha <auth_key 40-40>] priv [none | des <priv_key 32-32>]]}**
Description	The **create snmp user** command creates a new SNMP user and adds the user to an SNMP group that is also created by this command. SNMP ensures: Message integrity – Ensures that packets have not been tampered with during transit. Authentication – Determines if an SNMP message is from a valid

create snmp user

source.

Encryption – Scrambles the contents of messages to prevent it being viewed by an unauthorized source.

Parameters

<username 32> – An alphanumeric name of up to 32 characters that will identify the new SNMP user.

<groupname 32> – An alphanumeric name of up to 32 characters that will identify the SNMP group with which the new SNMP user will be associated.

encrypted – Allows the user to choose a type of authorization for authentication using SNMP. The user may choose:

by_password auth – Requires the SNMP user to enter a password for authentication and privacy. The password is defined by specifying the *auth_password* below. This method is recommended.

- *md5* – Specifies that the HMAC-MD5-96 authentication level will be used. md5 may be utilized by entering the following:
  - *<auth password 8-16>* - An alphanumeric sting of between 8 and 16 characters,used to authorize the agent to receive packets for the host.
- *sha* – Specifies that the HMAC-SHA-96 authentication level will be used.
  - *<auth password 8-20>* - An alphanumeric sting of between 8 and 20 characters, used to authorize the agent to receive packets for the host.

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

- *des* – Adding this parameter will allow for a 56-bit encryption to be added using the DES-56 standard using:
  - *<priv_password 8-16>* - An alphanumeric string of between 8 and 16 characters that will be used to encrypt the contents of messages the host sends to the agent.

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

- *md5* – Specifies that the HMAC-MD5-96 authentication level will be used. md5 may be utilized by entering the following:
  - *<auth_key 32-32>* - Enter an alphanumeric sting of exactly 32 characters, in hex form, to define the key that will be used to authorize the agent to receive packets for the host.
- *sha* – Specifies that the HMAC-SHA-96 authentication level will be used.
  - *<auth_key 40-40>* - Enter an alphanumeric sting

create snmp user	
	of exactly 40 characters, in hex form, to define the key that will be used to authorize the agent to receive packets for the host. *priv* – Adding the *priv* (privacy) parameter will allow for encryption in addition to the authentication algorithm for higher security. The user may choose: • *none* – Adding this parameter will add no encryption. • *des* – Adding this parameter will allow for a 56-bit encryption to be added using the DES-56 standard using: <*priv_key 32-32*> - Enter an alphanumeric key string of exactly 32 characters, in hex form, that will be used to encrypt the contents of messages the host sends to the agent.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To create an SNMP user on the switch:

```
DGS-3312SR:4#create snmp user dlink default encrypted
by_password auth md5 auth_password priv none
Command: create snmp user dlink default encrypted by_password
auth md5 auth_password priv none

Success.

DGS-3312SR:4#
```

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

Example usage:

To delete a previously entered SNMP user on the switch:

```
DGS-3312SR:4#delete snmp user dlink
Command: delete snmp user dlink

Success.

DGS-3312SR: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-3312SR:4#show snmp user
Command: show snmp user

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

Total Entries: 1


DGS-3312SR:4#
```

create snmp view	
Purpose	Used to assign views to community strings to limit which MIB objects and SNMP manager can access.
Syntax	**create snmp view <view_name 32> <oid> view_type [included | excluded]**
Description	The **create snmp view** command assigns views to community strings to limit which MIB objects an SNMP manager can access.
Parameters	<*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 manager can access.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To create an SNMP view:

```
DGS-3312SR:4#create snmp view dlinkview 1.3.6 view_type included
Command: create snmp view dlinkview 1.3.6 view_type included

Success.

DGS-3312SR:4#
```

delete snmp view

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

Example usage:

To delete a previously configured SNMP view from the switch:

```
DGS-3312SR:4#delete snmp view dlinkview all
Command: delete snmp view dlinkview all

Success.

DGS-3312SR:4#
```

show snmp view

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

Example usage:

To display SNMP view configuration:

```
DGS-3312SR:4#show snmp view
Command: show snmp view

 Vacm View Table Settings
 View Name                       Subtree                         View Type
 ------------------              -------------------------       ----------
 ReadView                        1                               Included
 WriteView                       1                               Included
 NotifyView                      1.3.6                           Included
 restricted                      1.3.6.1.2.1.1                   Included
 restricted                      1.3.6.1.2.1.11                  Included
 restricted                      1.3.6.1.6.3.10.2.1              Included
 restricted                      1.3.6.1.6.3.11.2.1              Included
 restricted                      1.3.6.1.6.3.15.1.1              Included
 CommunityView                   1                               Included
 CommunityView                   1.3.6.1.6.3                     Excluded
 CommunityView                   1.3.6.1.6.3.1                   Included

Total Entries: 11

DGS-3312SR:4#
```

create snmp community

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

create snmp community	
	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-3312SR:4#create snmp community dlink view ReadView read_write
Command: create snmp community dlink view ReadView read_write

Success.

DGS-3312SR: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-3312SR:4#delete snmp community dlink
Command: delete snmp community dlink

Success.

DGS-3312SR:4#
```

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

Example usage:

To display the currently entered SNMP community strings:

```
DGS-3312SR:4#show snmp community
Command: show snmp community

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

Total Entries: 3

DGS-3312SR: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-3312SR:4#config snmp engineID 0035636666
Command: config snmp engineID 0035636666

Success.

DGS-3312SR: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-3312SR:4#show snmp engineID
Command: show snmp engineID

SNMP Engine ID : 0035636666

DGS-3312SR: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 32> [v1 | v2c | v3 [noauth_nopriv | auth_nopriv | auth_priv]] {read_view <view_name 32> | write_view <view_name 32> | notify_view <view_name 32>}**
Description	The **create snmp group** command creates a new SNMP group, or a table that maps SNMP users to SNMP views.
Parameters	*<groupname 32>* – An alphanumeric name of up to 32 characters that will identify the SNMP group with which the new SNMP user will be associated. *v1* – Specifies that SNMP version 1 will be used. The Simple Network Management Protocol (SNMP), version 1, is a network management protocol that provides a means to monitor and control network devices. *v2c* – Specifies that SNMP version 2c will be used. The SNMP v2c supports both centralized and distributed network management strategies. It includes improvements in the Structure of Management Information (SMI) and adds some security features. *v3* – Specifies that the SNMP version 3 will be used. SNMP v3 provides secure access to devices through a combination of authentication and encrypting packets over the network. SNMP v3 adds:

create snmp group	
	▪ Message integrity – Ensures that packets have not been tampered with during transit. ▪ Authentication – Determines if an SNMP message is from a valid source. ▪ Encryption – Scrambles the contents of messages to prevent it being viewed by an unauthorized source. *noauth_nopriv* – Specifies that no authorization and no encryption of packets is sent between the switch and a remote SNMP manager. *auth_nopriv* – Specifies that authorization will be required, but there will be no encryption of packets sent between the switch and a remote SNMP manager. *auth_priv* – Specifies that authorization will be required, and that packets sent between the switch and a remote SNMP manger will be encrypted. *read_view* – Specifies that the SNMP group being created can request SNMP messages. • <*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. *write_view* – Specifies write privileges for the SNMP group being created. • <*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. *notify_view* – Specifies that the SNMP group being created can receive SNMP trap messages generated by the switch's SNMP agent. • <*view_name 32*> – An alphanumeric string of up to 32 characters that is used to identify the group of MIB objects that a remote SNMP manager is allowed to access on the switch.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To create an SNMP group named "sg1:"

```
DGS-3312SR:4#create snmp group sg1 v3 noauth_nopriv read_view v1
write_view v1 notify_view v1
Command: create snmp group sg1 v3 noauth_nopriv read_view v1
write_view v1 notify_view v1

Success.

DGS-3312SR: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 to be deleted.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To delete the SNMP group named "sg1".

```
DGS-3312SR:4#delete snmp group sg1
Command: delete snmp group sg1

Success.

DGS-3312SR: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 are also displayed.
Syntax	**show snmp groups**
Description	The **show snmp groups** command displays the group-names of SNMP groups currently configured on the switch. The security model, level, and status of each group are also displayed.
Parameters	None.
Restrictions	None.

Example usage:

To display the currently configured SNMP groups on the switch:

```
DGS-3312SR:4#show snmp groups
Command: show snmp groups

Vacm Access Table Settings

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

Group    Name        : Group4
ReadView Name        : ReadView
WriteView Name       : WriteView
```

```
Notify View Name    : NotifyView
Security Model      : SNMPv3
Security Level      : authNoPriv

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

Total Entries: 3

DGS-3312SR:4#
```

create snmp host

Purpose	Used to create a recipient of SNMP traps generated by the switch's SNMP agent.
Syntax	**create snmp host <ipaddr> [v1 | v2c | v3 [noauth_nopriv | auth_nopriv | auth_priv] <auth_string 32>]**
Description	The **create snmp host** command creates a recipient of SNMP traps generated by the switch's SNMP agent.
Parameters	*<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 packets have not been tampered with during transit. ▪ Authentication – Determines if an SNMP message is from a valid source. ▪ Encryption – Scrambles the contents of messages to prevent it being viewed by an unauthorized source. *noauth_nopriv* – Specifies no authorization and no encryption of packets is 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

create snmp host	
	and a remote SNMP manager. *auth_priv* – Specifies that authorization will be required, and that packets sent between the switch and a remote SNMP manger will be encrypted. • *<auth_sting 32>* – An alphanumeric string used to authorize a remote SNMP manager to access the switch's SNMP agent.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To create an SNMP host to receive SNMP messages:

```
DGS-3312SR:4#create snmp host 10.48.74.100 v3 auth_priv public
Command: create snmp host 10.48.74.100 v3 auth_priv public

Success.

DGS-3312SR: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-3312SR:4#delete snmp host 10.48.74.100
Command: delete snmp host 10.48.74.100

Success.

DGS-3312SR: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-3312SR:4#show snmp host
Command: show snmp host

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

Total Entries: 2


DGS-3312SR:4#
```

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

Example usage:

To create the trusted host:

```
DGS-3312SR:4#create trusted_host 10.48.74.121
Command: create trusted_host 10.48.74.121

Success.

DGS-3312SR: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	Only administrator-level users can issue this command.

Example Usage:

To display the list of trust hosts:

```
DGS-3312SR:4#show trusted_host
Command: show trusted_host

Management Stations

IP Address
---------------------
10.53.13.94

Total Entries: 1

DGS-3312SR:4#
```

delete trusted_host

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

Example Usage:

To delete a trusted host with an IP address 10.48.74.121:

```
DGS-3312SR:4#delete trusted_host 10.48.74.121
Command: delete trusted_host 10.48.74.121

Success.

DGS-3312SR:4#
```

enable snmp traps

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

Example usage:

To enable SNMP trap support on the switch:

```
DGS-3312SR:4#enable snmp traps
Command: enable snmp traps

Success.

DGS-3312SR:4#
```

enable snmp authenticate_traps

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

Example Usage:

To turn on SNMP authentication trap support:

```
DGS-3312SR:4#enable snmp authenticate_traps
Command: enable snmp authenticate_traps

Success.

DGS-3312SR: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-3312SR:4#disable snmp traps
Command: disable snmp traps

Success.

DGS-3312SR: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.

Example Usage:

To disable the SNMP authentication trap support:

```
DGS-3312SR:4#disable snmp authenticate_traps
Command: disable snmp authenticate_traps

Success.

DGS-3312SR:4#
```

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

Example usage:

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

```
DGS-3312SR:4#config snmp system_contact MIS Department II
Command: config snmp system_contact MIS Department II

Success.

DGS-3312SR: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	The **config snmp system_location** command is used to enter a description of the location of the switch. A maximum of 255 characters can be used.
Parameters	*<sw_location>* - A maximum of 255 characters is allowed. A NULL string is accepted if there is no location desired.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure the switch location for "**HQ 5F**":

```
DGS-3312SR:4#config snmp system_location HQ 5F
Command: config snmp system_location HQ 5F

Success.

DGS-3312SR:4#
```

config snmp system_name

Purpose	Used to configure the name for the switch.
Syntax	**config snmp system_name {<sw_name>}**
Description	The **config snmp system_name** command configures the name of the switch.
Parameters	*<sw_name>* - A maximum of 255 characters is allowed. A NULL string is accepted if no name is desired.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure the switch name for "**DGS-3312SR Stackable Switch**":

```
DGS-3312SR:4#config snmp system_name DGS-3312SR Stackable Switch
Command: config snmp system_name DGS-3312SR Stackable Switch

Success.

DGS-3312SR: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-3312SR:4#enable rmon
Command: enable rmon

 Success.

DGS-3312SR:4#
```

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

Example Usage:

To disable RMON:

```
DGS-3312SR:4#disable rmon
Command: disable rmon

Success.

DGS-3312SR:4#
```

8

SWITCH UTILITY COMMANDS

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

Command	Parameters
download	[firmware <ipaddr> <path_filename 64> {unit [all | master | <unitid 1-13>]} | configuration <ipaddr> <path_filename 64> {increment}]
upload	[configuration | log] <ipaddr> <path_filename 64>]
ping	<ipaddr> {times <value 1-255>} {timeout <sec 1-99>}
traceroute	<ipaddr> {ttl <value 1-60> | port <value 30000-64900> | timeout <sec 1-65535> | probe <value <1-9>}

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

download

Purpose	Used to download and install new firmware or a switch configuration file from a TFTP server.
Syntax	**download [firmware <ipaddr> <path_filename 64> {unit [all | master | <unitid 1-13>]} | configuration <ipaddr> <path_filename 64> {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. • *<ipaddr>* – The IP address of the TFTP server. • *<path_filename>* – The DOS path and filename of the firmware or switch configuration file on a TFTP server. For example, C:\3226S.had. The length of the filename must not exceed 64 characters. • *unit [all | <unitid 1-13>] – all* specifies all units (switches), *<unitid>* is the unit ID of the switch that will receive the download. • *master* – Specifies the master switch in a switch stack. *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 a TFTP server. For example, C:\3226S.had. • *increment* – Allows the download of a partial switch configuration file. This allows a file to be downloaded that will change only the switch parameters explicitly stated in the configuration file. All other switch parameters will remain unchanged.

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

Example usage:

To download a configuration file:

```
DGS-3312SR: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-3312SR: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 64]**
Description	This command is used to upload either the switch's current settings or the switch's history log to a TFTP server.
Parameters	*configuration* – Specifies that the switch's current settings will be uploaded to the TFTP server. *log* – Specifies that the switch's current 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 64>* – Specifies the location of the switch configuration file on the TFTP server. This file will be replaced by the uploaded file from the switch. The length of the filename must not exceed 64 characters.
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-3312SR: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-3312SR:4#
```

ping	
Purpose	Used to test the connectivity between network devices.
Syntax	**ping <ipaddr> {times <value 1-255>} {timeout <sec 1-99>}**
Description	The ping command sends Internet Control Message Protocol (ICMP) echo messages to a remote IP address. The remote IP address will then “echo” or return the message. This is used to confirm connectivity between the switch and the remote device.
Parameters	*<ipaddr>* - Specifies the IP address of the host. *times <value 1-255>* - The number of individual ICMP echo messages to be sent. The maximum value is 255. The default is 0. *timeout <sec 1-99>* - Defines the time-out period while waiting for a response from the remote device. A value of 1 to 99 seconds can be specified. The default is 1 second. Pinging an IP address without the *times* parameter will ping the target device an infinite amount of times.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To ping the IP address 10.48.74.121 four times:

```
DGS-3312SR:4#ping 10.48.74.121 times 4
Command: ping 10.48.74.121 times 4

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

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

DGS-3312SR:4#
```

traceroute	
Purpose	Used to trace the routed path between the switch and a destination endstation.
Syntax	**<ipaddr> {ttl <value 1-60> | port <value 30000-64900> | timeout <sec 1-65535> | probe <value <1-9>**
Description	The **traceroute** command allows you to trace a route between the switch and a give host on the network.
Parameters	*<ipaddr>* - Specifies the IP address of the host. *ttl <value 1-60>* - The time to live value of the trace route request. This is the maximum number of routers the traceroute command will cross while seeking the network path between two devices. *port <value 30000-64900>* The port number. Must be above 1024.The value range is from 30000 to 64900 . *timeout <sec 1-65535>*- Defines the time-out period while waiting for a response from the remote device. The user may choose an entry

traceroute	
	between 1 and 65535 seconds. *probe <value 1-9>* - The probe value is the number of times the switch will send probe packets to the next hop on the intended traceroute path. The default is 1.
Restrictions	None.

Example usage:

To trace the routed path between the switch and 10.48.74.121.

```
DGS-3312SR:4#traceroute 10.48.74.121 probe 3
Command: traceroute 10.48.74.121 probe 3

1  <10ms 10.254.254.251
2  <10ms 10.55.25.35
3  <10ms 10.22.35.1

DGS-3312SR:4#
```

9

NETWORK MONITORING COMMANDS

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

Command	Parameters
show packet ports	<portlist>
show error ports	<portlist>
show utilization	[cpu | unit_id <int>]
clear counters	ports <portlist>
clear log	
show log	index <value>
enable syslog	
disable syslog	
show syslog	
create syslog host	<index 1-4> ipaddress <ipaddr> {severity [informational | warning | all] | facility [local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7] | udp_port <udp_port_number> | ipaddress <ipaddr> | state [enable | disable]}
config syslog host	[all | <index 1-4>] {severity [informational | warning | all] | facility [local0 | local1| local2 | local3 | local4 | local5 | local6 | local7] | udp_port <udp_port_number> | ipaddress <ipaddr> | state [enable | disable]}
delete syslog host	[<index 1-4 | all >]
show syslog host	[<index 1-4>]

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

NOTE: As a stand-alone switch or as a master switch in a switch stack, the switch number will be referred to as 15 for all configurations, graphs and tables.

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 displayed. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the

show packet ports	
	highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3-2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order.
Restrictions	None.

Example usage:

To display the packets analysis for port 7 of module 2:

```
DGS-3312SR:4#show packet port 2:7

Command: show packet port 2:7

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

Unicast RX      152           1
Multicast RX    557           2
Broadcast RX    3686          16

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

show error ports	
Purpose	Used to display the error statistics for a range of ports.
Syntax	**show error ports <portlist>**
Description	This command will display all of the packet error statistics collected and logged by the switch for a given port list.
Parameters	*<portlist>* – Specifies a range of ports to be displayed. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3-2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order.
Restrictions	None.

Example usage:

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

```
DGS-3312SR:4#show errors port 1:3
Command : show errors port 1:3

Port number 1:3
Error Type    RX Frames       Error Type              TX Frames
--------------  --------------  --------------------------  ----------------
CRC Error     19              Excessive Deferral      0
Undersize     0               CRC Error               0
Oversize      0               Late Collision          0
Fragment      0               Excessive Collision     0
Jabber        11              Single Collision        0
Drop Pkts     20837           Collision               0

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

show utilization

Purpose	Used to display real-time port and cpu utilization statistics.
Syntax	**show utilization [cpu | unit_id <int>]**
Description	This command will display the real-time port and cpu utilization statistics for the switch.
Parameters	*cpu* – Entering this parameter will display the current cpu utilization of the switch, as a percentage. *unit_id* <*int*> - Entering this parameter, along with the appropriate switch number, will display the current utilization of all ports on the switch of a switch stack.
Restrictions	None.

Example usage:

To display the port utilization statistics:

```
DGS-3312SR:4#show utilization unit_id 1
Command: show utilization unit_id 1

Port    TX/sec     RX/sec    Util    Port    TX/sec     RX/sec    Util
 ----    ----------  ----------  ----    ----    ----------  ----------  ----
 1:1     0          0         0
 1:2     0          0         0
 1:3     0          0         0
 1:4     0          0         0
 1:5     0          0         0
 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

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

To display the current cpu utilization:

```
DGS-3312SR:4#show utilization cpu
Command: show utilization cpu

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

DGS-3312SR:4#
```

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 lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3-2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To clear the counters:

```
DGS-3312SR:4#clear counters ports 2:7-2:9
Command: clear counters ports 2:7-2:9

Success.

DGS-3312SR:4#
```

clear log

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

Example usage:

To clear the log information:

```
DGS-3312SR:4#clear log
Command: clear log

Success.

DGS-3312SR: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>* – Enter a value that corresponds to an entry made in the log. Multiple entries may be made in the form of *x-x* where x is the number of an entry in the log. The smallest number (and therefore the earlier entry) will be first.
Restrictions	None.

Example usage:

To display the switch history log**:**

```
DGS-3312SR:4#show log index 1-4
Command: show log index 1-4

Index  Time      Log Text
-----  --------  ----------------------------------------------------
4      01:54:53  Port 1:13 link up, 100Mbps FULL duplex
3      01:54:53  Spanning Tree Protocol is enabled
2      01:54:53  Unit 1, System started up
1      06:06:09  Spanning Tree Protocol is disabled

DGS-3312SR:4#
```

enable syslog

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

Example usage:

To the syslog function on the switch:

```
DGS-3312SR:4#enable syslog
Command: enable syslog

Success.

DGS-3312SR:4#
```

disable syslog

Purpose	Used to disable the system log function on the switch.
Syntax	**disable syslog**
Description	The **disable syslog** command disables the system log function on the switch. After disabling, Syslog entries will no longer be sent to a remote host.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To disable the syslog function on the switch:

```
DGS-3312SR:4#disable syslog
Command: disable syslog

Success.

DGS-3312SR:4#
```

show syslog

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

Example usage:

To display the current status of the syslog function:

```
DGS-3312SR:4#show syslog
Command: show syslog

Syslog Global State: Enabled

DGS-3312SR:4#
```

create syslog host	
Purpose	Used to create a new syslog host.
Syntax	**create syslog host <index 1-4> ipaddress <ipaddr> {severity [informational | warning | all] facility [local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7] | udp_port<int> | state [enable | disable]}**
Description	The **create syslog host** command is used to create a new syslog host.
Parameters	*<index 1-4>* – Specifies that the command will be applied to an index of hosts. There are four available indexes, numbered 1 through 4. *ipaddress <ipaddr>* – Specifies the IP address of the remote host where syslog messages will be sent. *severity* – Severity level indicator. These are described in the following: Bold font indicates that the corresponding severity level is currently supported on the switch. Numerical Severity Code 0 Emergency: system is unusable 1 Alert: action must be taken immediately 2 Critical: critical conditions 3 Error: error conditions **4 Warning: warning conditions** 5 Notice: normal but significant condition **6 Informational: informational messages** 7 Debug: debug-level messages *informational* – Specifies that informational messages will be sent to the remote host. This corresponds to number 6 from the list above. *warning* – Specifies that warning messages will be sent to the remote host. This corresponds to number 4 from the list above. *all* – Specifies that all of the currently supported syslog messages that are generated by the switch will be sent to the remote host. *facility* – Some of the operating system daemons and processes have been assigned Facility values. Processes and daemons that have not been explicitly assigned a Facility may use any of the "local use" facilities or they may use the "user-level" Facility. Those Facilities that have been designated are shown in the following: Bold font indicates the facility values that the switch currently supports.

create syslog host	
	Numerical Code Facility 0 kernel messages 1 user-level messages 2 mail system 3 system daemons 4 security/authorization messages 5 messages generated internally by syslog 6 line printer subsystem 7 network news subsystem 8 UUCP subsystem 9 clock daemon 10 security/authorization messages 11 FTP daemon 12 NTP subsystem 13 log audit 14 log alert 15 clock daemon **16 local use 0 (local0)** **17 local use 1 (local1)** **18 local use 2 (local2)** **19 local use 3 (local3)** **20 local use 4 (local4)** **21 local use 5 (local5)** **22 local use 6 (local6)** **23 local use 7 (local7)** *local0* – Specifies that local use 0 messages will be sent to the remote host. This corresponds to number 16 from the list above. *local1* – Specifies that local use 1 messages will be sent to the remote host. This corresponds to number 17 from the list above. *local2* – Specifies that local use 2 messages will be sent to the remote host. This corresponds to number 18 from the list above. *local3* – Specifies that local use 3 messages will be sent to the remote host. This corresponds to number 19 from the list above. *local4* – Specifies that local use 4 messages will be sent to the remote host. This corresponds to number 20 from the list above. *local5* – Specifies that local use 5 messages will be sent to the remote host. This corresponds to number 21 from the list above. *local6* – Specifies that local use 6 messages will be sent to the remote host. This corresponds to number 22 from the list above. *local7* – Specifies that local use 7 messages will be sent to the remote host. This corresponds to number 23 from the list above. *udp_port <int>* – Specifies the UDP port number that the syslog protocol will use to send messages to the remote host. *state [enable | disable]* – Allows the sending of syslog messages to the remote host, specified above, to be enabled and disabled.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To create syslog host:

```
DGS-3312SR:4#create syslog host 1 ipaddress 10.53.13.200
severity all facility local0 state enable

Command: create syslog host 1 ipaddress 10.53.13.200 severity
all facility local0 state enable


Success.


DGS-3312SR:4#
```

config syslog host

Purpose	Used to configure the syslog protocol to send system log data to a remote host.
Syntax	**config syslog host [all | <index 1-4>] {severity [informational | warning | all] | facility [local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7] | udp_port<int> | ipaddress <ipaddr> | state [enable | disable]}**
Description	The **config syslog host** command is used to configure the syslog protocol to send system log information to a remote host.

config syslog host

Parameters

all – Specifies that the command will be applied to all hosts.

<index 1-4> – Specifies that the command will be applied to an index of hosts. There are four available indexes, numbered 1 through 4.

severity – Severity level indicator. These are described in the following:

Bold font indicates that the corresponding severity level is currently supported on the switch.

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

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

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

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

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

Numerical Code	Facility
0	kernel messages
1	user-level messages
2	mail system
3	system daemons
4	security/authorization messages
5	messages generated internally by syslog
6	line printer subsystem
7	network news subsystem
8	UUCP subsystem
9	clock daemon
10	security/authorization messages
11	FTP daemon
12	NTP subsystem
13	log audit
14	log alert
15	clock daemon

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

Example usage:

To configure a syslog host:

```
DGS-3312SR:4#config syslog host all severity all facility local0
Command: config syslog host all severity all facility local0

Success.

DGS-3312SR:4#
```

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

Example usage:

To delete a previously configured syslog host:

```
DGS-3312SR:4#delete syslog host 4
Command: delete syslog host 4

Success.

DGS-3312SR:4#
```

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

Example usage:

To show syslog host information:

```
DGS-3312SR:4#show syslog host
Command: show syslog host

Syslog Global State: Disabled

Host Id  Host IP Address  Severity  Facility  UDP port  Status
-------  ---------------  --------  --------  --------  --------
1        10.1.1.2         All       Local0    514       Disabled
2        10.40.2.3        All       Local0    514       Disabled
3        10.21.13.1       All       Local0    514       Disabled

Total Entries : 3

DGS-3312SR:4#
```

10

MULTIPLE SPANNING TREE PROTOCOL (MSTP) COMMANDS

This switch supports three versions of the Spanning Tree Protocol; 802.1d STP, 802.1w Rapid STP and 802.1s MSTP. Multiple Spanning Tree Protocol, or MSTP, is a standard defined by the IEEE community that allows multiple VLANs to be mapped to a single spanning tree instance, which will provide multiple pathways across the network. Therefore, these MSTP configurations will balance the traffic load, preventing wide scale disruptions when a single spanning tree instance fails. This will allow for faster convergences of new topologies for the failed instance. Frames designated for these VLANs will be processed quickly and completely throughout interconnected bridges utilizing either of the three spanning tree protocols (STP, RSTP or MSTP). This protocol will also tag BDPU packets so receiving devices can distinguish spanning tree instances, spanning tree regions and the VLANs associated with them. These instances will be classified by an *instance_id*. MSTP will connect multiple spanning trees with a Common and Internal Spanning Tree (CIST). The CIST will automatically determine each MSTP region, its maximum possible extent and will appear as one virtual bridge that runs a single spanning tree. Consequentially, frames assigned to different VLANs will follow different data routes within administratively established regions on the network, continuing to allow simple and full processing of frames, regardless of administrative errors in defining VLANs and their respective spanning trees. Each switch utilizing the MSTP on a network will have a single MSTP configuration that will have the following three attributes:

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

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

c) A 4094 element table (defined here as a *vid_range*) which will associate each of the possible 4094 VLANs supported by the Switch for a given instance.

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

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

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

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

Command	Parameters
enable stp	
disable stp	
config stp version	[mstp | rstp | stp]
config stp	{maxage <value 6-40> | maxhops <value 1-20> | hellotime <value 1-10> | forwarddelay <value 4-30>| txholdcount <value 1-10> | fbpdu [enable | disable]}
config stp ports	<portlist> {externalCost [auto | <value 1-200000000>] | hellotime <value 1-10> | migrate [yes | no] | edge [true | false] | p2p [true | false | auto] | state [enable | disable]
create stp instance_id	<value 1-15>
config stp instance _id	<value 1-15> [add_vlan | remove_vlan] <vidlist>
delete stp instance_id	<value 1-15>
config stp priority	<value 0-61440> instance_id <value 0-15>
config stp	{revision_level <int 0-65535> | name <string>}

Command	Parameters
mst_config_id	
config stp mst_ports	<portlist> instance_id <value 0-15> {internalCost [auto | value 1-200000000] | priority <value 0-240>}
show stp	
show stp ports	{<portlist>}
show stp instance_id	{<value 0-15>}
show stp mst_config id	

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

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

Example usage:

To enable STP, globally, on the Switch:

```
DGS-3312SR:4#enable stp
Command: enable stp

Success.

DGS-3312SR: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-3312SR:4#disable stp
Command: disable stp

Success.

DGS-3312SR:4#
```

config stp version

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

Example usage:

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

```
DGS-3312SR:4#config stp version mstp
Command: config stp version mstp

Success.

DGS-3312SR:4#
```

config stp

Purpose	Used to setup STP, RSTP and MSTP on the Switch.
Syntax	**config stp {maxage <value 6-40> | maxhops <value 1-20> | hellotime <1-10> | forwarddelay <value 4-30> | txholdcount <value 1-10> | fbpdu [enable | disable]}**
Description	This command is used to setup the Spanning Tree Protocol (STP) for the entire switch. All commands here will be implemented for the STP version that is currently set on the Switch.
Parameters	*maxage* <*value 6-40*> – This value may be set to ensure that old information does not endlessly circulate through redundant paths

config stp	
	in the network, preventing the effective propagation of the new information. Set by the Root Bridge, this value will aid in determining that the Switch has spanning tree configuration values consistent with other devices on the bridged LAN. If the value ages out and a BPDU has still not been received from the Root Bridge, the Switch will start sending its own BPDU to all other switches for permission to become the Root Bridge. If it turns out that your switch has the lowest Bridge Identifier, it will become the Root Bridge. The user may choose a time between 6 and 40 seconds. The default value is 20. *maxhops* <*value 1-20*> - The number of hops between devices in a spanning tree region before the BPDU (bridge protocol data unit) packet sent by the Switch will be discarded. Each switch on the hop count will reduce the hop count by one until the value reaches zero. The Switch will then discard the BDPU packet and the information held for the port will age out. The user may set a hop count from 1 to 20. The default is 20. *hellotime* <*value 1-10*> – The user may set the time interval between transmission of configuration messages by the root device in STP, or by the designated router in RSTP, thus stating that the Switch is still functioning. A time between 1 and 10 seconds may be chosen, with a default setting of 2 seconds. In MSTP, the spanning tree is configured by port and therefore, the *hellotime* must be set using the **configure stp ports** command for switches utilizing the Multiple Spanning Tree Protocol. *forwarddelay* <*value 4-30*> – The maximum amount of time (in seconds) that the root device will wait before changing states. The user may choose a time between 4 and 30 seconds. The default is 15 seconds. *txholdcount* <*value 1-10*> - The maximum number of BDPU Hello packets transmitted per interval. Default value = 3. *fbpdu [enable* | *disable]* – Allows the forwarding of STP BPDU packets from other network devices when STP is disabled on the Switch. The default is *enable*.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure STP with maxage 18 and maxhops of 15:

```
DGS-3312SR:4#config stp maxage 18 maxhops 15

Command: config stp maxage 18 maxhops 15


Success.


DGS-3312SR:4#
```

config stp ports

Purpose	Used to setup STP on the port level.
Syntax	**config stp ports <portlist> {externalCost [auto | <value 1-200000000>] | hellotime <value 1-10> | migrate [yes | no] | edge [true | false] | p2p [true | false | auto] | state [enable | disable]**
Description	This command is used to create and configure STP for a group of ports.
Parameters	*<portlist>* – Specifies a range of ports to be configured. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3-2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. *externalCost* – This defines a metric that indicates the relative cost of forwarding packets to the specified port list. Port cost can be set automatically or as a metric value. The default value is *auto*. *auto* – Setting this parameter for the external cost will automatically set the speed for forwarding packets to the specified port(s) in the list for optimal efficiency. Default port cost: 100Mbps port = 200000. Gigabit port = 20000. • *<value 1-200000000>* - Define a value between 1 and 200000000 to determine the external cost. The lower the number, the greater the probability the port will be chosen to forward packets. *hellotime <value 1-10>* – The time interval between transmission of configuration messages by the designated port, to other devices on the bridged LAN, thus stating that the Switch is still functioning. The user may choose a time between 1 and 10 seconds. The default is 2 seconds. *migrate [yes | no]* – Setting this parameter as "*yes*" will set the ports to send out BDPU packets to other bridges, requesting information on their STP setting If the Switch is configured for RSTP, the port will be capable to migrate from 802.1d STP to 802.1w RSTP. If the Switch is configured for MSTP, the port is capable of migrating from 802.1d STP to 802.1s MSTP. RSTP and MSTP can coexist with standard STP, however the benefits of RSTP and MSTP are not realized on a port where an 802.1d network connects to an 802.1w or 802.1s enabled network. Migration should be set as *yes* on ports connected to network stations or segments that are capable of being upgraded to 802.1w RSTP or 802.1s MSTP on all or some portion of the segment. *edge [true | false]* – *true* designates the port as an edge port. Edge ports cannot create loops, however an edge port can lose edge port status if a topology change creates a potential for a loop. An edge port normally should not receive BPDU packets. If a BPDU packet is received it automatically loses edge port status. *false* indicates that the port does not have edge port status. *p2p [true | false | auto]* – *true* indicates a point-to-point (P2P)

config stp ports	
	shared link. P2P ports are similar to edge ports however they are restricted in that a P2P port must operate in full-duplex. Like edge ports, P2P ports transition to a forwarding state rapidly thus benefiting from RSTP. A p2p value of false indicates that the port cannot have p2p status. auto allows the port to have p2p status whenever possible and operate as if the p2p status were true. If the port cannot maintain this status (for example if the port is forced to half-duplex operation) the p2p status changes to operate as if the p2p value were false. The default setting for this parameter is auto. *state [enable* | *disable]* – Allows STP to be enabled or disabled for the ports specified in the port list. The default is enable.
Restrictions	Only administrator-level users can issue this command.

Example usage:

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

```
DGS-3312SR:4#config stp ports 1:1-1:5 externalCost 19 hellotime
5 migrate yes state enable
Command: config stp ports 1:1-1:5 externalCost 19 hellotime 5
migrate yes state enable

Success.

DGS-3312SR:4#
```

create stp instance_id	
Purpose	Used to create a STP instance ID for MSTP.
Syntax	**create stp instance_id <value 1-15>**
Description	This command allows the user to create a STP instance ID for the Multiple Spanning Tree Protocol. There are 16 STP instances on the Switch (one internal CIST, unchangeable) and the user may create up to 15 instance IDs for the Switch.
Parameters	*<value 1-15>* - Enter a value between 1 and 15 to identify the Spanning Tree instance on the Switch.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To create a spanning tree instance 2:

```
DGS-3312SR:4#create stp instance_id 2
Command: create stp instance_id 2

Success.

DGS-3312SR:4#
```

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

Example usage:

To configure instance id 2 to add VID 10:

```
DGS-3312SR:4#config stp instance_id 2 add_vlan 10
Command : config stp instance_id 2 add_vlan 10

Success.

DGS-3312SR:4#
```

Example usage:

To remove VID 10 from instance id 2:

```
DGS-3312SR:4#config stp instance_id 2 remove_vlan 10
Command : config stp instance_id 2 remove_vlan 10

Success.

DGS-3312SR:4#
```

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

Example usage:

To delete stp instance id 2 from the Switch.

```
DGS-3312SR:4#delete stp instance_id 2
Command: delete stp instance_id 2

Success.

DGS-3312SR:4#
```

config stp priority	
Purpose	Used to update the STP instance configuration.
Syntax	**config stp priority <value 0-61440> instance_id <value 0-15>**
Description	This command is used to update the STP instance configuration settings on the Switch. The MSTP will utilize the priority in selecting the root bridge, root port and designated port. Assigning higher priorities to STP regions will instruct the Switch to give precedence to the selected *instance_id* for forwarding packets. The lower the priority value set, the higher the priority.
Parameters	*priority <value 0-61440>* - Select a value between 0 and 61440 to specify the priority for a specified instance id for forwarding packets. The lower the value, the higher the priority. This entry must be divisible by 4096. *instance_id <value 0-15>* - Enter the value corresponding to the previously configured instance id of which the user wishes to set the priority value. An instance id of *0* denotes the default *instance_id* (CIST) internally set on the Switch.
Restrictions	Only administrator-level users can issue this command.

Example usage:

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

```
DGS-3312SR:4#config stp priority 4096 instance_id 2
Command : config stp priority 4096 instance_id 2

Success.

DGS-3312SR:4#
```

config stp mst_config_id	
Purpose	Used to update the MSTP configuration identification.
Syntax	**config stp mst_config_id {revision_level <int 0-65535> | name <string>**
Description	This command will uniquely identify the MSTP configuration currently configured on the Switch. Information entered here will be attached to BDPU packets as an identifier for the MSTP region to which it belongs. Switches having the same *revision_level* and *name* will be considered as part of the same MSTP region.
Parameters	*revision_level <int 0-65535>*– Enter a number between 0 and 65535 to identify the MSTP region. This value, along with the name will identify the MSTP region configured on the Switch. The default setting is *0*. *name <string>* - Enter an alphanumeric string of up to 32 characters to uniquely identify the MSTP region on the Switch. This *name*, along with the *revision_level* value will identify the MSTP region configured on the Switch. If no *name* is entered, the default name will be the MAC address of the device.
Restrictions	Only administrator-level users can issue this command.

Example usage:

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

```
DGS-3312SR:4#config stp mst_config_id revision_level 10 name Trinity

Command : config stp mst_config_id revision_level 10 name Trinity


Success.


DGS-3312SR:4#
```

config stp mst_ports	
Purpose	Used to update the port configuration for a MSTP instance.
Syntax	**config stp mst_ports <portlist> instance_id <value 0-15> {internalCost [auto | <value 1-20000000>] `priority <value 0-240>}**
Description	This command will update the port configuration for a STP *instance_id*. If a loop occurs, the MSTP function will use the port priority to select an interface to put into the forwarding state. Set a higher priority value for interfaces to be selected for forwarding first. In instances where the priority value is identical, the MSTP function will implement the lowest port number into the forwarding state and other interfaces will be blocked. Remember that lower priority values mean higher priorities for forwarding packets.
Parameters	*<portlist>* - Specifies a port or range of ports to be configured. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For

config stp mst_ports	
	example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3-2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. *instance_id* <*value 0-15*> - Enter a numerical value between 0 and 15 to identify the *instance_id* previously configured on the Switch. An entry of 0 will denote the CIST (Common and Internal Spanning Tree. *internalCost* – This parameter is set to represent the relative cost of forwarding packets to specified ports when an interface is selected within a STP instance. The default setting is *auto*. There are two options: • *auto* – Selecting this parameter for the *internalCost* will set quickest route automatically and optimally for an interface. The default value is derived from the media speed of the interface. • *value 1-2000000* – Selecting this parameter with a value in the range of 1-2000000 will set the quickest route when a loop occurs. A lower *internalCost* represents a quicker transmission. *priority* <*value 0-240*> - Enter a value between 0 and 240 to set the priority for the port interface. A higher priority will designate the interface to forward packets first. A lower number denotes a higher priority.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To designate ports 1 through 5 on module one, with instance ID 2, to have an auto internalCost and a priority of 16:

```
DGS-3312SR:4#config stp mst_config_id ports 1:1-1:5 instance_id
2 internalCost auto priority 16

Command : config stp mst_config_id ports 1:1-1:5 instance_id 2
internalCost auto priority 16


Success.


DGS-3312SR:4#
```

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

Example usage:

To display the status of STP on the Switch:

Status 1: STP enabled with STP compatible version

```
DGS-3312SR:4#show stp
Command: show stp

STP Status              : Enabled
STP Version             : STP Compatible
Max Age                 : 20
Hello Time              : 2
Forward Delay           : 15
Max Age                 : 20
TX Hold Count           : 3
Forwarding BPDU         : Enabled

DGS-3312SR:4#
```

Status 2 : STP enabled for RSTP

```
DGS-3312SR:4#show stp
Command: show stp

STP Status              : Enabled
STP Version             : RSTP
Max Age                 : 20
Hello Time              : 2
Forward Delay           : 15
Max Age                 : 20
TX Hold Count           : 3
Forwarding BPDU         : Enabled

DGS-3312SR:4#
```

Status 3 : STP enabled for MSTP

```
DGS-3312SR:4#show stp
Command: show stp

STP Status              : Enabled
STP Version             : MSTP
Max Age                 : 20
Forward Delay           : 15
Max Age                 : 20
TX Hold Count           : 3
Forwarding BPDU         : Enabled

DGS-3312SR:4#
```

show stp ports

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

Example usage:

To show stp ports 1 through 9 on switch one:

```
DGS-3312SR:4#show stp ports 1:1-1:9

Command: show stp ports 1:1-1:9


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


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


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

show stp instance_id

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

Example usage:

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

```
DGS-3312SR:4#show stp instance 0
Command: show stp instance 0

STP Instance Settings
 --------------------------
 Instance Type              : CIST
 Instance Status            : Enabled
 Instance Priority          : 32768(bridge priority : 32768, sys ID ext : 0 )

 STP Instance Operational Status
 -------------------------------
 Designated Root Bridge   : 32766/00-90-27-39-78-E2
 External Root Cost       : 200012
 Regional Root Bridge     : 32768/00-53-13-1A-33-24
 Internal Root Cost       : 0
 Designated Bridge        : 32768/00-50-BA-71-20-D6
 Root Port                : 1:1
 Max Age                  : 20
 Forward Delay            : 15
 Last Topology Change     : 856
 Topology Changes Count : 2987

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

show stp mst_config_id

Purpose	Used to display the MSTP configuration identification.
Syntax	**show stp mst_config_id**
Description	This command displays the Switch's current MSTP configuration identification.
Parameters	None.
Restrictions	None.

Example usage:

To show the MSTP configuration identification currently set on the Switch:

```
DGS-3312SR:4#show stp mst_config_id
Command: show stp mst_config_id

Current MST Configuration Identification
 ---------------------------------------

 Configuration Name : 00:53:13:1A:33:24          Revision Level :0
 MSTI ID    Vid list
 -------    -----------
   CIST     2-4094
      1     1

DGS-3312SR:4#
```

11

FORWARDING DATABASE COMMANDS

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

Command	Parameters
create fdb	<vlan_name 32> <macaddr> port <port>
create multicast_fdb	<vlan_name 32> <macaddr>
config multicast_fdb	<vlan_name 32> <macaddr> [add | delete] <portlist>
config fdb aging_time	<sec 10-1000000>
delete fdb	<vlan_name 32> <macaddr>
clear fdb	[vlan <vlan_name 32> | port <port> | all]
show multicast_fdb	{vlan <vlan_name 32> | mac_address <macaddr>}
show fdb	{port <port> | vlan <vlan_name 32> | mac_address <macaddr> | static | aging_time}
show ipfdb	{ip_address <ipaddr> | interface <ipif_name 12> | port <port>}

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

NOTE: As a stand-alone switch or as a master switch in a switch stack, the switch number will be referred to as 15 for all configurations, graphs and tables.

create fdb	
Purpose	Used to create a static entry to the unicast MAC address forwarding table (database).
Syntax	**create fdb <vlan_name 32> <macaddr> [port <port>]**
Description	This command will make an entry into the switch's unicast MAC address forwarding database.
Parameters	*<vlan_name 32>* – The name of the VLAN on which the MAC address resides. *<macaddr>* – The MAC address that will be added to the forwarding table. *port <port>* – The port number corresponding to the MAC destination address. The switch will always forward traffic to the specified device through this port.
Restrictions	Only administrator-level users can issue this command.

Example usage:

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

```
DGS-3312SR:4#create fdb default 00-00-00-00-01-02 port 2:5
Command: create fdb default 00-00-00-00-01-02 port 2:5

Success.

DGS-3312SR:4#
```

create multicast_fdb

Purpose	Used to create a static entry to the multicast MAC address forwarding table (database)
Syntax	**create multicast_fdb <vlan_name 32> <macaddr>**
Description	This command will make an entry into the switch's multicast MAC address forwarding database.
Parameters	*<vlan_name 32>* – The name of the VLAN on which the MAC address resides. *<macaddr>* – The MAC address that will be added to the forwarding table.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To create multicast MAC forwarding**:**

```
DGS-3312SR:4#create multicast_fdb default 01-00-00-00-00-01
Command: create multicast_fdb default 01-00-00-00-00-01

Success.

DGS-3312SR:4#
```

config multicast_fdb

Purpose	Used to configure the switch's multicast MAC address forwarding database.
Syntax	**config multicast_fdb <vlan_name 32> <macaddr> [add | delete] <portlist>**
Description	This command configures the multicast MAC address forwarding table.
Parameters	*<vlan_name 32>* – The name of the VLAN on which the MAC address resides. *<macaddr>* – The MAC address that will be added to the multicast forwarding table. *[add | delete]* – Add will add ports to the forwarding table. Delete will remove ports from the multicast forwarding table. ▪ *<portlist>* – Specifies a range of ports to be configured. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are

config multicast_fdb	
	separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3-2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To add multicast MAC forwarding:

```
DGS-3312SR:4#config multicast_fdb default 01-00-00-00-00-01 add 1:1-1:5
Command: config multicast_fdb default 01-00-00-00-00-01 add 1:1-1:5

Success.

DGS-3312SR:4#
```

config fdb aging_time	
Purpose	Used to set the aging time of the forwarding database.
Syntax	**config fdb aging_time <sec 10-1000000>**
Description	The aging time affects the learning process of the switch. Dynamic forwarding table entries, which are made up of the source MAC addresses and their associated port numbers, are deleted from the table if they are not accessed within the aging time. The aging time can be from 10 to 1000000 seconds with a default value of 300 seconds. A very long aging time can result in dynamic forwarding table entries that are out-of-date or no longer exist. This may cause incorrect packet forwarding decisions by the switch. If the aging time is too short however, many entries may be aged out too soon. This will result in a high percentage of received packets whose source addresses cannot be found in the forwarding table, in which case the switch will broadcast the packet to all ports, negating many of the benefits of having a switch.
Parameters	*<sec 10-1000000>* – The aging time for the MAC address forwarding database value. The value in seconds may be between 10 and 1000000 seconds. The default is 300 seconds.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To set the fdb aging time:

```
DGS-3312SR:4#config fdb aging_time 300
Command: config fdb aging_time 300

Success.

DGS-3312SR:4#
```

delete fdb	
Purpose	Used to delete an entry to the switch's forwarding database.
Syntax	**delete fdb <vlan_name 32> <macaddr>**
Description	This command is used to delete a previous entry to the switch's MAC address forwarding database.
Parameters	*<vlan_name 32>* – The name of the VLAN on which the MAC address resides. *<macaddr>* – The MAC address that will be deleted from the forwarding table.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To delete a permanent FDB entry:

```
DGS-3312SR:4#delete fdb default 00-00-00-00-01-02
Command: delete fdb default 00-00-00-00-01-02

Success.

DGS-3312SR:4#
```

Example usage:

To delete a multicast fdb entry:

```
DGS-3312SR:4#delete fdb default 01-00-00-00-01-02
Command: delete fdb default 01-00-00-00-01-02

Success.

DGS-3312SR:4#
```

clear fdb	
Purpose	Used to clear the switch's forwarding database of all dynamically learned MAC addresses.
Syntax	**clear fdb [vlan <vlan_name 32> | port <port> | all]**
Description	This command is used to clear dynamically learned entries to the switch's forwarding database.
Parameters	*vlan <vlan_name 32>* – The name of the VLAN on which the MAC address resides. *port <port>* – The port number corresponding to the MAC destination address. The switch will always forward traffic to the

clear fdb	
	specified device through this port. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3-2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. *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-3312SR:4#clear fdb all
Command: clear fdb all

Success.

DGS-3312SR:4#
```

show multicast_fdb	
Purpose	Used to display the contents of the switch's multicast forwarding database.
Syntax	**show mulitcast_fdb [vlan <vlan_name 32> | mac_address <macaddr>]**
Description	This command is used to display the current contents of the switch's multicast MAC address forwarding database.
Parameters	*<vlan_name 32>* – The name of the VLAN on which the MAC address resides. *<macaddr>* – The MAC address that is present in the forwarding database table.
Restrictions	None.

Example usage:

To display multicast MAC address table:

```
DGS-3312SR:4#show multicast_fdb
Command: show multicast_fdb

VLAN Name       : default
MAC Address     : 01-00-5E-00-00-00
Egress Ports    : 1:1-1:5,1:12,2:12
Mode            : Static

Total Entries   : 1

DGS-3312SR:4#
```

show fdb

Purpose	Used to display the current unicast MAC address forwarding database.
Syntax	**show fdb {port <port> | vlan <vlan_name 32> | mac_address <macaddr> | static | aging_time}**
Description	This command will display the current contents of the switch's forwarding database.
Parameters	*port <port>* – The port number corresponding to the MAC destination address. The switch will always forward traffic to the specified device through this port. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3-2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. *<vlan_name 32>* – The name of the VLAN on which the MAC address resides. *<macaddr>* – The MAC address that is present in the forwarding database table. *static* – Displays the static MAC address entries. *aging_time* – Displays the aging time for the MAC address forwarding database.
Restrictions	None.

Example usage:

To display unicast MAC address table:

```
DGS-3312SR:4#show fdb
Command: show fdb

Unicast MAC Address Aging Time = 300

VID  VLAN Name      MAC Address          Port     Type
----  ---------------  ------------------------  ------  ---------------
1    default        00-00-39-34-66-9A    10       Dynamic
1    default        00-00-51-43-70-00    10       Dynamic
1    default        00-00-5E-00-01-01    10       Dynamic
1    default        00-00-74-60-72-2D    10       Dynamic
1    default        00-00-81-05-00-80    10       Dynamic
1    default        00-00-81-05-02-00    10       Dynamic
1    default        00-00-81-48-70-01    10       Dynamic
1    default        00-00-E2-4F-57-03    10       Dynamic
1    default        00-00-E2-61-53-18    10       Dynamic
1    default        00-00-E2-6B-BC-F6    10       Dynamic
1    default        00-00-E2-7F-6B-53    10       Dynamic
1    default        00-00-E2-82-7D-90    10       Dynamic
1    default        00-00-F8-7C-1C-29    10       Dynamic
1    default        00-01-02-03-04-00    CPU      Self
1    default        00-01-30-10-2C-C7    10       Dynamic
1    default        00-01-30-FA-5F-00    10       Dynamic
1    default        00-02-3F-63-DD-68    10       Dynamic
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

show ipfdb	
Purpose	Used to display the current IP address forwarding database table.
Syntax	**show ipfdb {ip_address <ipaddr> | interface <ipif_name 12> | port <port>}**
Description	This command will display the current contents of the switch's IP forwarding database.
Parameters	The user has three methods in which to view the table by, which are: *ip_address <ipaddr>* - Use this parameter to view the table by an IP address entered here. *interface <ipif_name 12>* - Use this parameter to view the table by an IP interface entered here, and set on the switch. *port <port>* - Use this parameter to view the table by a port entered here. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3-2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. Adding no parameters will display all entries in the IP forwarding database.
Restrictions	None.

Example usage:

To view the IP forwarding database table:

```
DGS-3312SR:4#show ipfdb
Command: show ipfdb

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

12

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 [enable | disable] | multicast [enable | disable] | dlf [enable | disable] | threshold <value 0-255> }
show traffic control	{group_list <storm_grouplist>}

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

NOTE: As a stand-alone switch or as a master switch in a switch stack, the switch number will be referred to as 15 for all configurations, graphs and tables.

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 0-255>}**
Description	This command is used to configure broadcast storm control.
Parameters	*<storm_grouplist>* – Used to specify a broadcast storm control group. This is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3-2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. *all* – Specifies all storm control groups on the switch. *broadcast [enable | disable]* – Enables or disables broadcast storm control. *multicast [enable | disable]* – Enables or disables multicast storm control. *dlf [enable | disable]* – Enables or disables dlf traffic control. *threshold <value 0-255>* – 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.
Restrictions	Only administrator-level users can issue this command.

Example usage:

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

```
DGS-3312SR:4#config traffic control all broadcast enable
Command: config traffic control all broadcast enable

Success.

DGS-3312SR: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. This is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3-2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order.
Restrictions	None.

Example usage:

To display traffic control setting:

```
DGS-3312SR:4#show traffic control 1:1-1:5
Command: show traffic control 1:1-1:5

Traffic Control
                                          Broadcast   Multicast   Destination
Module  Group [ports]   Threshold        Storm       Storm       Lookup Fail
------  -------------   ---------        ---------   ---------   --------
1        1   [ 1 ]      128              Disabled    Disabled    Disabled
1        2   [ 2 ]      128              Disabled    Disabled    Disabled
1        3   [ 3 ]      128              Disabled    Disabled    Disabled
1        4   [ 4 ]      128              Disabled    Disabled    Disabled
1        5   [ 5 ]      128              Disabled    Disabled    Disabled

Total Entries: 5

DGS-3312SR:4#
```

13

QOS COMMANDS

The DGS-3312SR switch supports 802.1p priority queuing. The switch has nine hardware priority queues, one of which is internal and not configurable. These hardware priority queues are numbered from 7 (Class 7) — the highest hardware priority queue — to 0 (Class 0) — the lowest hardware priority queue. The eight priority tags specified in IEEE 802.1p (p0 to p7) are mapped to the switch's hardware priority queues as follows:

- Priority 0 is assigned to the Switch's Q2 queue.
- Priority 1 is assigned to the Switch's Q0 queue.
- Priority 2 is assigned to the Switch's Q1 queue.
- Priority 3 is assigned to the Switch's Q3 queue.
- Priority 4 is assigned to the Switch's Q4 queue.
- Priority 5 is assigned to the Switch's Q5 queue.
- Priority 6 is assigned to the Switch's Q6 queue.
- Priority 7 is assigned to the Switch's Q7 queue.

For strict priority-based scheduling, any packets residing in the higher priority queues are transmitted first. Multiple strict priority queues empty based on their priority tags. Only when these queues are empty, are packets of lower priority transmitted.

For round-robin queuing, the number of packets sent from each priority queue depends upon the assigned weight. For a configuration of 8 CoS queues, A~H with their respective weight value: 8~1, the packets are sent in the following sequence: A1, B1, C1, D1, E1, F1, G1, H1, A2, B2, C2, D2, E2, F2, G2, A3, B3, C3, D3, E3, F3, A4, B4, C4, D4, E4, A5, B5, C5, D5, A6, B6, C6, A7, B7, A8, A1, B1, C1, D1, E1, F1, G1, H1.

For round-robin queuing, if each CoS queue has the same weight value, then each CoS queue has an equal opportunity to send packets just like round-robin queuing.

For round-robin queuing, if the weight for a CoS is set to 0, then it will continue processing the packets from this CoS until there are no more packets for this CoS. The other CoS queues that have been given a nonzero value, and depending upon the weight, will follow a common round-robin scheme.

Remember that the switch has 8 priority queues (and eight Classes of Service) for each port on the Switch.

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

NOTE: As a stand-alone switch or as a master switch in a switch stack, the switch number will be referred to as 15 for all configurations, graphs and tables.

Command	Parameters
config bandwidth_control	[<portlist> | all] {rx_rate [no_limit | <value 1-999>] | tx_rate [no_limit <value 1-999>]}
show bandwidth_control	{<portlist>}
config 802.1p user_priority	{<priority 0-7> <class_id 0-7>}
show 802.1p user_priority	
config 802.1p default_priority	[<portlist> | all] | <priority 0-7>

Command	Parameters
show 802.1p default_priority	{<portlist>}
config scheduling_mechanism	[strict | round_robin]
show scheduling_mechanism	

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

config bandwidth_control

Purpose	Used to configure bandwidth control on a by-port basis.
Syntax	**config bandwidth_control [<portlist> | all] {rx_rate [no_limit | <value 1-1000>] | tx_rate [no_limit | <value 1-1000>]}**
Description	The **config bandwidth_control** command is used to configure bandwidth on a by-port basis.
Parameters	*<portlist>* – Specifies a range of ports to be configured. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3-2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. *all* – Choose this parameter to select all configurable ports. *rx_rate* – Specifies that one of the parameters below (*no_limit* or *<value 1-1000>*) will be applied to the rate at which the above specified ports will be allowed to receive packets ▪ *no_limit* – Specifies that there will be no limit on the rate of packets received by the above specified ports. ▪ *<value 1-1000>* – Specifies the packet limit, in Mbps, that the above ports will be allowed to receive. *tx_rate* – Specifies that one of the parameters below (*no_limit* or *<value 1-1000>*) will be applied to the rate at which the above specified ports will be allowed to transmit packets. ▪ *no_limit* – Specifies that there will be no limit on the rate of packets received by the above specified ports. ▪ *<value 1-1000>* – Specifies the packet limit, in Mbps, that the above ports will be allowed to receive.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure bandwidth control:

```
DGS-3312SR:4#config bandwidth_control 1:1-1:10 tx_rate 10
Command: config bandwidth_control 1:1-1:10 tx_rate 10

Success.

DGS-3312SR:4#
```

show bandwidth_control

Purpose	Used to display the bandwidth control configuration on the switch.
Syntax	**show bandwidth_control {<portlist>}**
Description	The **show bandwidth_control** command displays the current bandwidth control configuration on the switch, on a port-by-port basis.
Parameters	*<portlist>* – Specifies a range of ports to be configured. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3-2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. Using this command without adding a portlist entry will show the bandwidth control for all ports in the switch stack.
Restrictions	None.

Example usage:

To display bandwidth control settings:

```
DGS-3312SR:4#show bandwidth_control  1:1-1:10
Command: show bandwidth_control 1:1-1:10

Bandwidth Control Table

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

DGS-3312SR:4#
```

config 802.1p user_priority

Purpose	Used to map the 802.1p user priority tags of an incoming packet to one of the eight hardware queues available on the switch.
Syntax	**config 802.1p user_priority <priority 0-7> <class_id 0-7>**
Description	The **config 802.1p user_priority** command is used to configure the way the switch will map an incoming packet, based on its 802.1p user priority tag, to one of the eight hardware priority

config 802.1p user_priority

	queues available on the switch. The switch's default is to map the incoming 802.1p priority values to the eight hardware priority queues according to the following chart: 802.1p Switch Hardware Value Priority Queue --------- ---------- 0 2 1 0 2 1 3 3 4 4 5 5 6 6 7 7
Parameters	*<priority 0-7>* – Specifies which of the eight 802.1p priority tags (0 through 7) you want to map to one of the switch's hardware priority queues (*<class_id>*, 0 through 7). *<class_id 0-7>* – Specifies to which of the switch's hardware priority queues the 802.1p priority tags (specified above) will be mapped.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure 802.1 user priority on the switch:

```
DGS-3312SR:4# config 802.1p user_priority 1 3
Command: config 802.1p user_priority 1 3

Success.

DGS-3312SR:4#
```

show 802.1p user_priority

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

Example usage:

To show 802.1p user priority:

```
DGS-3312SR: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-7>

DGS-3312SR:4#
```

config 802.1p default_priority

Purpose	Used to specify default priority settings on the switch. Untagged packets that are received by the switch will be assigned a priority tag in its priority field using this command.
Syntax	**config 802.1p default_priority [<portlist> | all] <priority 0-7>**
Description	The **config 802.1p default_priority** command allows you to specify the 802.1p priority value an untagged, incoming packet will be assigned before being forwarded to its destination.
Parameters	*<portlist>* – Specifies a range of ports to be configured. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3-2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. *all* – Specifies that the **config 802.1p default_priority** command will be applied to all ports on the switch. *<priority 0-7>* – Specifies the 802.1p priority tag that an untagged, incoming packet will be given before being forwarded to its destination.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure 802.1p default priority on the switch:

```
DGS-3312SR:4#config 802.1p default_priority all 5
Command: config 802.1p default_priority all 5

Success.

DGS-3312SR:4#
```

show 802.1p default_priority

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

Example usage:

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

```
DGS-3312SR:4# show 802.1p default_priority
Command: show 802.1p default_priority

Port    Priority
------- -----------
15:1      1
15:2      1
15:3      1
15:4      1
15:5      1
15:6      1
15:7      1
15:8      1
15:9      1
15:10     1
15:11     1
15:12     1
2:1       0
2:2       0
2:3       0
2:4       0
2:5       0
2:6       0
2:7       0
2:8       0
2:9       0
2:10      0
2:11      0
2:12      0

DGS-3312SR:4#
```

config scheduling_mechanism	
Purpose	Used to configure the scheduling mechanism for the QoS function
Syntax	**config scheduling mechanism [strict | round_robin]**
Description	The **config scheduling_mechanism** command allows the user to select between a *round_robin* and a *strict* mechanism for emptying the priority queues of the QoS function. The switch contains 9 hardware priority queues, one of which is internal and unoperational. Incoming packets must be mapped to one of these eight hardware priority queues. This command is used to specify the rotation by which these eight hardware priority queues are emptied. The switch's default is to empty the eight priority queues in order – from the highest priority queue (queue 7) to the lowest priority queue (queue 0). Each queue will transmit all of the packets in its buffer before allowing the next lower priority queue to transmit its packets. When the lowest priority queue has finished transmitting all of its packets, the highest hardware priority queue can again transmit any packets it may have received.
Parameters	*strict* – Entering the *strict* parameter indicates that the highest queue is the first to be processed. That is, the highest queue should finish emptying before the others begin. *round_robin*– Entering the *round_robin* parameter indicates that the priority queues will empty packets in a round-robin order. That is to say that they will be emptied in an even distribution.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure the traffic scheduling mechanism for each COS queue:

```
DGS-3312SR:4#config scheduling_mechanism strict
Command: config scheduling_mechanism strict

Success.

DGS-3312SR: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-3312SR: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-3312SR: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.

NOTE: As a stand-alone switch or as a master switch in a switch stack, the switch number will be referred to as 15 for all configurations, graphs and tables.

NOTE: Port mirroring can only be used for regular ports on the master DGS-3312SR switch. No port mirroring can be done between slave switches in a stacking configuration, and the master switch.

config mirror port

Purpose	Used to configure a mirror port – source port pair on the switch.
Syntax	**config mirror port <port> add source ports <portlist> [rx | tx | both]**
Description	This command allows a range of ports to have all of their traffic also sent to a designated port, where a network sniffer or other device can monitor the network traffic. In addition, you can specify that only traffic received by or sent by one or both is mirrored to the Target port.
Parameters	*port <port>* – This specifies the Target port (the port where mirrored packets will be sent). The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3-2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. *add source ports* – The port or ports being mirrored. This cannot include the Target port. ▪ *<portlist>* – This specifies a range of ports that will be

config mirror port	
	mirrored. That is, the range of ports in which all traffic will be copied and sent to the Target port. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 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 in the port list. *tx* – Allows the mirroring of only packets sent to (flowing out of) the port or ports in the port list. *both* – Mirrors all the packets received or sent by the port or ports in the port list.
Restrictions	The Target port cannot be listed as a source port. Target or mirrored ports cannot be members of a trunking (link aggregation) group. Only administrator-level users can issue this command.

Example usage:

To add the mirroring ports:

```
DGS-3312SR:4# config mirror port 1:5 add source ports 1:1-1:5 both
Command: config mirror port 1:5 add source ports 1:1-1:5 both

Success.

DGS-3312SR:4#
```

config mirror delete	
Purpose	Used to delete a port mirroring configuration.
Syntax	**config mirror port <port> delete source port <portlist> [rx | tx | both]**
Description	This command is used to delete a previously entered port mirroring configuration.
Parameters	*port* <*port*> –This specifies the Target port (the port where mirrored packets will be sent). The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3-2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. *delete source port* – Adding this parameter will delete source ports according to ports entered using the *<portlist>.* ▪ *<portlist>* – This specifies a range of ports that will be

config mirror delete	
	mirrored. That is, the range of ports in which all traffic will be copied and sent to the Target port. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 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 in the port list. *tx* – Allows the mirroring of only packets sent to (flowing out of) the port or ports in the port list. *both* – Mirrors all the packets received or sent by the port or ports in the port list.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To delete the mirroring ports:

```
DGS-3312SR:4#config mirror port 1:5 delete source port 1:1-1:5 both
Command: config mirror 1:5 delete source 1:1-1:5 both

Success.

DGS-3312SR: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	Only administrator-level users can issue this command.

Example usage:

To enable mirroring configurations:

```
DGS-3312SR:4#enable mirror
Command: enable mirror

Success.

DGS-3312SR:4#
```

disable mirror	
Purpose	Used to disable a previously entered port mirroring configuration.
Syntax	**disable mirror**
Description	This command, combined with the **enable mirror** command above, allows you to enter a port mirroring configuration into the 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-3312SR:4#disable mirror
Command: disable mirror

Success.

DGS-3312SR:4#
```

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

Example usage:

To display mirroring configuration:

```
DGS-3312SR:4#show mirror
Command: show mirror

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

DGS-3312SR: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 32> {tag <vlanid 1-4094> | advertisement}
delete vlan	<vlan_name 32>
config vlan	<vlan_name 32> {[add [tagged | untagged | forbidden] | delete] <portlist> | advertisement [enable | disable]}
config gvrp	[<portlist> | all] {state [enable | disable] | ingress_checking [enable | disable] | acceptable_frame [tagged_only | admit_all] | pvid <vlanid 1-4094>}
enable gvrp	
disable gvrp	
show vlan	<vlan_name 32>
show gvrp	<portlist>

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

NOTE: As a stand-alone switch or as a master switch in a switch stack, the switch number will be referred to as 15 for all configurations, graphs and tables.

create vlan	
Purpose	Used to create a VLAN on the switch.
Syntax	**create vlan <vlan_name 32> {tag <vlanid 1-4094> | advertisement}**
Description	This command allows you to create a VLAN on the switch.
Parameters	*<vlan_name 32>* – The name of the VLAN to be created. *<vlanid 1-4094>* – The VLAN ID of the VLAN to be created. Allowed values = 1-4094 *advertisement* – Specifies that the VLAN is able to join GVRP. If this parameter is not set, the VLAN 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 will be a port-based VLAN. Only administrator-level users can issue this command.

Example usage:

To create a VLAN v1, tag 2:

```
DGS-3312SR:4#create vlan v1 tag 2
Command: create vlan v1 tag 2

Success.

DGS-3312SR:4#
```

delete vlan

Purpose	Used to delete a previously configured VLAN on the switch.
Syntax	**delete vlan <vlan_name 32>**
Description	This command will delete a previously configured VLAN on the switch.
Parameters	*<vlan_name 32>* – The VLAN name of the VLAN you want to delete.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To remove the vlan "v1":

```
DGS-3312SR:4#delete vlan v1
Command: delete vlan v1

Success.

DGS-3312SR:4#
```

config vlan

Purpose	Used to add additional ports to a previously configured VLAN.
Syntax	**config vlan <vlan_name 32> { [add [tagged | untagged | forbidden] | delete] <portlist> | advertisement [enable | disable]}**
Description	This command allows you to add ports to the port list of a previously configured VLAN. You can specify the additional ports as tagging, untagging, or forbidden. The default is to assign the ports as untagging.
Parameters	*<vlan_name 32>* – The name of the VLAN to be configured. *add* – Used to add ports to the specified VLAN, in conjunction with the *portlist* parameter. *tagged* – Specifies that the ports are to be VLAN tagged. untagged – Specifies the ports as untagged.

config vlan	
	forbidden – Specifies the ports as forbidden ports. *delete* – Used to delete ports from the specified VLAN, in conjunction with the *portlist* parameter. <*portlist*> – A range of ports to add to the VLAN. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3-2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. *advertisement [enable* | *disable]* – Enables or disables GVRP on the specified VLAN.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To add 4 through 8 of module 2 as tagged ports to the VLAN v1:

```
DGS-3312SR:4#config vlan v1 add tagged 2:4-2:8
Command: config vlan v1 add tagged 2:4-2:8

Success.

DGS-3312SR:4#
```

config gvrp	
Purpose	Used to configure GVRP on the switch.
Syntax	**config gvrp [<portlist> | all] {state [enable | disable] | ingress_checking [enable | disable] | acceptable_frame [tagged_only | admit_all] | pvid <vlanid 1-4094>}**
Description	This command is used to configure the Group VLAN Registration Protocol on the switch. You can configure ingress checking, the sending and receiving of GVRP information, and the Port VLAN ID (PVID).
Parameters	<*portlist*> – A range of ports for which you want ingress checking. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3-2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. *all* – Specifies all of the ports on the switch.

config gvrp	
	state [enable | *disable]* – Enables or disables GVRP for the ports specified in the port list. *ingress_checking [enable* | *disable]* – Enables or disables ingress checking for the specified port list. *acceptable_frame [tagged_only* | *admit_all]* – This parameter states the frame type that will be accepted by the switch for this function. *tagged_only* implies that only VLAN tagged frames will be accepted, while *admit_all* implies tagged and untagged frames will be accepted by the switch. *pvid <vlanid 1-4094>*– Specifies the default VLAN associated with the port.
Restrictions	Only administrator-level users can issue this command.

Example usage:

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

```
DGS-3312SR:4#config gvrp 1:1-1:4 state enable ingress_checking
enable acceptable_frame tagged_only pvid 2

Command: config gvrp 1:1-1:4 state enable ingress_checking enable
acceptable_frame tagged_only pvid 2


Success.


DGS-3312SR: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 on the switch, without changing the GVRP configuration 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-3312SR:4#enable gvrp
Command: enable gvrp

Success.

DGS-3312SR:4#
```

disable gvrp

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

Example usage:

To disable the Generic VLAN Registration Protocol (GVRP):

```
DGS-3312SR:4#disable gvrp
Command: disable gvrp

Success.

DGS-3312SR:4#
```

show vlan

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

Example usage:

To display the switch's current VLAN settings:

```
DGS-3312SR:4#show vlan
Command: show vlan

VID              : 1              VLAN Name       : default
VLAN TYPE        : static         Advertisement   : Enabled
Member ports     : 1:1-1:11,2:1-2:11
Static ports     : 1:1-1:11,2:1-2:11
Untagged ports   : 1:1-1:11,2:1-2:11
Forbidden ports  :

VID              : 2              VLAN Name       : v1
VLAN TYPE        : static         Advertisement   : Disabled
Member ports     : 1:12,2:12
Static ports     : 1:12,2:12
Untagged ports   :
Forbidden ports  :

Total Entries : 2


DGS-3312SR: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 GVRP status for a port list on the switch
Parameters	*<portlist>* – Specifies a range of ports for which the GVRP status is to be displayed. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3-2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order.
Restrictions	None.

Example usage:

To display GVRP port status:

```
DGS-3312SR:4#show gvrp
Command: show gvrp

Global GVRP : Disabled

Port   PVID   GVRP        Ingress Checking  Acceptable Frame Type
------ ----   --------    ----------------  --------------------------
1:1    1      Disabled    Enabled           All Frames
1:2    1      Disabled    Enabled           All Frames
1:3    1      Disabled    Enabled           All Frames
1:4    1      Disabled    Enabled           All Frames
1:5    1      Disabled    Enabled           All Frames
1:6    1      Disabled    Enabled           All Frames
1:7    1      Disabled    Enabled           All Frames
1:8    1      Disabled    Enabled           All Frames
1:9    1      Disabled    Enabled           All Frames
1:10   1      Disabled    Enabled           All Frames
1:11   1      Disabled    Enabled           All Frames
1:12   1      Disabled    Enabled           All Frames
2:1    1      Disabled    Enabled           All Frames
2:2    1      Disabled    Enabled           All Frames
2:3    1      Disabled    Enabled           All Frames
2:4    1      Disabled    Enabled           All Frames
2:5    1      Disabled    Enabled           All Frames
2:6    1      Disabled    Enabled           All Frames
2:7    1      Disabled    Enabled           All Frames
2:8    1      Disabled    Enabled           All Frames
2:9    1      Disabled    Enabled           All Frames
2:10   1      Disabled    Enabled           All Frames
2:11   1      Disabled    Enabled           All Frames
2:12   1      Disabled    Enabled           All Frames

Total Entries : 24

DGS-3312SR: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 1-6> {type [lacp | static]}
delete link_aggregation	group_id <value 1-6>
config link_aggregation	group_id <value 1-6> {master_port <port> | ports <portlist> state [enable | disable]}
config link_aggregation algorithm	[mac_source | mac_destination | mac_source_dest | ip_source | ip_destination | ip_source_dest]
show link_aggregation	{group_id <value 1-6> | algorithm}
config lacp_port	<portlist> mode [active | passive]
show lacp_port	{<portlist>}

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

NOTE: As a stand-alone switch or as a master switch in a switch stack, the switch number will be referred to as 15 for all configurations, graphs and tables.

create link_aggregation

Purpose	Used to create a link aggregation group on the switch.
Syntax	**create link_aggregation group_id <value 1-6> {type [lacp | static]}**
Description	This command will create a link aggregation group with a unique identifier.
Parameters	*<value 1-6>* – Specifies the group ID. The switch allows up to 6 link aggregation groups to be configured. The group number identifies each of the groups. *type* – Specify the type of link aggregation used for the group. If the type is not specified the default type is static. ▪ *lacp* – This designates the port group as LACP compliant. LACP allows dynamic adjustment to the aggregated port group. LACP compliant ports may be further configured (see config lacp_ports). LACP compliant must be connected to LACP compliant devices. ▪ *static* – This designates the aggregated port group as static. Static port groups can not be changed as easily as LACP compliant port groups since both linked devices must be manually configured if the configuration of the trunked group is changed. If static link aggregation is used, be sure that both ends of the connection are properly configured and that all ports have the same speed/duplex settings.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To create a link aggregation group:

```
DGS-3312SR:4#create link_aggregation group_id 1
Command: create link_aggregation group_id 1

Success.

DGS-3312SR:4#
```

delete link_aggregation group_id

Purpose	Used to delete a previously configured link aggregation group.
Syntax	**delete link_aggregation group_id <value 1-6>**
Description	This command is used to delete a previously configured link aggregation group.
Parameters	*<value 1-6>* – Specifies the group ID. The switch allows up to 6 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-3312SR:4#delete link_aggregation group_id 6
Command: delete link_aggregation group_id 6

Success.

DGS-3312SR:4#
```

config link_aggregation

Purpose	Used to configure a previously created link aggregation group.
Syntax	**config link_aggregation group_id <value 1-6> {master_port <port> | ports <portlist> | state [enable | disable]**
Description	This command allows you to configure a link aggregation group that was created with the **create link_aggregation** command above. The DGS-3312SR supports link aggregation cross box which specifies that link aggregation groups may be spread over multiple switches in the switching stack.
Parameters	*group _id <value 1-6>* – Specifies the group ID. The switch allows up to 6 link aggregation groups to be configured. The group number identifies each of the groups. *master_port<port>* – Master port ID. Specifies which port (by port number) of the link aggregation group will be the master port. All of the ports in a link aggregation group will share the port configuration

config link_aggregation	
	with the master port. *ports <portlist>* – Specifies a range of ports that will belong to the link aggregation group. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3-2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. *state [enable* | *disable]* – Allows you to enable or disable the specified link aggregation group.
Restrictions	Only administrator-level users can issue this command. Link aggregation groups may not overlap. Link aggregation members cannot be configured as a mirrored port or target port of a mirroring configuration.

Example usage:

To define a load-sharing group of ports, group-id 1, master port 5 of module 1 with group members ports 5-7 plus port 9:

```
DGS-3312SR:4#config link_aggregation group_id 1 master_port 1:5 ports 1:5-1:7, 1:9
Command: config link_aggregation group_id 1 master_port 1:5 ports 1:5-1:7, 1:9

Success.

DGS-3312SR:4#
```

config link_aggregation algorithm	
Purpose	Used to configure the link aggregation algorithm.
Syntax	**config link_aggregation algorithm [mac_source | mac_destination | mac_source_dest | ip_source | ip_destination | ip_source_dest]**
Description	This command configures to part of the packet examined by the switch when selecting the egress port for transmitting load-sharing data. This feature is only available using the address-based load-sharing algorithm.
Parameters	*mac_source* – Indicates that the switch should examine the MAC source address. *mac_destination* – Indicates that the switch should examine the MAC destination address. *mac_source_dest* – Indicates that the switch should examine the MAC source and destination addresses *ip_source* – Indicates that the switch should examine the IP source address. *ip_destination* – Indicates that the switch should examine the IP destination address. *ip_source_dest* – Indicates that the switch should examine the IP source address and the destination address.

config link_aggregation algorithm	
Restrictions	Only administrator-level users can issue this command.

Example usage:

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

```
DGS-3312SR:4#config link_aggregation algorithm mac_source_dest
Command: config link_aggregation algorithm mac_source_dest

Success.

DGS-3312SR:4#
```

show link_aggregation	
Purpose	Used to display the current link aggregation configuration on the switch.
Syntax	**show link_aggregation {group_id <value 1-6> | algorithm}**
Description	This command will display the current link aggregation configuration of the switch.
Parameters	*group_id <value 1-6>* – Specifies the group ID. The switch allows up to 6 link aggregation groups to be configured. The group number identifies each of the groups. *algorithm* – Allows you to specify the display of link aggregation by the algorithm in use by that group.
Restrictions	None.

Example usage:

To display Link Aggregation configuration:

```
DGS-3312SR:4#show link_aggregation
Command: show link_aggregation

Link Aggregation Algorithm = MAC-source-dest
Group ID          : 1
Master Port       : 2:10
Member Port       : 1:5-1:10,2:10
Active Port:
Status            : Disabled
Flooding Port     : 1:5

DGS-3312SR:4
```

config lacp_ports

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

Example usage:

To configure LACP port mode settings:

```
DGS-3312SR:4#config lacp_port 1:1-1:12 mode active
Command: config lacp_port 1:1-1:12 mode active

Success.

DGS-3312SR:4#
```

show lacp_port	
Purpose	Used to display current LACP port mode settings.
Syntax	**show lacp_port {<portlist>}**
Description	This command will display the LACP mode settings as they are currently configured.
Parameters	*<portlist>* - Specifies a range of ports that will be viewed. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3-2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To display LACP port mode settings:

```
DGS-3312SR:4#show lacp_port 1:1-1:11
Command: show lacp_port 1:1-1:11

Port    Activity
------   --------
1:1     Active
1:2     Active
1:3     Active
1:4     Active
1:5     Active
1:6     Active
1:7     Active
1:8     Active
1:9     Active
1:10    Active
1:11    Active

DGS-3312SR:4#
```

17

IP COMMANDS (INCLUDING IP MULTINETTING)

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

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

Application Limitation: A multicast router cannot be connected to IP interfaces that are utilizing the IP Multinetting function.

NOTE: Only the primary IP interface will support the BOOTP relay agent.

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

The amount of broadcast data, such as RIP update packets and PIM hello packets, will be increased.

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

Command	Parameters
enable ipif	{<ipif_name 12> | all}
create ipif	<ipif_name12> <network_address> <vlan_name 32> {secondary | state [enable | disable]}
config ipif	<ipif_name12> [{ipaddress <network_address> | {vlan <vlan_name 32> | state [enable | disable]} | bootp | dhcp]
show ipif	<ipif_name 12>
delete ipif	<ipif_name 12> | all
disable ipif	<ipif_name 12> | all

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

NOTE: As a stand-alone switch or as a master switch in a switch stack, the switch number will be referred to as 15 for all configurations, graphs and tables.

enable ipif	
Purpose	Used to enable an IP interface on the switch.
Syntax	**enable ipif {<ipif_name 12> | all}**
Description	This command will enable the IP interface function on the switch.
Parameters	*<ipif_name 12>* – The name for the IP interface to be created. This name cannot exceed 12 characters. *all* – Entering this parameter will enable the IP interfaces currently configured with this command.
Restrictions	None.

Example usage:

To enable the ipif function on the switch:

```
DGS-3312SR:4#enable ipif s2
Command: enable ipif s2

Success.

DGS-3312SR:4#
```

create ipif	
Purpose	Used to create an IP interface on the switch.
Syntax	**create ipif <ipif_name12> <network_address> <vlan_name 32> {state [enable | disable]} {secondary | {state [enable | disable]}**
Description	This command will create an IP interface.
Parameters	*<ipif_name 12>* – The name for the IP interface to be created. The user may enter an alphanumeric string of up to 12 characters to define the IP interface. *<network_address>* – IP address and netmask of the IP interface to be created. The address and mask information can be specified using the traditional format (for example, 10.1.2.3/255.0.0.0 or in CIDR format, 10.1.2.3/8). *<vlan_name 32>* – The name of the VLAN that will be associated with the above IP interface. *secondary* – Enter this parameter if this configured IP interface is to be a *secondary* IP interface of the VLAN previously specified. *secondary* interfaces can only be configured if a *primary* interface is first configured. *state [enable | disable]* – Allows you to enable or disable the IP interface.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To create an IP interface on the switch:

```
DGS-3312SR:4# create ipif p1 ipaddress 10.1.1.1 Trinity state enable
Command: create ipif p1 ipaddress 10.1.1.1 Trinity state enable

Success.

DGS-3312SR:4#
```

To create the secondary IP interface, s1 on VLAN Trinity:

```
DGS-3312SR:4#create ipif p1 ipaddress 12.1.1.1 Trinity secondary state enable
Command: create ipif p1 ipaddress 12.1.1.1 Trinity secondary state enable

Success.

DGS-3312SR:4#
```

config ipif

Purpose	Used to configure the System IP interface.
Syntax	**config ipif <ipif_name 12> [{ipaddress <network_address> | {vlan <vlan_name 32> | state [enable | disable]} | bootp | dhcp]**
Description	This command is used to configure the System IP interface on the switch.
Parameters	*<ipif_name 12>* – The name for the IP interface previously created, that is to be configured. *ipaddress <network_address>* – IP address and netmask of the IP interface to be configured. 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, 10.1.2.3/8). *vlan <vlan_name 32>* – The name of the VLAN corresponding to the System IP interface. *state [enable | disable]* – Allows you to enable or disable the IP interface. *bootp* – Allows the selection of the BOOTP protocol for the assignment of an IP address to the switch's System IP interface. *dhcp* – Allows the selection of the DHCP protocol for the assignment of an IP address to the switch's System IP interface.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure the IP interface System:

```
DGS-3312SR:4#config ipif System ipaddress 10.48.74.122/8
Command: config ipif System ipaddress 10.48.74.122/8

Success.

DGS-3312SR:4#
```

show ipif

Purpose	Used to display the configuration of an IP interface on the switch.
Syntax	**show ipif <ipif_name 12>**
Description	This command will display the configuration of an IP interface on the switch.
Parameters	*<ipif_name 12>* – The name created for the IP interface to view.
Restrictions	None.

Example usage:

To display IP interface settings.

```
DGS-3312SR:4#show ipif System
Command: show ipif System

 IP Interface Settings

 Interface Name     : System
 IP Address         : 10.48.74.122    (MANUAL)
 Subnet Mask        : 255.0.0.0
 VLAN Name          : default
 Admin. State       : Disabled
 Link Status        : Link UP
 Member Ports       : 1:1-1:12

DGS-3312SR:4#
```

delete ipif

Purpose	Used to delete the configuration of an IP interface on the switch.
Syntax	**delete ipif <ipif_name 12 | all>**
Description	This command will delete the configuration of an IP interface on the switch.
Parameters	*<ipif_name>* – The name created for the IP interface. *all* – Entering this parameter will delete all the IP interfaces currently configured on the switch.
Restrictions	None.

Example usage:

To delete the IP interface named s2:

```
DGS-3312SR:4#delete ipif s2
Command: delete ipif s2

Success.

DGS-3312SR:4#
```

disable ipif

Purpose	Used to disable the configuration of an IP interface on the switch.
Syntax	**disable ipif <ipif_name 12> | all**
Description	This command will disable the configuration of an IP interface on the switch.
Parameters	*<ipif_name 12>* – The name created for the IP interface. *all* – Entering this parameter will delete all the IP interfaces currently configured on the switch.
Restrictions	None.

Example usage:

To disable the IP interface named "s2":

```
DGS-3312SR:4#disable ipif s2
Command: disable ipif s2

Success.

DGS-3312SR:4#
```

18

IGMP COMMANDS

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

Command	Parameters
config igmp	[ipif <ipif_name 12> | all] {version <value 1-2> | query_interval <sec 1-65535> max_response_time <sec 1-25> | robustness_variable <value 1-255> | last_member_query_interval <sec 1-25> | state [enable | disable]
show igmp	{ipif <ipif_name 12>}
show igmp group	{group <group>} {ipif <ipif_name 12>}

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

config igmp

Purpose	Used to configure IGMP on the switch.
Syntax	**config igmp [ipif <ipif_name 12> | all] {version <value 1-2> | {query_interval <sec 1-65535> | max_response_time <sec 1-25> | robustness_variable <value 1-255> | last_member_query_interval <sec 1-25> | state [enable | disable]**
Description	This command allows you to configure IGMP on the switch.
Parameters	*<ipif_name 12>* – The name of the IP interface for which to configure IGMP. *all* – Specifies all the IP interfaces on the switch. *version <value 1-2>* – The IGMP version number. *query_interval <sec 1-25>* – The time in seconds between general query transmissions, in seconds. *max_response_time <sec 1-25>* – Enter the maximum time in seconds that the switch will wait for reports from members. *robustness_variable <value 1-255>* – This value states the permitted packet loss that guarantees IGMP. *last_member_query_interval <value 1-25>* – The Max Response Time inserted into Group-Specific Queries sent in response to Leave Group messages, and is also the amount of time between Group-Specific Query messages. The default is 1 second *state [enable | disable]* – Enables or disables IGMP for the specified IP interface.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To configure the IGMP for the IP interface System.

```
DGS-3312SR:4#config igmp all version 1 state enable
Command: config igmp all version 1 state enable

Success.

DGS-3312SR:4#
```

show igmp

Purpose	Used to display the IGMP configuration for the switch of for a specified IP interface.
Syntax	**show igmp {ipif <ipif_name 12>}**
Description	This command will display the IGMP configuration for the switch if no IP interface name is specified. If an IP interface name is specified, the command will display the IGMP configuration for that IP interface.
Parameters	*<ipif_name 12>* – The name of the IP interface for which the IGMP configuration will be displayed.
Restrictions	None.

Example Usage:

To display IGMP configurations:

```
DGS-3312SR:4#show igmp
Command: show igmp

IGMP Interface Configurations
QI : Query Interval                  MRT  : Maximum Response Time
RV : Robustness Value                LMQI : Last Member Query Interval
Interface   IP Address/Netmask  Version  QI    MRT  RV  LMQI  State
----------- ------------------  -------  ----- ---  --- ------ --------
System      10.53.13.12/8       1        25    2    2   2      Enabled

Total Entries: 1

DGS-3312SR:4#
```

show igmp group

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

Example Usage:

To display IGMP group table:

```
DGS-3312SR:4#show igmp group
Command: show igmp group

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

Total Entries: 5

DGS-3312SR:4#
```

19

IGMP SNOOPING COMMANDS

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

Command	Parameters
config igmp_snooping	[<vlan_name 32> | all] {host_timeout <sec 1-16711450> | router_timeout <sec 1-16711450> | leave_timer <sec 0-6711450> state [enable | disable]
config igmp_snooping querier	[<vlan_name 32> | all] {query_interval <sec 1-65535> | max_response_time <sec 1-25> | robustness_variable <value 1-255> | last_member_query_interval <sec 1-25> | state [enable | disable]
enable igmp snooping	{forward_mcrouter_only}
disable igmp snooping	
config router_ports	{<vlan_name 32>} [add | delete] <portlist>
show router_ports	{vlan <vlan_name 32>} {static | dynamic}
show igmp_snooping	{vlan<vlan_name 32>}
show igmp_snooping group	{vlan <vlan_name 32>}
show igmp_snooping forwarding	{vlan <vlan_name 32>}

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

NOTE: As a stand-alone switch or as a master switch in a switch stack, the switch number will be referred to as 15 for all configurations, graphs and tables.

config igmp_snooping

Purpose	Used to configure IGMP snooping on the switch.
Syntax	**config igmp_snooping [<vlan_name 32> | all] {host_timeout <sec 1-16711450> | router_timeout <sec 1-16711450> | leave_timer <sec 0-16711450> | state [enable | disable]}**
Description	This command allows you to configure IGMP snooping on the switch.
Parameters	*<vlan_name 32>* – The name of the VLAN for which IGMP snooping is to be configured. *all* – Selecting this parameter will configure IGMP snooping for all VLANs on the switch. *host_timeout <sec 1-16711450>* – Specifies the maximum amount of time a host can be a member of a multicast group

config igmp_snooping	
	without the switch receiving a host membership report. The default is 260 seconds. *router_timeout <sec 1-16711450>* – Specifies the maximum amount of time a route can be a member of a multicast group without the switch receiving a host membership report. The default is 260 seconds. *leave_timer <sec 0-16711450>* – Leave timer. The default is 2 seconds. *state [enable | disable]* – Allows you to enable or disable IGMP snooping for the specified VLAN.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure the igmp snooping:

```
DGS-3312SR:4#config igmp_snooping default host_timeout 250 state enable

Command: config igmp_snooping default host_timeout 250 state enable


Success.


DGS-3312SR:4#
```

config igmp_snooping querier	
Purpose	This command configures IGMP snooping querier.
Syntax	**config igmp_snooping querier [<vlan_name 32> | all] {query_interval <sec 1-65535> | max_response_time <sec 1-25> | robustness_variable <value 1-255> | last_member_query_interval <sec 1-25> | state [enable | disable]**
Description	Used to configure the time in seconds between general query transmissions, the maximum time in seconds to wait for reports from members and the permitted packet loss that guarantees IGMP snooping.
Parameters	*<vlan_name 32>* – The name of the VLAN for which IGMP snooping querier is to be configured. *all* – Selecting this parameter will configure the IGMP snooping querier for all VLANs on the switch. *query_interval <sec 1-65535>* – Specifies the amount of time in seconds between general query transmissions. The default setting is 125 seconds. *max_response_time <sec 1-25>* – Specifies the maximum time in seconds to wait for reports from members. The default setting is 10 seconds.

config igmp_snooping querier	
	robustness_variable <*value 1-255*> – Provides fine-tuning to allow for expected packet loss on a subnet. The value of the robustness variable is used in calculating the following IGMP message intervals: • Group member interval—Amount of time that must pass before a multicast router decides there are no more members of a group on a network. This interval is calculated as follows: (robustness variable x query interval) + (1 x query response interval). • Other querier present interval—Amount of time that must pass before a multicast router decides that there is no longer another multicast router that is the querier. This interval is calculated as follows: (robustness variable x query interval) + (0.5 x query response interval). • Last member query count—Number of group-specific queries sent before the router assumes there are no local members of a group. The default number is the value of the robustness variable. • By default, the robustness variable is set to 2. You might want to increase this value if you expect a subnet to be lossy. *last_member_query_interval* <*sec 1-25*> – The maximum amount of time between group-specific query messages, including those sent in response to leave-group messages. You might lower this interval to reduce the amount of time it takes a router to detect the loss of the last member of a group. *state [enable*	*disable]* – Allows the switch to be specified as an IGMP Querier or Non-querier.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure the igmp snooping:

```
DGS-3312SR:4#config igmp_snooping querier default query_interval 125
state enable

Command: config igmp_snooping querier default query_interval 125
state enable


Success.


DGS-3312SR:4#
```

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

Example usage:

To enable IGMP snooping on the switch:

```
DGS-3312SR:4#enable igmp_snooping
Command: enable igmp_snooping

Success.

DGS-3312SR:4#
```

disable igmp_snooping	
Purpose	Used to enable IGMP snooping on the switch.
Syntax	**disable igmp_snooping**
Description	This command disables IGMP snooping on the switch. IGMP snooping can be disabled only if IP multicast routing is not being used. Disabling IGMP snooping allows all IGMP and IP multicast traffic to flood within a given IP interface.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To disable IGMP snooping on the switch:

```
DGS-3312SR:4#disable igmp_snooping
Command: disable igmp_snooping

Success.

DGS-3312SR:4#
```

config router_ports

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

Example usage:

To set up static router ports:

```
DGS-3312SR:4#config router_ports default add 2:1-2:10
Command: config router_ports default add 2:1-2:10

Success.

DGS-3312SR:4#
```

show router_ports

Purpose	Used to display the currently configured router ports on the switch.
Syntax	**show router_ports {vlan <vlan_name 32>} {static | dynamic}**
Description	This command will display the router ports currently configured on the switch.
Parameters	*<vlan_name 32>* – The name of the VLAN on which the router port resides. *static* – Displays router ports that have been statically configured. *dynamic* – Displays router ports that have been dynamically configured.
Restrictions	None.

Example usage:

To display the router ports.

```
DGS-3312SR:4#show router_ports
Command: show router_ports

VLAN Name            : default
Static router port   : 2:1-2:10
Dynamic router port :

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

Total Entries: 2

DGS-3312SR:4#
```

show igmp_snooping

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

Example usage:

To show igmp snooping:

```
DGS-3312SR:4#show igmp_snooping
Command: show igmp_snooping

IGMP Snooping Global State    : Disabled
Multicast router Only         : Disabled

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

VLAN  Name                    : vlan2
Query Interval                : 125
Max Response Time             : 10
Robustness Value              : 2
```

```
Last Member Query Interval      : 1
Host Timeout                    : 260
Route Timeout                   : 260
Leave Timer                     : 2
Querier State                   : Disabled
Querier Router Behavior         : Non-Querier
State                           : Disabled

Total Entries: 2


DGS-3312SR:4#
```

show igmp_snooping group

Purpose	Used to display the current IGMP snooping group configuration on the switch.
Syntax	**show igmp_snooping group {vlan <vlan_name 32>}**
Description	This command will display the current IGMP snooping group configuration on the switch.
Parameters	*vlan <vlan_name 32>* – 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-3312SR:4#show igmp_snooping group
Command: show igmp_snooping group

 VLAN Name      : default
 Multicast group: 224.0.0.2
 MAC address    : 01-00-5E-00-00-02
 Reports        : 1
 Port Member    : 1:2,2:7

 VLAN Name      : default
 Multicast group: 224.0.0.9
 MAC address    : 01-00-5E-00-00-09
 Reports        : 1
 Port Member    : 1:5,2:4

 VLAN Name      : default
 Multicast group: 234.5.6.7
 MAC address    : 01-00-5E-05-06-07
 Reports        : 1
 Port Member    : 1:6,2:9

 VLAN Name      : default
 Multicast group: 236.54.63.75
 MAC address    : 01-00-5E-36-3F-4B
 Reports        : 1
 Port Member    : 1:10,2:2
```

```
VLAN Name      : default
Multicast group: 239.255.255.250
MAC address    : 01-00-5E-7F-FF-FA
Reports        : 2
Port Member    : 1:8,2:4

VLAN Name      : default
Multicast group: 239.255.255.254
MAC address    : 01-00-5E-7F-FF-FE
Reports        : 1
Port Member    : 1:5,2:5

Total Entries  : 6


DGS-3312SR:4#
```

show igmp_snooping forwarding

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

Example usage:

To view the IGMP snooping forwarding table for VLAN "Trinity":

```
DGS-3312SR:4#show igmp_snooping forwarding vlan Trinity
Command: show igmp_snooping forwarding vlan Trinity

VLAN Name      : Trinity
Multicast group : 224.0.0.2
MAC address    : 01-00-5E-00-00-02
Port Member    : 1:11

Total Entries: 1

DGS-3312SR:4#
```

20

MAC NOTIFICATION COMMANDS

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

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

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

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

Example Usage:

To enable MAC notification without changing basic configuration:

```
DGS-3312SR:4#enable mac_notification
Command: enable mac_notification

Success.

DGS-3312SR:4#
```

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

Example Usage:

To disable MAC notification without changing basic configuration:

```
DGS-3312SR:4#disable mac_notification
Command: disable mac_notification

Success.

DGS-3312SR:4#
```

config mac_notification

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

Example usage:

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

```
DGS-3312SR:4#config mac_notification interval 1 historysize 500
Command: config mac_notification interval 1 historysize 500

Success.

DGS-3312SR:4#
```

config mac_notification ports

Purpose	Used to configure MAC address notification status settings.
Syntax	**config mac_notification ports [<portlist | all] [enable | disable]**
Description	MAC address notification is used to monitor MAC addresses learned and entered into the FDB.
Parameters	*<portlist>* - Specify a port or range of ports to be configured. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3-2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. *all* – Entering this command will set all ports on the system.

config mac_notification ports

	[enable | *disable]* – These commands will enable or disable MAC address table notification on the switch.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To enable port 7 for MAC address table notification:

```
DGS-3312SR:4#config mac_notification ports 7 enable
Command: config mac_notification ports 7 enable

Success.

DGS-3312SR:4#
```

show mac_notification

Purpose	Used to display the switch's MAC address table notification global settings
Syntax	**show mac_notification**
Description	This command is used to display the switch's MAC address table notification global settings.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To view the switch's MAC address table notification global settings:

```
DGS-3312SR:4#show mac_notification
Command: show mac_notification

Global Mac Notification Settings

State        : Enabled
Interval     : 1
History Size : 1

DGS-3312SR:4#
```

show mac_notification ports

show mac_notification ports	
Purpose	Used to display the switch's MAC address table notification status settings
Syntax	**show mac_notification ports <portlist>**
Description	This command is used to display the switch's MAC address table notification status settings.
Parameters	*<portlist>* - Specify a port or group of ports to be viewed. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3-2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. Entering this command without the parameter will display the MAC notification table for all ports.
Restrictions	None

Example usage:

To display all port's MAC address table notification status settings:

```
DGS-3312SR:4#show mac_notification ports
Command: show mac_notification ports

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

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

21

ACCESS AUTHENTICATION CONTROL COMMANDS

The TACACS / XTACACS / TACACS+ / RADIUS commands let you secure access to the switch using the TACACS / XTACACS / TACACS+ / RADIUS protocols. When a user logs in to the switch or tries to access the administrator level privilege, he or she is prompted for a password. If TACACS / XTACACS / TACACS+ / RADIUS authentication is enabled on the switch, it will contact a TACACS / XTACACS / TACACS+ / RADIUS server to verify the user. If the user is verified, he or she is granted access to the switch.

There are currently three versions of the TACACS security protocol, each a separate entity. The switch's software supports the following versions of TACACS:

- TACACS (Terminal Access Controller Access Control System) —Provides password checking and authentication, and notification of user actions for security purposes utilizing via one or more centralized TACACS servers, utilizing the UDP protocol for packet transmission.

- Extended TACACS (XTACACS) — An extension of the TACACS protocol with the ability to provide more types of authentication requests and more types of response codes than TACACS. This protocol also uses UDP to transmit packets.

- TACACS+ (Terminal Access Controller Access Control System plus) — Provides detailed access control for authentication for network devices. TACACS+ is facilitated through Authentication commands via one or more centralized servers. The TACACS+ protocol encrypts all traffic between the switch and the TACACS+ daemon, using the TCP protocol to ensure reliable delivery

In order for the TACACS / XTACACS / TACACS+ / RADIUS security function to work properly, a TACACS / XTACACS / TACACS+ / RADIUS server must be configured on a device other than the switch, called a *server host* and it must include usernames and passwords for authentication. When the user is prompted by the switch to enter usernames and passwords for authentication, the switch contacts the TACACS / XTACACS / TACACS+ / RADIUS server to verify, and the server will respond with one of three messages:

A) The server verifies the username and password, and the user is granted normal user privileges on the switch.

B) The server will not accept the username and password and the user is denied access to the switch.

C) The server doesn't respond to the verification query. At this point, the switch receives the timeout from the server and then moves to the next method of verification configured in the method list.

The Switch also supports the RADIUS protocol for authentication using the Access Authentication Control commands. RADIUS or Remote Authentication Dial In User Server also uses a remote server for authentication and can be responsible for receiving user connection requests, authenticating the user and returning all configuration information necessary for the client to deliver service through the user. RADIUS may be facilitated on this Switch using the commands listed in this section.

The switch has four built-in *server groups*, one for each of the TACACS, XTACACS and TACACS+ / RADIUS protocols. These built-in *server groups* are used to authenticate users trying to access the switch. The users will set *server hosts* in a preferable order in the built-in *server group* and when a user tries to gain access to the switch, the switch will ask the first *server host* for authentication. If no authentication is made, the second *server host* in the list will be queried, and so on. The built-in *server group* can only have hosts that are running the specified protocol. For example, the TACACS *server group* can only have TACACS *server hosts*.

The administrator for the switch may set up 6 different authentication techniques per user-defined *method list* (TACACS / XTACACS / TACACS+ / RADIUS / local / none) for authentication. These techniques will be listed in an order preferable, and defined by the user for normal user authentication on the switch, and may contain up to eight authentication techniques. When a user attempts to access the switch, the switch will select the first technique listed for authentication. If the first technique goes through its *server hosts* and no authentication is returned, the switch will then go to the next technique listed in the server group for authentication, until the authentication has been verified or denied, or the list is exhausted.

Please note that user granted access to the switch will be granted normal user privileges on the switch. To gain access to admin level privileges, the user must enter the *enable admin* command and then enter a password, which was previously configured by the administrator of the switch.

NOTE: TACACS, XTACACS and TACACS+ are separate entities and are not compatible. The switch and the server must be configured exactly the same, using the same protocol. (For example, if the switch is set up for TACACS authentication, so must be the host server.)

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

Command	Parameters
enable authen_policy	
disable authen_policy	
show authen_policy	
create authen_login method_list_name	<string 15>
config authen_login	[default | method_list_name <string 15>] method {tacacs | xtacacs | tacacs+ | radius | server_group <string 15> | local | none}
delete authen_login method_list_name	<string 15>
show authen_login	{default | method_list_name <string 15> | all}
create authen_enable method_list_name	<string 15>
config authen_enable	[default | method_list_name <string 15>] method {tacacs | xtacacs | tacacs+ | radius | server_group <string 15> | local_enable | none}
delete authen_enable method_list_name	<string 15>
show authen_enable	[default | method_list_name <string 15> | all]
config authen application	{console | telnet | ssh | http | all] [login | enable] [default | method_list_name <string 15>]
show authen application	
create authen server_group	<string 15>
config authen server_group	[tacacs | xtacacs | tacacs+ | radius | <string 15>] [add | delete] server_host <ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius]
delete authen server_group	<string 15>
show authen server_group	{<string 15>}
create authen server_host	<ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius] {port <int 1-65535> | key [<key_string 254> | none] | timeout <int 1-255> | retransmit <int 1-255>}
config authen server_host	<ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius] {port <int 1-65535> | key [<key_string 254> | none] | timeout <int 1-255> | retransmit <int 1-255>}
delete authen server_host	<ipaddr> protocol [tacacs | xtacacs | tacacs+ |

Command	Parameters
	radius]
show authen server_host	
config authen parameter response_timeout	<int 1-255>
config authen parameter attempt	<int 1-255>
show authen parameter	
enable admin	
config admin local_enable	<password 15>

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

enable authen_policy

Purpose	Used to enable system access authentication policy.
Syntax	**enable authen_policy**
Description	This command will enable an administrator-defined authentication policy for users trying to access the switch. When enabled, the device will check the method list and choose a technique for user authentication upon login.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To enable the system access authentication policy:

```
DGS-3312SR:4#enable authen_policy
Command: enable authen_policy

Success.

DGS-3312SR:4#
```

disable authen_policy

Purpose	Used to disable system access authentication policy.
Syntax	**disable authen_policy**
Description	This command will disable the administrator-defined authentication policy for users trying to access the switch. When disabled, the switch will access the local user account database for username and password verification. In addition, the switch will now accept the local enable password as the authentication for normal users attempting to access administrator level privileges.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To disable the system access authentication policy:

```
DGS-3312SR:4#disable authen_policy
Command: disable authen_policy

Success.

DGS-3312SR:4#
```

show authen_policy

Purpose	Used to display the system access authentication policy status on the switch.
Syntax	**show authen_policy**
Description	This command will show the current status of the access authentication policy on the switch
Parameters	None.
Restrictions	None.

Example usage:

To display the system access authentication policy:

```
DGS-3312SR:4#show authen_policy
Command: show authen_policy

Authentication Policy: Enabled

DGS-3312SR:4#
```

create authen_login method_list_name

Purpose	Used to create a user defined method list of authentication methods for users logging on to the switch.
Syntax	**create authen_login method_list_name <string 15>**
Description	This command is used to create a list for authentication techniques for user login. The switch can support up to eight method lists, but one is reserved as a default and cannot be deleted. Multiple method lists must be created and configured separately.
Parameters	*<string 15>* - Enter an alphanumeric string of up to 15 characters to define the given *method list*.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To create the method list “Trinity.”:

```
DGS-3312SR:4#create authen_login method_list_name Trinity
Command: create authen_login method_list_name Trinity

Success.

DGS-3312SR:4#
```

config authen_login

Purpose	Used to configure a user-defined or default *method list* of authentication methods for user login.
Syntax	**config authen_login [default | method_list_name <string 15>] method {tacacs | xtacacs | tacacs+ | radius | server_group <string 15> | local | none}**
Description	This command will configure a user-defined or default *method list* of authentication methods for users logging on to the switch. The sequence of methods implemented in this command will affect the authentication result. For example, if a user enters a sequence of methods like *tacacs – xtacacs – local,* the switch will send an authentication request to the first *tacacs* host in the server group. If no response comes from the server host, the switch will send an authentication request to the second *tacacs* host in the server group and so on, until the list is exhausted. At that point, the switch will restart the same sequence with the following protocol listed, *xtacacs*. If no authentication takes place using the *xtacacs* list, the *local* account database set in the switch is used to authenticate the user. When the local method is used, the privilege level will be dependant on the local account privilege configured on the switch. Successful login using any of these methods will give the user a “user” privilege only. If the user wishes to upgrade his or her status to the administrator level, the user must implement the *enable admin* command, followed by a previously configured password. (*See the **enable admin** part of this section for more detailed information, concerning the **enable admin** command.)*

config authen_login

Parameters

default – The default method list for access authentication, as defined by the user. The user may choose one or a combination of up to four (4) of the following authentication methods:

- *tacacs* – Adding this parameter will require the user to be authenticated using the TACACS protocol from the remote TACACS *server hosts* of the TACACS *server group* list.
- *xtacacs* – Adding this parameter will require the user to be authenticated using the XTACACS protocol from the remote XTACACS *server hosts* of the XTACACS *server group* list.
- *tacacs+* – Adding this parameter will require the user to be authenticated using the TACACS+ protocol from the remote TACACS+ *server hosts* of the TACACS+ *server group* list.
- *radius* – Adding this parameter will require the user to be authenticated using the RADIUS protocol from the remote RADIUS *server hosts* of the RADIUS *server group* list.
- *server_group* <*string 15*> - Adding this parameter will require the user to be authenticated using a user-defined server group previously configured on the switch.
- *local* - Adding this parameter will require the user to be authenticated using the local *user account* database on the switch.
- *none* – Adding this parameter will require no authentication to access the switch.

method_list_name – Enter a previously implemented method list name defined by the user. The user may add one, or a combination of up to four (4) of the following authentication methods to this method list:

- *tacacs* – Adding this parameter will require the user to be authenticated using the TACACS protocol from a remote TACACS server.
- *xtacacs* – Adding this parameter will require the user to be authenticated using the XTACACS protocol from a remote XTACACS server.
- *tacacs+* – Adding this parameter will require the user to be authenticated using the TACACS protocol from a remote TACACS server.
- *radius* – Adding this parameter will require the user to be authenticated using the RADIUS protocol from a remote RADIUS server.
- *server_group* <*string 15*> - Adding this parameter will require the user to be authenticated using a user-defined server group previously configured on the switch.
- *local* - Adding this parameter will require the user to be authenticated using the local *user account* database on the switch.

none – Adding this parameter will require no authentication to access the switch.

config authen_login

NOTE: Entering *none* or *local* as an authentication protocol will override any other authentication that follows it on a method list or on the default method list.

Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure the user defined method list "Trinity" with authentication methods tacacs, xtacacs and local, in that order.

```
DGS-3312SR:4#config authen_login method_list_name Trinity method
tacacs xtacacs local

Command: config authen_login method_list_name Trinity method tacacs
xtacacs local

Success.

DGS-3312SR:4#
```

Example usage:

To configure the default method list with authentication methods xtacacs, tacacs+ and local, in that order:

```
DGS-3312SR:4#config authen_login default method xtacacs tacacs+ local

Command: config authen_login default method xtacacs tacacs+ local

Success.

DGS-3312SR:4#
```

delete authen_login method_list_name

Purpose	Used to delete a previously configured user defined method list of authentication methods for users logging on to the switch.
Syntax	**delete authen_login method_list_name <string 15>**
Description	This command is used to delete a list for authentication methods for user login.
Parameters	<*string 15*> - Enter an alphanumeric string of up to 15 characters to define the given *method list* the user wishes to delete.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To delete the method list name "Trinity":

```
DGS-3312SR:4#delete authen_login method_list_name Trinity
Command: delete authen_login method_list_name Trinity

Success.

DGS-3312SR:4#
```

show authen_login

Purpose	Used to display a previously configured user defined method list of authentication methods for users logging on to the switch.
Syntax	**show authen_login [default | method_list_name <string 15> | all]**
Description	This command is used to show a list of authentication methods for user login. The window will display the following parameters: ▪ Method List Name – The name of a previously configured method list name. ▪ Priority – Defines which order the method list protocols will be queried for authentication when a user attempts to log on to the switch. Priority ranges from 1(highest) to 4 (lowest). ▪ Method Name – Defines which security protocols are implemented, per method list name. ▪ Comment – Defines the type of Method. *User-defined Group* refers to server group defined by the user. *Built-in Group* refers to the TACACS, XTACACS, TACACS+ or RADIUS security protocols which are permanently set in the switch. *Keyword* refers to authentication using a technique ***instead*** of TACACS/XTACACS/TACACS+ or RADIUS, which are local (authentication through the user account on the switch) and none (no authentication necessary to access any function on the switch).
Parameters	*default* – Entering this parameter will display the default method list for users logging on to the switch. *method_list_name <string 15>* - Enter an alphanumeric string of up to 15 characters to define the given *method list* the user wishes to view. *all* – Entering this parameter will display all the authentication login methods currently configured on the switch.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To view all method list configurations:

```
DGS-3312SR:4#show authen_login method_list_name all
Command: show authen_login method_list_name all

Method List Name  Priority   Method Name  Comment
----------------  --------   -----------  ---------
                  1          tacacs+      Built-in Group
GoHabs!           2          radius       Built-in Group
Trinity           3          Darren       User-defined Group
default           4          local        Keyword

DGS-3312SR:4#
```

create authen_enable method_list_name	
Purpose	Used to create a user-defined method list of authentication methods for promoting normal user level privileges to Administrator level privileges on the switch.
Syntax	**create authen_enable method_list_name <string 15>**
Description	This command is used to promote users with normal level privileges to Administrator level privileges using authentication methods on the switch. Once a user acquires normal user level privileges on the switch, he or she must be authenticated by a method on the switch to gain administrator privileges on the switch, which is defined by the Administrator. A maximum of eight (8) enable method lists can be implemented on the switch.
Parameters	*<string 15>* - Enter an alphanumeric string of up to 15 characters to define the given *enable method list* the user wishes to create.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To create a user-defined method list, named "Permit" for promoting user privileges to Adminstrator privileges:

```
DGS-3312SR:4#create authen_enable method_list_name Permit
Command: show authen_login method_list_name Permit

Success.

DGS-3312SR:4#
```

config authen_enable	
Purpose	Used to configure a user-defined method list of authentication methods for promoting normal user level privileges to Administrator level privileges on the switch.
Syntax	**config authen_enable [default | method_list_name <string 15>] method {tacacs | xtacacs | tacacs+ | radius | server_group <string 15> | local_enable | none}**

config authen_enable

Description	This command is used to promote users with normal level privileges to Administrator level privileges using authentication methods on the switch. Once a user acquires normal user level privileges on the switch, he or she must be authenticated by a method on the switch to gain administrator privileges on the switch, which is defined by the Administrator. A maximum of eight (8) enable method lists can be implemented on the switch. The sequence of methods implemented in this command will affect the authentication result. For example, if a user enters a sequence of methods like *tacacs* – *xtacacs* – *local_enable,* the switch will send an authentication request to the first *tacacs* host in the server group. If no verification is found, the switch will send an authentication request to the second *tacacs* host in the server group and so on, until the list is exhausted. At that point, the switch will restart the same sequence with the following protocol listed, *xtacacs*. If no authentication takes place using the *xtacacs* list, the *local_enable* password set in the switch is used to authenticate the user. Successful authentication using any of these methods will give the user a "Admin" privilege.
Parameters	*default* – The default method list for administration rights authentication, as defined by the user. The user may choose one or a combination of up to four (4) of the following authentication methods: ▪ *tacacs* – Adding this parameter will require the user to be authenticated using the TACACS protocol from the remote TACACS *server hosts* of the TACACS *server group* list. ▪ *xtacacs* – Adding this parameter will require the user to be authenticated using the XTACACS protocol from the remote XTACACS *server hosts* of the XTACACS *server group* list. ▪ *tacacs+* – Adding this parameter will require the user to be authenticated using the TACACS+ protocol from the remote TACACS+ *server hosts* of the TACACS+ *server group* list. ▪ *radius* – Adding this parameter will require the user to be authenticated using the RADIUS protocol from the remote RADIUS *server hosts* of the RADIUS *server group* list. ▪ *server_group* <*string 15*> - Adding this parameter will require the user to be authenticated using a user-defined server group previously configured on the switch. ▪ *local_enable* - Adding this parameter will require the user to be authenticated using the local *user account* database on the switch. ▪ *none* – Adding this parameter will require no authentication to access the switch. *method_list_name* – Enter a previously implemented method list name defined by the user (*create authen_enable*). The user may add one, or a combination of up to four (4) of the following authentication methods to this method list: ▪ *tacacs* – Adding this parameter will require the user to be authenticated using the TACACS protocol from a remote TACACS server. ▪ *xtacacs* – Adding this parameter will require the user to be authenticated using the XTACACS protocol from a remote

config authen_enable

	XTACACS server. ▪ *tacacs+* – Adding this parameter will require the user to be authenticated using the TACACS+ protocol from a remote TACACS+ server. ▪ *radius* – Adding this parameter will require the user to be authenticated using the RADIUS protocol from a remote RADIUS server. ▪ *server_group <string 15>* - Adding this parameter will require the user to be authenticated using a user-defined server group previously configured on the switch. ▪ *local_enable* - Adding this parameter will require the user to be authenticated using the local *user account* database on the switch. The local enable password of the device can be configured using the "*config admin local_password*" command. ▪ *none* – Adding this parameter will require no authentication to access the administration level privileges on the switch.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure the user defined method list "Permit" with authentication methods tacacs, xtacacs and local, in that order.

```
DGS-3312SR:4#config authen_enable method_list_name Trinity method
tacacs xtacacs local
Command: config authen_enable method_list_name Trinity method tacacs
xtacacs local

Success.

DGS-3312SR:4#
```

Example usage:

To configure the default method list with authentication methods xtacacs, tacacs+ and local, in that order:

```
DGS-3312SR:4#config authen_enable default method xtacacs tacacs+ local
Command: config authen_enable default method xtacacs tacacs+ local

Success.

DGS-3312SR:4#
```

delete authen_enable method_list_name

Purpose	Used to delete a user-defined method list of authentication methods for promoting normal user level privileges to Administrator level privileges on the switch.
Syntax	**delete authen_enable method_list_name <string 15>**
Description	This command is used to delete a user-defined method list of authentication methods for promoting user level privileges to Administrator level privileges.

delete authen_enable method_list_name	
Parameters	<*string 15*> Enter an alphanumeric string of up to 15 characters to define the given *enable method list* the user wishes to delete.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To delete the user-defined method list "Permit"

```
DGS-3312SR:4#delete authen_enable method_list_name Permit
Command: delete authen_enable method_list_name Permit

Success.

DGS-3312SR:4#
```

show authen_enable	
Purpose	Used to display the method list of authentication methods for promoting normal user level privileges to Administrator level privileges on the switch.
Syntax	**show authen_enable [default | method_list_name <string 15> | all]**
Description	This command is used to delete a user-defined method list of authentication methods for promoting user level privileges to Administrator level privileges. The window will display the following parameters: ▪ Method List Name – The name of a previously configured method list name. ▪ Priority – Defines which order the method list protocols will be queried for authentication when a user attempts to log on to the switch. Priority ranges from 1(highest) to 4 (lowest). ▪ Method Name – Defines which security protocols are implemented, per method list name. ▪ Comment – Defines the type of Method. *User-defined Group* refers to *server groups* defined by the user. *Built-in Group* refers to the TACACS/XTACACS/TACACS+/RADIUS security protocols which are permanently set in the switch. *Keyword* refers to authentication using a technique INSTEAD of TACACS/XTACACS/TACACS+/RADIUS which are local (authentication through the *local_enable* password on the switch) and none (no authentication necessary to access any function on the switch).
Parameters	*default* – Entering this parameter will display the default method list for users attempting to gain access to Administrator level privileges on the switch. *method_list_name* <*string 15*> Enter an alphanumeric string of up to 15 characters to define the given *method list* the user wishes to view. *all* – Entering this parameter will display all the authentication login methods currently configured on the switch.
Restrictions	None

Example usage:

To display all method lists for promoting user level privileges to administrator level privileges.

```
DGS-3312SR:4#show authen_enable all
Command: show authen_enable all

Method List Name   Priority   Method Name   Comment
----------------   --------   ---------------   ------------------
Permit             1          tacacs+           Built-in Group
                   2          tacacs            Built-in Group
                   3          Darren            User-defined Group
                   4          local             Keyword

default            1          tacacs+           Built-in Group
                   2          local             Keyword

Total Entries : 2

DGS-3312SR:4#
```

config authen application

Purpose	Used to configure various applications on the switch for authentication using a previously configured method list.
Syntax	**config authen application [console | telnet | ssh | http | all] [login | enable] [default | method_list_name <string 15>]**
Description	This command is used to configure switch configuration applications (console, telnet, ssh, web) for login at the user level and at the administration level (*authen_enable*) utilizing a previously configured method list.
Parameters	*application* – Choose the application to configure. The user may choose one of the following four applications to configure. ▪ *console* – Choose this parameter to configure the command line interface login method. ▪ *telnet* – Choose this parameter to configure the telnet login method. ▪ *ssh* – Choose this parameter to configure the ssh login method. ▪ *http* – Choose this parameter to configure the web interface login method. ▪ *all* – Choose this parameter to configure all applications (console, telnet, web) login method. *login* – Use this parameter to configure an application for normal login on the user level, using a previously configured method list. *enable* - Use this parameter to configure an application for upgrading a normal user level to administrator privileges, using a previously configured method list. *default* – Use this parameter to configure an application for user authentication using the default method list. *method_list_name <string 15>* - Use this parameter to configure an application for user authentication using a previously configured method list. Enter a alphanumeric string of up to 15 characters to define a previously configured method list.

config authen application	
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure the default method list for the web interface:

```
DGS-3312SR:4#config authen application http login default
Command: config authen application http login default

Success.

DGS-3312SR:4#
```

show authen application	
Purpose	Used to display authentication methods for the various applications on the switch.
Syntax	**show authen application**
Description	This command will display all of the authentication method lists (login, enable administrator privileges) for switch configuration applications (console, telnet, ssh, web) currently configured on the switch.
Parameters	None.
Restrictions	None.

Example usage:

To display the login and enable method list for all applications on the switch:

```
DGS-3312SR:4#show authen application
Command: show authen application

Application   Login Method List   Enable Method List
-----------   -----------------   ------------------------
Console       default             default
Telnet        Trinity             default
SSH           default             default
HTTP          default             default

DGS-3312SR:4#
```

create authen server_host	
Purpose	Used to create an authentication server host.

create authen server_host

Syntax	**create authen server_host <ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius] {port <int 1-65535> | key [<key_string 254> | none] | timeout <int 1-255> | retransmit <1-255>}**
Description	This command will create an authentication server host for the TACACS/XTACACS/TACACS+/RADIUS security protocols on the switch. When a user attempts to access the switch with authentication protocol enabled, the switch will send authentication packets to a remote TACACS/XTACACS/TACACS+/RADIUS server host on a remote host. The TACACS/XTACACS/TACACS+/RADIUS server host will then verify or deny the request and return the appropriate message to the switch. More than one authentication protocol can be run on the same physical server host but, remember that TACACS/XTACACS/TACACS+/RADIUS are separate entities and are not compatible with each other. The maximum supported number of server hosts is 16.
Parameters	*server_host <ipaddr>* - The IP address of the remote server host the user wishes to add. *protocol* – The protocol used by the server host. The user may choose one of the following: ▪ *tacacs* – Enter this parameter if the server host utilizes the TACACS protocol. ▪ *xtacacs* - Enter this parameter if the server host utilizes the XTACACS protocol. ▪ *tacacs+* - Enter this parameter if the server host utilizes the TACACS+ protocol. ▪ *radius* - Enter this parameter if the server host utilizes the RADIUS protocol. *port <int 1-65535>* - Enter a number between 1 and 65535 to define the virtual port number of the authentication protocol on a server host. The default port number is 49 for TACACS/XTACACS/TACACS+ servers but the user may set a unique port number for higher security. The default port number of the authentication protocol on the RADIUS server is 1812 *key <key_string 254>* - Authentication key to be shared with a configured TACACS+ server only. Specify an alphanumeric string up to 254 characters. *timeout <int 1-255>* - Enter the time in seconds the switch will wait for the server host to reply to an authentication request. The default value is 5 seconds. *retransmit <int 1-255>* - Enter the value in the retransmit field to change how many times the device will resend an authentication request when the TACACS/XTACACS/TACACS+ or RADIUS server does not respond.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To create a TACACS+ authentication server host, with port number 1234, a timeout value of 10 seconds and a retransmit count of 5.

```
DGS-3312SR:4#create authen server_host 10.1.1.121 protocol tacacs+ port
1234 timeout 10 retransmit 5

Command: create authen server_host 10.1.1.121 protocol tacacs+ port 1234
timeout 10 retransmit 5


Success.


DGS-3312SR:4#
```

config authen server_host

Purpose	Used to configure a user-defined authentication server host.
Syntax	**config authen server_host <ipaddr> protocol [tacacs | xtacacs | tacacs+] {port <int 1-65535> | key [<key_string 254> | none] | timeout <int 1-255> | retransmit < 1-255>}**
Description	This command will configure a user-defined authentication server host for the TACACS/XTACACS/TACACS+/RADIUS security protocols on the switch. When a user attempts to access the switch with authentication protocol enabled, the switch will send authentication packets to a remote TACACS/XTACACS/TACACS+/RADIUS server host on a remote host. The TACACS/XTACACS/TACACS+/RADIUS server host will then verify or deny the request and return the appropriate message to the switch. More than one authentication protocol can be run on the same physical server host but, remember that TACACS/XTACACS/TACACS+/RADIUS are separate entities and are not compatible with each other. The maximum supported number of server hosts is 16.
Parameters	*server_host <ipaddr>* - The IP address of the remote server host the user wishes to alter. *protocol* – The protocol used by the server host. The user may choose one of the following: ▪ *tacacs* – Enter this parameter if the server host utilizes the TACACS protocol. ▪ *xtacacs* - Enter this parameter if the server host utilizes the XTACACS protocol. ▪ *tacacs+* - Enter this parameter if the server host utilizes the TACACS+ protocol. ▪ *radius*- Enter this parameter if the server host utilizes the RADIUS protocol. *port <int 1-65535>* Enter a number between 1 and 65535 to define the virtual port number of the authentication protocol on a server host. The default port number is 49 for TACACS/XTACACS/TACACS+ servers but the user may set a unique port number for higher security. *key <key_string 254>* - Authentication key to be shared with a

config authen server_host	
	configured TACACS+ server only. Specify an alphanumeric string up to 254 characters or choose none. *timeout <int 1-255>* - Enter the time in seconds the switch will wait for the server host to reply to an authentication request. The default value is 5 seconds. *retransmit <int 1-255>* - Enter the value in the retransmit field to change how many times the device will resend an authentication request when the TACACS, XTACACS server does not respond. This field is inoperable for the TACACS+ protocol.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure a TACACS authentication server host, with port number 4321, a timeout value of 12 seconds and a retransmit count of 4.

```
DGS-3312SR:4#config authen server_host 10.1.1.121 protocol
tacacs port 4321 timeout 12 retransmit 4

Command: config authen server_host 10.1.1.121 protocol tacacs
port 4321 timeout 12 retransmit 4


Success.


DGS-3312SR:4#
```

delete authen server_host	
Purpose	Used to delete a user-defined authentication server host.
Syntax	**delete authen server_host <ipaddr> protocol [tacacs | xtacacs | tacacs+]**
Description	This command is used to delete a user-defined authentication server host previously created on the switch.
Parameters	*server_host <ipaddr>* - The IP address of the remote server host the user wishes to delete. *protocol* – The protocol used by the server host the user wishes to delete. The user may choose one of the following: ▪ *tacacs* – Enter this parameter if the server host utilizes the TACACS protocol. ▪ *xtacacs* - Enter this parameter if the server host utilizes the XTACACS protocol. ▪ *tacacs+* - Enter this parameter if the server host utilizes the TACACS+ protocol. ▪ *radius* - Enter this parameter if the server host utilizes the RADIUS protocol.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To delete a user-defined TACACS+ authentication server host:

```
DGS-3312SR:4#delete authen server_host 10.1.1.121 protocol tacacs+
Command: delete authen server_host 10.1.1.121 protocol tacacs+

Success.

DGS-3312SR:4#
```

show authen server_host

Purpose	Used to view a user-defined authentication server host.
Syntax	**show authen server_host**
Description	This command is used to view user-defined authentication server hosts previously created on the switch. The following parameters are displayed: IP address – The IP address of the authentication server host. Protocol – The protocol used by the server host. Possible results will include tacacs, xtacacs, tacacs+ and radius. Port – The virtual port number on the server host. The default value is 49. Timeout - The time in seconds the switch will wait for the server host to reply to an authentication request. Retransmit - The value in the retransmit field denotes how many times the device will resend an authentication request when the TACACS server does not respond. This field is inoperable for the tacacs+ protocol. Key - Authentication key to be shared with a configured TACACS+ server only.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To view authentication server hosts currently set on the switch:

```
DGS-3312SR:4#show authen server_host
Command: show authen server_host

IP Address   Protocol   Port  Timeout  Retransmit  Key
---------------  --------  -----  -------  ---------------  --------
10.53.13.94  TACACS   49    5          2             No Use

Total Entries : 1

DGS-3312SR:4#
```

create authen server_group	
Purpose	Used to create a user-defined authentication server group.
Syntax	**create authen server_group <string 15>**
Description	This command will create an authentication server group. A server group is a technique used to group TACACS/XTACACS/TACACS+/RADIUS server hosts into user defined categories for authentication using method lists. The user may add up to eight (8) authentication server hosts to this group using the **config authen server_group** command.
Parameters	<*string 15*> Enter an alphanumeric string of up to 15 characters to define the newly created server group.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To create the server group "group_1":

```
DGS-3312SR:4#create server_group group_1
Command: create server_group group_1

Success.

DGS-3312SR:4#
```

config authen server_group	
Purpose	Used to create a user-defined authentication server group.
Syntax	**config authen server_group [tacacs | xtacacs | tacacs+ | radius <string 15>] [add | delete] server_host <ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius]**
Description	This command will configure an authentication server group. A server group is a technique used to group TACACS/XTACACS/TACACS+/RADIUS server hosts into user defined categories for authentication using method lists. The user may define the type of server group by protocol or by previously defined server group. Up to eight (8) authentication server hosts may be added to any particular group
Parameters	*server_group* - The user may define the group by protocol groups built into the switch (TACACS/XTACACS/TACACS+/RADIUS), or by a user-defined group previously created using the **create authen server_group** command. ▪ *tacacs* – Use this parameter to utilize the built-in TACACS server protocol on the switch. Only server hosts utilizing the TACACS protocol may be added to this group. ▪ *xtacacs* – Use this parameter to utilize the built-in XTACACS server protocol on the switch. Only server hosts utilizing the XTACACS protocol may be added to this group. ▪ *tacacs+* – Use this parameter to utilize the built-in TACACS+ server protocol on the switch. Only server hosts utilizing the TACACS+ protocol may be added to this group.

config authen server_group	
	▪ *radius* – Use this parameter to utilize the built-in RADIUS server protocol on the switch. Only server hosts utilizing the RADIUS protocol may be added to this group. ▪ <*string 15*> Enter an alphanumeric string of up to 15 characters to define the previously created server group. This group may add any combination of server hosts to it, regardless of protocol. *[add | delete]* – Enter the correct parameter to add or delete a server host from a server group. *server_host* <*ipaddr*> - Enter the IP address of the previously configured server host the user wishes to add or delete. *protocol* – Enter the protocol utilized by the server host. There are three options: ▪ *tacacs* – Use this parameter to define the protocol if the server host is using the TACACS authentication protocol. ▪ *xtacacs* – Use this parameter to define the protocol if the server host is using the XTACACS authentication protocol. ▪ *tacacs+* – Use this parameter to define the protocol if the server host is using the TACACS+ authentication protocol. ▪ *radius* – Use this parameter to define the protocol if the server host is using the RADIUS authentication protocol.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To add an authentication host to server group "group_1":

```
DGS-3312SR:4#config authen server_group group_1 add server_host
10.1.1.121 protocol tacacs+

Command: config authen server_group group_1 add server_host
10.1.1.121 protocol tacacs+


Success.


DGS-3312SR:4#
```

delete authen server_group	
Purpose	Used to delete a user-defined authentication server group.
Syntax	**delete authen server_group <string 15>**
Description	This command will delete an authentication server group.
Parameters	<*string 15*> - Enter an alphanumeric string of up to 15 characters to define the previously created server group the user wishes to delete.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To delete the server group “group_1”:

```
DGS-3312SR:4#delete server_group group_1
Command: delete server_group group_1

Success.

DGS-3312SR:4#
```

show authen server_group

Purpose	Used to view authentication server groups on the switch.
Syntax	**show authen server_group <string 15>**
Description	This command will display authentication server groups currently configured on the switch. This command will display the following fields: Group Name: The name of the server group currently configured on the switch, including built in groups and user defined groups. IP Address: The IP address of the server host. Protocol: The authentication protocol used by the server host.
Parameters	*<string 15>* - Enter an alphanumeric string of up to 15 characters to define the previously created server group the user wishes to view. Entering this command without the *<string>* parameter will display all authentication server groups on the switch.
Restrictions	None.

```
DGS-3312SR:4#show authen server_group
Command: show authen server_group

Group Name    IP Address                    Protocol
---------------  ---------------                --------
Darren        10.53.13.2                    TACACS
tacacs        10.53.13.94                   TACACS
tacacs+       (This group has no entry)
xtacacs       (This group has no entry)

Total Entries : 4

DGS-3312SR:4#
```

config authen parameter response_timeout

Purpose	Used to configure the amount of time the switch will wait for a user to enter authentication before timing out.

config authen parameter response_timeout	
Syntax	**config authen parameter response_timeout <int 1-255>**
Description	This command will set the time the switch will wait for a response of authentication from the user.
Parameters	*response_timeout <int 1-255>* - Set the time, in seconds, the switch will wait for a response of authentication from the user attempting to log in from the command line interface or telnet interface.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure the response timeout for 60 seconds:

```
DGS-3312SR:4# config authen parameter response_timeout 60
Command: config authen parameter response_timeout 60

Success.

DGS-3312SR:4#
```

config authen parameter attempt	
Purpose	Used to configure the maximum number of times the switch will accept authentication attempts.
Syntax	**config authen parameter attempt <int 1-255>**
Description	This command will configure the maximum number of times the switch will accept authentication attempts. Users failing to be authenticated after the set amount of attempts will be denied access to the switch and will be locked out of further authentication attempts. Command line interface users will have to wait 60 seconds before another authentication attempt. Telnet users will be disconnected from the switch.
Parameters	*parameter attempt <int 1-255>* - Set the maximum number of attempts the user may try to become authenticated by the switch, before being locked out.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To set the maximum number of authentication attempts at 5:

```
DGS-3312SR:4#config authen parameter attempt 5
Command: config authen parameter attempt 5

Success.

DGS-3312SR:4#
```

show authen parameter	
Purpose	Used to display the authentication parameters currently configured on the switch.

	on the switch.
Syntax	**show authen parameter**
Description	This command will display the authentication parameters currently configured on the switch, including the response timeout and user authentication attempts. This command will display the following fields: Response timeout – The configured time allotted for the switch to wait for a response of authentication from the user attempting to log in from the command line interface or telnet interface. User attempts – The maximum number of attempts the user may try to become authenticated by the switch, before being locked out.
Parameters	None.
Restrictions	None.

```
DGS-3312SR:4#show authen parameter
Command: show authen parameter

Response timeout: 60 seconds
User attempts     : 5

DGS-3312SR:4#
```

enable admin

Purpose	Used to promote user level privileges to administrator level privileges
Syntax	**enable admin**
Description	This command is for users who have logged on to the switch on the normal user level, to become promoted to the administrator level. After logging on to the switch users, will have only user level privileges. To gain access to administrator level privileges, the user will enter this command and will have to enter an authentication password. Possible authentication methods for this function include TACACS/XTACACS/TACACS+/RADIUS, user defined server groups, local enable (local account on the switch), or no authentication (none). Because XTACACS and TACACS do not support the enable function, the user must create a special account on the server host which has the username “enable”, and a password configured by the administrator that will support the “enable” function. This function becomes inoperable when the authentication policy is disabled.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To enable administrator privileges on the switch:

```
DGS-3312SR:4#enable admin
```

```
Password: ******

DGS-3312SR:4#
```

config admin local_enable

Purpose	Used to configure the local enable password for administrator level privileges.
Syntax	**config admin local_enable**
Description	This command will configure the locally enabled password for the *enable admin* command. When a user chooses the "*local_enable*" method to promote user level privileges to administrator privileges, he or she will be prompted to enter the password configured here, that is set locally on the switch.
Parameters	*<password 15>* - After entering this command, the user will be prompted to enter the old password, then a new password in an alphanumeric string of no more than 15 characters, and finally prompted to enter the new password again to confirm. See the example below.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure the password for the "local_enable" authentication method.

```
DGS-3312SR:4#config admin local_enable
Command: config admin local_enable

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

Success.

DGS-3312SR:4#
```

22

SSH COMMANDS

The steps required to use the SSH protocol for secure communication between a remote PC (the SSH Client) and the Switch (the SSH Server), are as follows:

- Create a user account with admin-level access using the *create account admin <username> <password>* command. This is identical to creating any other admin-lever User account on the Switch, including specifying a password. This password is used to login to the Switch, once secure communication has been established using the SSH protocol.
- Configure the user account to use a specified authorization method to identify users that are allowed to establish SSH connections with the Switch using the *config ssh user authmode* command. There are three choices as to the method SSH will use to authorize the user, and they are password, publickey and hostbased.
- Configure the encryption algorithm that SSH will use to encrypt and decrypt messages sent between the SSH Client and the SSH Server.
- Finally, enable SSH on the Switch using the *enable ssh* command.
- After following the above steps, you can configure an SSH Client on the remote PC and manage the Switch using secure, in-band communication.

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

Command	Parameters
enable ssh	
disable ssh	
config ssh authmode	[password | publickey | hostbased] [enable | disable]
show ssh authmode	
config ssh server	{maxsession <int 1-8> | contimeout <sec 120-600> | authfail <int 2-20> | rekey [10min | 30min | 60min | never] port <tcp_port_number 1-65535>}
show ssh server	
config ssh user	<username> authmode {Hostbased [hostname <string> | hostname_IP <string> <ipaddr>} | Password | Publickey | None]
show ssh user authmode	
config ssh algorithm	[3DES | AES128 | AES192 | AES256 | arcfour | blowfish | cast128 | twofish128 | twofish192 | twofish256 | MD5 | SHA1 | DSA | RSA] [enable | disable]
show ssh algorithm	

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

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

Usage Example:

To enable SSH:

```
DGS-3312SR:4#enable ssh
Command: enable ssh

Success.

DGS-3312SR:4#
```

disable ssh

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

Usage Example:

To disable SSH:

```
DGS-3312SR:4# disable ssh
Command: disable ssh

Success.

DGS-3312SR:4#
```

config ssh authmode

Purpose	Used to configure the SSH authentication mode setting.
Syntax	**config ssh authmode [password | publickey | hostbased] [enable | disable]**
Description	This command will allow you to configure the SSH authentication mode for users attempting to access the switch.

config ssh authmode	
Parameters	*password* – This parameter may be chosen if the administrator wishes to use a locally configured password for authentication on the switch. *publickey* - This parameter may be chosen if the administrator wishes to use a publickey configuration set on a SSH server, for authentication. *hostbased* - This parameter may be chosen if the administrator wishes to use a host computer for authentication. This parameter is intended for Linux users requiring SSH authentication techniques and the host computer is running the Linux operating system with a SSH program previously installed. *[enable* | *disable]* - This allows you to enable or disable SSH authentication on the switch.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To enable the SSH authentication mode by password:

```
DGS-3312SR:4#config ssh authmode password enable

Command: config ssh authmode password enable


Success.


DGS-3312SR:4#
```

show ssh authmode	
Purpose	Used to display the SSH authentication mode setting.
Syntax	**show ssh authmode**
Description	This command will allow you to display the current SSH authentication set on the switch.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To view the current authentication mode set on the switch:

```
DGS-3312SR:4#show ssh authmode
Command: show ssh authmode

The SSH authmode
Password     : Enable
Publickey    : Enable
Hostbased    : Enable

DGS-3312SR:4#
```

config ssh server	
Purpose	Used to configure the SSH server.
Syntax	**config ssh server {maxsession <int 1-8> | contimeout <sec 120-600> | authfail <int 2-20> | rekey [10min | 30min | 60min | never] | port <tcp_port_number 1-65535>}**
Description	This command allows you to configure the SSH server.
Parameters	*maxsession <int 1-8>* - Allows the user to set the number of users that may simultaneously access the switch. The default is 8. *contimeout <sec 120-600>* - Allows the user to set the connection timeout. The user may set a time between 120 and 600 seconds. The default is 300 seconds. *authfail <int 2-20>* - Allows the administrator to set the maximum number of attempts that a user may try to log on utilizing SSH authentication. After the maximum number of attempts is exceeded, the switch will be disconnected and the user must reconnect to the switch to attempt another login. *rekey [10min | 30min | 60min | never]* - Sets the time period that the switch will change the security shell encryptions. *port <tcp_port_number 1-65535>* - Enter the TCP port number associated with this function. The default TCP port number for SSH is 22.
Restrictions	Only administrator-level users can issue this command.

Usage Example:

To configure the SSH server:

```
DGS-3312SR:4# config ssh server maxsession 2 contimeout 300 authfail 2
Command: config ssh server maxsession 2 contimeout 300 authfail 2

Success.

DGS-3312SR:4#
```

show ssh server	
Purpose	Used to display the SSH server setting.
Syntax	**show ssh server**
Description	This command allows you to display the current SSH server setting.
Parameters	None.
Restrictions	Only adminstrator-level users can issue this command.

Usage Example:

To display the SSH server:

```
DGS-3312SR:4# show ssh server
Command: show ssh server
The SSH server configuration
max Session                    : 8
Connection timeout             : 300 (sec)
Authfail attempts              : 2
Rekey timeout                  : never
SSH server status              : Disable
Listened Port Number           : 22

DGS-3312SR:4#
```

config ssh user

Purpose	Used to configure the SSH user.
Syntax	**config ssh user <username> authmode {Hostbased [hostname <string> | hostname_IP <string> <ipaddr>} | Password | Publickey | None]**
Description	This command allows you to configure the SSH user authentication method.
Parameters	*<username>* - Enter a username of no more than 15 characters to identify the SSH user. *authmode* – Specifies the authentication mode of the SSH user wishing to log on to the switch. The administrator may choose between: ▪ *Hostbased* – This parameter should be chosen if the user wishes to use a remote SSH server for authentication purposes. Choosing this parameter requires the user to input the following information to identify the SSH user. • *hostname <string>* - Enter an alphanumeric string of up to 31 characters identifying the remote SSH user. • *hostname_IP <string> <ipaddr>* - Enter the hostname and the corresponding IP address of the SSH user. ▪ *Password* – This parameter should be chosen if the user wishes to use an administrator defined password for authentication. Upon entry of this command, the switch will prompt the user for a password, and then to retype the password for confirmation. ▪ *Publickey* – This parameter should be chosen if the user wishes to use the publickey on a SSH server for authentication. ▪ *None* – Choose this parameter if no authentication is desired.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure the SSH user:

```
DGS-3312SR:4# config ssh user Trinity authmode Password
Command: config ssh user Trinity authmode Password

Success.

DGS-3312SR:4#
```

show ssh user authmode

Purpose	Used to display the SSH user setting.
Syntax	**show ssh user authmode**
Description	This command allows you to display the current SSH user setting.
Parameters	None.
Restrictions	Only adminstrator-level users can issue this command.

Example usage:

To display the SSH user:

```
DGS-3312SR:4#show ssh user authmode
Command: show ssh user authmode

Current Accounts:    Authentication
UserName
-------------------- --------------------
Trinity              Publickey

DGS-3312SR:4#
```

Note: To configure the SSH user, the administrator must create a user account on the switch. For information concerning configuring a user account, please see the section of this manual entitled **Basic Switch Commands** and then the command, **create user account.**

config ssh algorithm

Purpose	Used to configure the SSH algorithm.
Syntax	**config ssh algorithm [3DES | AES128 | AES192 | AES256 | arcfour | blowfish | cast128 | twofish128 | twofish192 | twofish256 | MD5 | SHA1 | RSA | DSA] [enable | disable]**
Description	This command allows you to configure the desired type of SSH algorithm used for authentication encryption.
Parameters	*3DES* – This parameter will enable or disable the Triple_Data Encryption Standard encryption algorithm.

config ssh algorithm	
	AES128 - This parameter will enable or disable the Advanced Encryption Standard AES128 encryption algorithm. *AES192* - This parameter will enable or disable the Advanced Encryption Standard AES192 encryption algorithm. *AES256* - This parameter will enable or disable the Advanced Encryption Standard AES256 encryption algorithm. *arcfour* - This parameter will enable or disable the Arcfour encryption algorithm. *blowfish* - This parameter will enable or disable the Blowfish encryption algorithm. *cast128* - This parameter will enable or disable the Cast128 encryption algorithm. *twofish128* - This parameter will enable or disable the twofish128 encryption algorithm. *twofish192* - This parameter will enable or disable the twofish192 encryption algorithm. *MD5* - This parameter will enable or disable the MD5 Message Digest encryption algorithm. *SHA1* - This parameter will enable or disable the Secure Hash Algorithm encryption. *DSA* - This parameter will enable or disable the Digital Signature Algorithm encryption. *RSA* - This parameter will enable or disable the RSA encryption algorithm. *[enable* | *disable]* – This allows you to enable or disable algorithms entered in this command, on the switch.
Restrictions	Only administrator-level users can issue this command.

Usage Example:

To configure SSH algorithm:

```
DGS-3312SR:4# config ssh algorithm blowfish enable

Command: config ssh algorithm blowfish enable


Success.


DGS-3312SR:4#
```

show ssh algorithm	
Purpose	Used to display the SSH algorithm setting.
Syntax	**show ssh algorithm**
Description	This command will display the current SSH algorithm setting status.
Parameters	None.
Restrictions	Only adminstrator-level users can issue this command.

Usage Example:

To display SSH algorithms currently set on the switch:

```
DGS-3312SR:4#show ssh algorithm
Command: show ssh algorithm

Encryption Algorithm
3DES            :Enable
AES128          :Enable
AES192          :Enable
AES256          :Enable
ARC4            :Enable
Blowfish        :Enable
Cast128         :Enable
Twofish128      :Enable
Twofish192      :Enable
Twofish256      :Enable
MD5             :Enable
SHA             :Enable
RSA             :Enable
DSA             :Enable

DGS-3312SR:4#
```

23

SSL COMMANDS

Secure Sockets Layer or *SSL* is a security feature that will provide a secure communication path between a host and client through the use of authentication, digital signatures and encryption. These security functions are implemented through the use of a *ciphersuite*, which is a security string that determines the exact cryptographic parameters, specific encryption algorithms and key sizes to be used for an authentication session and consists of three levels:

1. **Key Exchange:** The first part of the cyphersuite string specifies the public key algorithm to be used. This switch utilizes the Rivest Shamir Adleman (RSA) public key algorithm and the Digital Signature Algorithm (DSA), specified here as the *DHE_DSS* Diffie-Hellman (DHE) public key algorithm. This is the first authentication process between client and host as they "exchange keys" in looking for a match and therefore authentication to be accepted to negotiate encryptions on the following level.
2. **Encryption:** The second part of the ciphersuite that includes the encryption used for encrypting the messages sent between client and host. The switch supports two types of cryptology algorithms:
   - Stream Ciphers – There are two types of stream ciphers on the switch, *RC4 with 40-bit keys* and *RC4 with 128-bit keys*. These keys are used to encrypt messages and need to be consistent between client and host for optimal use.
   - CBC Block Ciphers – CBC refers to Cipher Block Chaining, which means that a portion of the previously encrypted block of encrypted text is used in the encryption of the current block. The switch supports the *3DES_EDE* encryption code defined by the Data Encryption Standard (DES) to create the encrypted text.
3. **Hash Algorithm**: This part of the ciphersuite allows the user to choose a message digest function which will determine a Message Authentication Code. This Message Authentication Code will be encrypted with a sent message to provide integrity and prevent against replay attacks. The switch supports two hash algorithms, *MD5* (Message Digest 5) and *SHA* (Secure Hash Algorithm).

These three parameters are uniquely assembled in four choices on the switch to create a three-layered encryption code for secure communication between the server and the host. The user may implement any one or combination of the ciphersuites available, yet different ciphersuites will affect the security level and the performance of the secured connection. The information included in the ciphersuites is not included with the switch and requires downloading from a third source in a file form called a *certificate*. This function of the switch cannot be executed without the presence and implementation of the certificate file and can be downloaded to the switch by utilizing a TFTP server. The switch supports SSLv3 and TLSv1. Other versions of SSL may not be compatible with this switch and may cause problems upon authentication and transfer of messages from client to host.

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

Command	Parameters
enable ssl	[ciphersuite {RSA_with_RC4_128_MD5 | RSA_with_3DES_EDE_CBC_SHA | DHE_DSS_with_3DES_EDE_CBC_SHA | RSA_EXPORT_with_RC4_40_MD5}}
disable ssl	[ciphersuite {RSA_with_RC4_128_MD5 | RSA_with_3DES_EDE_CBC_SHA | DHE_DSS_with_3DES_EDE_CBC_SHA | RSA_EXPORT_with_RC4_40_MD5}}
show ssl	
download certificate	<ipaddr> certfilename <path_filename 64> keyfilename <path_filename 64>
show certificate	

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

enable ssl	
Purpose	To enable the SSL function on the switch.
Syntax	**enable ssl {ciphersuite {RSA_with_RC4_128_MD5 | RSA_with_3DES_EDE_CBC_SHA | DHE_DSS_with_3DES_EDE_CBC_SHA | RSA_EXPORT_with_RC4_40_MD5}}**
Description	This command will enable SSL on the switch by implementing any one or combination of listed ciphersuites on the switch. Entering this command without a parameter will enable the SSL status on the switch. Enabling SSL will disable the web-manager on the switch.
Parameters	*ciphersuite* - A security string that determines the exact cryptographic parameters, specific encryption algorithms and key sizes to be used for an authentication session. The user may choose any combination of the following: ▪ *RSA_with_RC4_128_MD5* – This ciphersuite combines the RSA key exchange, stream cipher RC4 encryption with 128-bit keys and the MD5 Hash Algorithm. ▪ *RSA_with_3DES_EDE_CBC_SHA* - This ciphersuite combines the RSA key exchange, CBC Block Cipher 3DES_EDE encryption and the SHA Hash Algorithm. ▪ *DHE_DSS_with_3DES_EDE_CBC_SHA* - This ciphersuite combines the DSA Diffie Hellman key exchange, CBC Block Cipher 3DES_EDE encryption and SHA Hash Algorithm. ▪ *RSA_EXPORT_with_RC4_40_MD5* - This ciphersuite combines the RSA Export key exchange, stream cipher RC4 encryption with 40-bit keys. The ciphersuites are enabled by default on the switch, yet the SSL status is disabled by default.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To enable SSL on the switch for all ciphersuites:

```
DGS-3312SR:4#enable ssl
Command: enable ssl

Success.

DGS-3312SR:4#
```

NOTE: Enabling the SSL function on the switch will disable the port for the web manager (port 80). To log on to the web based manager, the entry of your URL must begin with *https://*. (ex. https://10.90.90.90)

disable ssl	
Purpose	To disable the SSL function on the switch.
Syntax	**disable ssl {ciphersuite {RSA_with_RC4_128_MD5 | RSA_with_3DES_EDE_CBC_SHA | DHE_DSS_with_3DES_EDE_CBC_SHA | RSA_EXPORT_with_RC4_40_MD5}}**
Description	This command will disable SSL on the switch and can be used to disable any one or combination of listed ciphersuites on the switch.
Parameters	*ciphersuite* - A security string that determines the exact cryptographic parameters, specific encryption algorithms and key sizes to be used for an authentication session. The user may choose any combination of the following: ▪ *RSA_with_RC4_128_MD5* – This ciphersuite combines the RSA key exchange, stream cipher RC4 encryption with 128-bit keys and the MD5 Hash Algorithm. ▪ *RSA_with_3DES_EDE_CBC_SHA* - This ciphersuite combines the RSA key exchange, CBC Block Cipher 3DES_EDE encryption and the SHA Hash Algorithm. ▪ *DHE_DSS_with_3DES_EDE_CBC_SHA* - This ciphersuite combines the DSA Diffie Hellman key exchange, CBC Block Cipher 3DES_EDE encryption and SHA Hash Algorithm. ▪ *RSA_EXPORT_with_RC4_40_MD5* - This ciphersuite combines the RSA Export key exchange, stream cipher RC4 encryption with 40-bit keys.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To disable the SSL status on the switch:

```
DGS-3312SR:4#disable ssl
Command: disable ssl

Success.

DGS-3312SR:4#
```

To disable ciphersuite *RSA_EXPORT_with_RC4_40_MD5* only:

```
DGS-3312SR:4#disable ssl ciphersuite RSA_EXPORT_with_RC4_40_MD5
Command: disable ssl ciphersuite RSA_EXPORT_with_RC4_40_MD5

Success.

DGS-3312SR:4#
```

show ssl	
Purpose	Used to view the SSL status and the certificate file status on the switch.
Syntax	**show ssl**
Description	This command is used to view the SSL status on the switch.
Parameters	None.
Restrictions	None.

Example usage:

To view the SSL status on the switch:

```
DGS-3312SR:4#show ssl

Command: show ssl

 SSL Status                                Disabled
 RSA_WITH_RC4_128_MD5                0x0004 Enabled
 RSA_WITH_3DES_EDE_CBC_SHA           0x000A Enabled
 DHE_DSS_WITH_3DES_EDE_CBC_SHA       0x0013 Enabled
 RSA_EXPORT_WITH_RC4_40_MD5          0x0003 Enabled


DGS-3312SR:4#
```

download certificate	
Purpose	Used to download a certificate file for the SSL function on the switch.
Syntax	**download certificate <ipaddr> certfilename <path_filename 64> keyfilename <path_filename 64>**
Description	This command is used to download a certificate file for the SSL function on the switch from a TFTP server. The certificate file is a data record used for authenticating devices on the network. It contains information on the owner, keys for authentication and digital signatures. Both the server and the client must have consistent certificate files for optimal use of the SSL function. The switch only supports certificate files with .der file extensions.
Parameters	*<ipaddr>* - Enter the IP address of the TFTP server. *certfilename <path_filename 64>* - Enter the path and the filename of the certificate file you wish to download. *keyfilename <path_filename 64>* - Enter the path and the filename of the key exchange file you wish to download.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To download a certificate file and key file to the switch:

```
DGS-3312SR:4# DGS-3312SR:4#download certificate 10.53.13.94
certfilename c:/cert.der keyfilename c:/pkey.der

Command: download certificate 10.53.13.94 certfilename
c:/cert.der keyfilename c:/pkey.der


Certificate Loaded Successfully!


DGS-3312SR:4#
```

show certificate

Purpose	Used to view the certificate files for the SSL function on the switch.
Syntax	**show certificate**
Description	This command is used to view the SSL certificate currently in use on the switch.
Parameters	None.
Restrictions	None.

Example usage:

To view the SSL certificate:

```
DGS-3312SR:4# show certificate

Command: show certificate


Loaded with RSA Certificate!


DGS-3312SR:4#
```

24

802.1X COMMANDS

The DGS-3312SR 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.

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

Command	Parameters
enable 802.1x	
disable 802.1x	
show 802.1x auth_state	ports [<portlist>]
show 802.1x auth_configuration	ports [<portlist>]
config 802.1x auth_mode	[port_based | mac_based]
config 802.1x capability	[ports <portlist> | all] [authenticator | none]
config 802.1x auth_parameter ports	[<portlist> | all] [default | {direction [both | in] | port_control [force_unauth | auto | force_auth] | quiet_period <sec 0-65535> | tx_period <sec 1-65535> | supp_timeout <sec 1-65535> | server_timeout <sec 1-65535> | max_req <value 1-10> | reauth_period <sec 1-65535> | enable_reauth [enable | disable]}]
config 802.1x init	{port_based ports [<portlist> | all]} | mac_based [ports] [<portlist> | all] {mac_address <macaddr>}]
config 802.1x reauth	{port_based ports [<portlist> | all]} [<portlist> | all] {mac_address <macaddr>}]
config radius add	<server_index 1-3> <server_ip> key <passwd 32> [default {auth_port <udp_port_number 1-65535> | acct_port <udp_port_number 1-65535>}]
config radius delete	<server_index 1-3>
config radius	<server_index 1-3> {ipaddress <server_ip> | key <passwd 32> [auth_port <udp_port_number 1-65535> acct_port <udp_port_number 1-65535>]}
show radius	

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

NOTE: As a stand-alone switch or as a master switch in a switch stack, the switch number will be referred to as 15 for all configurations, graphs and tables.

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

Example usage:

To enable 802.1x switch wide:

```
DGS-3312SR:4#enable 802.1x
Command: enable 802.1x

Success.

DGS-3312SR: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 Network Access control server application on the switch.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To disable 802.1x on the switch:

```
DGS-3312SR:4#disable 802.1x
Command: disable 802.1x

Success.

DGS-3312SR:4#
```

show 802.1x auth_configuration	
Purpose	Used to display the current configuration of the 802.1x server on the switch.
Syntax	**show 802.1x auth_configuration {ports [<portlist>}**
Description	The show 802.1x command is used to display the current configuration of the 802.1x Port-based Network Access Control server application on the switch.

show 802.1x auth_configuration

Parameters	*ports <portlist>* – Specifies a range of ports. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3-2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. The following details what is displayed: 802.1x Enabled/Disabled – Shows the current status of 802.1x functions on the switch. Authentication Protocol: Radius_Eap – Shows the authentication protocol suite in use between the switch and a Radius server. Port number – Shows the physical port number on the switch. Capability: Authenticator/None – Shows the capability of 802.1x functions on the port number displayed above. There are two 802.1x capabilities that can be set on the switch: Authenticator and None. AdminCtlDir: Both/In – Shows whether a controlled Port that is unauthorized will exert control over communication in both receiving and transmitting directions, or just the receiving direction. OpenCtlDir: Both/In – Shows whether a controlled Port that is unauthorized will exert control over communication in both receiving and transmitting directions, or just the receiving direction. Port Control: ForceAuth/ForceUnauth/Auto – Shows the administrative control over the port's authorization status. ForceAuth forces the Authenticator of the port to become Authorized. ForceUnauth forces the port to become Unauthorized. QuietPeriod – Shows the time interval between authentication failure and the start of a new authentication attempt. TxPeriod – Shows the time to wait for a response from a supplicant (user) to send EAP Request/Identity packets. SuppTimeout – Shows the time to wait for a response from a supplicant (user) for all EAP packets, except for the Request/Identity packets. ServerTimeout – Shows the length of time to wait for a response from a RADIUS server. MaxReq – Shows the maximum number of times to retry sending packets to the supplicant. ReAuthPeriod – Shows the time interval between successive re-authentications. ReAuthenticate: Enabled/Disabled – Shows whether or not to re-authenticate.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To display the 802.1x authentication states (stacking disabled):

```
DGS-3312SR:4#show 802.1x auth_configuration ports 1
Command: show 802.1x auth_configuration ports 1

802.1X                    : Enabled
Authentication Mode       : None
Authentication Protocol   : Radius_EAP

Port number       : 1:1
Capability        : None
AdminCrlDir       : Both
OpenCrlDir        : Both
Port Control      : Auto
QuietPeriod       : 60    sec
TxPeriod          : 30    sec
SuppTimeout       : 30    sec
ServerTimeout     : 30    sec
MaxReq            : 2     times
ReAuthPeriod      : 3600  sec
ReAuthenticate    : Disabled

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

show 802.1x auth_state

Purpose	Used to display the current authentication state of the 802.1x server on the switch.
Syntax	**show 802.1x auth_state {ports [<portlist>}**
Description	The **show 802.1x auth_state** command is used to display the current authentication state of the 802.1x Port-based Network Access Control server application on the switch.
Parameters	*ports <portlist>* – Specifies a range of ports. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 3 would specify port 3. 4 specifies port 4. 3-4 specifies all of the ports between port 3 and port 4 – in numerical order. The following details what is displayed: Port number – Shows the physical port number on the switch. Auth PAE State: Initialize / Disconnected / Connecting / Authenticating / Authenticated / Held / ForceAuth / ForceUnauth – Shows the current state of the Authenticator PAE. Backend State: Request / Response / Fail / Idle / Initialize / Success / Timeout – Shows the current state of the Backend Authenticator. Port Status: Authorized / Unauthorized – Shows the result of the authentication process. Authorized means that the user was authenticated, and can access the network. Unauthorized means that the user was not authenticated, and cannot access the network.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To display the 802.1x auth state:

```
DGS-3312SR:4#show 802.1x auth_state 1:1-1:12
Command: show 802.1x auth_state 1:1-1:12

Port     Auth PAE State       Backend State       Port Status
------   ----------------     ----------------    ----------------
1:1      ForceAuth            Success             Authorized
1:2      ForceAuth            Success             Authorized
1:3      ForceAuth            Success             Authorized
1:4      ForceAuth            Success             Authorized
1:5      ForceAuth            Success             Authorized
1:6      ForceAuth            Success             Authorized
1:7      ForceAuth            Success             Authorized
1:8      ForceAuth            Success             Authorized
1:9      ForceAuth            Success             Authorized
1:10     ForceAuth            Success             Authorized
1:11     ForceAuth            Success             Authorized
1:12     ForceAuth            Success             Authorized

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

config 802.1x auth_mode

Purpose	Used to configure the 802.1x authentication mode on the switch.
Syntax	**config 802.1x auth_mode [port_based | mac_based]**
Description	The **config 802.1x auth_mode** command is used to enable either the port-based or MAC-based 802.1x authentication feature on the switch.
Parameters	*[port_based* | *mac_based ports]* – The switch allows you to authenticate 802.1x by either port or MAC address.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure 802.1x authentication by MAC address:

```
DGS-3312SR:4#config 802.1x auth_mode mac_based
Command: config 802.1x auth_mode mac_based

Success.

DGS-3312SR:4#
```

config 802.1x capability ports

Purpose	Used to configure the 802.1x capability of a range of ports on the switch.
Syntax	**config 802.1x capability ports [<portlist> | all] [authenticator | none]**
Description	The **config 802.1x capability ports** command has four capabilities that can be set for each port. Authenticator, Supplicant, Authenticator and Supplicant, and None.
Parameters	*<portlist>* – Specifies a range of ports. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3-2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. *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 on switch 1:

```
DGS-3312SR:4#config 802.1x capability ports 1:1 – 1:10 authenticator
Command: config 802.1x capability ports 1:1 – 1:10  authenticator

Success.

DGS-3312SR:4#
```

config 802.1x auth_parameter

Purpose	Used to configure the 802.1x Authentication parameters on a range of ports. The default parameter will return all ports in the specified range to their default 802.1x settings.
Syntax	**config 802.1x auth_parameter ports [<portlist> | all] [default | {direction [both | in] | port_control [force_unauth | auto | force_auth] | quiet_period <sec 0-65535>| tx_period <sec 1-65535> | supp_timeout <sec 1-65535> | server_timeout <sec 1-65535> | max_req <value 1-10> | reauth_period <sec 1-65535> | enable_reauth [enable | disable]}]**
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.

config 802.1x auth_parameter	
Parameters	*<portlist>* – Specifies a range of ports. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3-2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. *all* – Specifies all of the ports on the switch. *default* – Returns all of the ports in the specified range to their 802.1x default settings. *direction [both | in]* – Determines whether a controlled port blocks communication in both the receiving and transmitting directions, or just the receiving direction. *port_control* – Configures the administrative control over the authentication process for the range of ports. The user has the following authentication options: • *force_auth* – Forces the Authenticator for the port to become authorized. Network access is allowed. • *auto* – Allows the port's status to reflect the outcome of the authentication process. • *force_unauth* – Forces the Authenticator for the port to become unauthorized. Network access will be blocked. *quiet_period <sec 0-65535>* – Configures the time interval between authentication failure and the start of a new authentication attempt. *tx_period <sec 1-65535>* – Configures the time to wait for a response from a supplicant (user) to send EAP Request/Identity packets. *supp_timeout <sec 1-65535>* – Configures the time to wait for a response from a supplicant (user) for all EAP packets, except for the Request/Identity packets. *server_timeout <sec 1-65535>* – Configure the length of time to wait for a response from a RADIUS server. *max_req <value 1-10>* – Configures the number of times to retry sending packets to a supplicant (user). *reauth_period <sec 1-65535>* – Configures the time interval between successive re-authentications. *enable_reauth [enable | disable]* – Determines whether or not the switch will re-authenticate. Enabled causes re-authentication of users at the time interval specified in the Re-authentication Period field, above.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure 802.1x authentication parameters for ports 1 – 20 of switch 1:

```
DGS-3312SR: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-3312SR:4#
```

config 802.1x init

Purpose	Used to initialize the 802.1x function on a range of ports.
Syntax	**config 802.1x init [port_based ports [<portlist | all>] | mac_based [ports] [<portlist> | all] {mac_address <macaddr>}]**
Description	The **config 802.1x init** command is used to immediately initialize the 802.1x functions on a specified range of ports or for specified MAC addresses operating from a specified range of ports.
Parameters	*port_based* – This instructs the switch to initialize 802.1x functions based only on the port number. Ports approved for initialization can then be specified. ▪ *<portlist>* – Specifies a range of ports. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3-2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. ▪ *all* – Specifies all of the ports on the switch. *mac_based* - This instructs the switch to initialize 802.1x functions based on the MAC address of a device on a specific port or range of ports. MAC address approved for initialization can then be specified. ▪ *<portlist>* – Specifies a range of ports. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3-2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. ▪ *all* – Specifies all of the ports on the switch. *mac_address <macaddr>* - Specifies the MAC address of the client the user wishes to add.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To initialize the authentication state machine of some or all:

```
DGS-3312SR:4# config 802.1x init port_based ports all
Command: config 802.1x init port_based ports all

Success.

DGS-3312SR:4#
```

config 802.1x reauth ports

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

Example usage:

To configure 802.1x reauthentication for ports 1-10:

```
DGS-3312SR:4#config 802.1x reauth port_based ports 1:1-1:18
Command: config 802.1x reauth port_based ports 1:1-1:18

Success.

DGS-3312SR:4#
```

config radius add

Purpose	Used to add a new RADIUS server.
Syntax	**config radius add <server_index 1-3> <server_ip> key <passwd 32> [default | {auth_port <udp_port_number 1-65535> | acct_port <udp_port_number 1-65535>}]**
Description	The **config radius add** command is used to add RADIUS servers to the switch.
Parameters	*<server_index 1-3>* – Assigns a number to the current set of RADIUS server settings. Up to 3 groups of RADIUS server settings can be entered on the switch. The lowest index number will have a higher authenticative priority *<server_ip>* – The IP address of the RADIUS server. *key* – Specifies that a password and encryption key will be used between the switch and the RADIUS server. ▪ *<passwd 32>* – The shared-secret key used by the RADIUS server and the switch. Up to 32 characters can be used. *default* – Uses the default udp port number in both the "auth_port" and "acct_port" settings. *auth_port <udp_port_number>* – 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 the RADIUS server communication settings:

```
DGS-3312SR: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-3312SR: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>* – A number identifying the current set of RADIUS server settings the user wishes to delete. Up to 3 groups of RADIUS server settings can be entered on the switch.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To delete previously configured RADIUS server communication settings:

```
DGS-3312SR:4#config radius delete 1
Command: config radius delete 1

Success.

DGS-3312SR:4#
```

config radius

Purpose	Used to configure the switch's RADIUS settings.
Syntax	**config radius <server_index 1-3> {ipaddress <server_ip> | key <passwd 32> | auth_port <udp_port_number 1-65535> | acct_port <udp_port_number 1-65535>}**
Description	The **config radius** command is used to configure the switch's RADIUS settings.
Parameters	*<server_index 1-3>* – Assigns a number to the current set of RADIUS server settings. Up to 3 groups of RADIUS server settings can be entered on the switch. *ipaddress <server_ip>* – The IP address of the RADIUS server. *key* – Specifies that a password and encryption key will be used between the switch and the RADIUS server. ▪ <passwd 32> – The shared-secret key used by the RADIUS server and the switch. Up to 32 characters can be used. *auth_port <udp_port_number>* – 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 the RADIUS settings:

```
DGS-3312SR:4#config radius 1 10.48.74.121 key dlink default
Command: config radius 1 10.48.74.121 key dlink default

 Success.

DGS-3312SR:4#
```

show radius

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

Example usage:

To display RADIUS settings on the switch:

```
DGS-3312SR:4#show radius
Command: show radius

Index  IP Address      Auth-Port   Acct-Port   Status      Key
                       Number      Number
-----  ---------------  ---------   ---------   ----------  ----------
1      10.1.1.1         1812        1813        Active      switch
2      20.1.1.1         1800        1813        Active      des3226
3      30.1.1.1         1812        1813        Active      dlink

Total Entries : 3

DGS-3312SR:4#
```

25

ACCESS CONTROL LIST (ACL) COMMANDS

The DGS-3312SR 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. The ACL commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

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> | flag_mask [all | {urg | ack | psh | rst | syn | fin}]} | udp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | protocol_id {user_mask <hex 0x0-0xffffffff>}]} | packet_content_mask {offset_0-15 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_16-31 <hex0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_32-47 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_48-63 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_64-79 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff>}] {port [<portlist> | all]} [profile_id <value 1-255>]
delete access_profile profile_id	<value 1-255>
config access_profile profile_id	<value 1-255> [add access_id <value 1-255> [ethernet {vlan <vlan_name 32> | source_mac <macaddr> | destination_mac <macaddr> | 802.1p <value 0-7> | ethernet_type <hex 0x0-0xffff> [permit {priority <value 0-7> {replace_priority}} | deny] | ip {vlan <vlan_name 32> | source_ip <ipaddr> | destination_ip <ipaddr> | dscp <value 0-63> | [icmp {type <value 0-255> code <value 0-255>} | igmp {type <value 0-255>} | tcp {src_port <value 0-65535> | dst_port <value 0-65535> | flag_mask [all | {urg | ack | psh | rst | syn | fin}]} | udp {src_port <value 0-65535> | dst_port <value 0-65535>} | protocol_id <value 0 - 255> {user_define <hex 0x0-0xffffffff>}]} [permit {priority <value 0-7> {replace_priority }} | deny] | packet_content {offset_0-15 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_16-31 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_32-47 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_48-63 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_64-79 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff>}] [permit {priority <value 0-7> {replace_priority} | deny] | delete access_id <value 1-255>]
show access_profile	{profile_id <value 1-255>}

Access profiles allow you to establish criteria to determine whether or not the switch will forward packets based on the information contained in each packet's header. These criteria can be specified on a VLAN-by-VLAN basis.

Creating an access profile is divided into two basic parts. First, an access profile must be created using the **create access_profile** command. For example, if you want to deny all traffic to the subnet 10.42.73.0 to 10.42.73.255, you must first **create** an access profile that instructs the switch to examine all of the relevant fields of each frame:

create access_profile ip source_ip_mask 255.255.255.0 profile_id 1

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 deny

Here we use the **profile_id 1** which was specified when the access profile was created. The **add** parameter instructs the switch to add the criteria that follows to the list of rules that are associated with access profile 1. For each rule entered into the access profile, you can assign an **access_id** that both identifies the rule and establishes a priority within the list of rules. A lower **access_id** gives the rule a higher priority.

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.

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

NOTE: As a stand-alone switch or as a master switch in a switch stack, the switch number will be referred to as 15 for all configurations, graphs and tables.

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> | flag_mask [all | {urg | ack | psh | rst | syn | fin}]} | udp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | protocol_id {user_mask <hex 0x0-0xffffffff>}]} | packet_content_mask {offset_0-15 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_16-31 <hex0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_32-47 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_48-63 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_64-79 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff>}] {port [<portlist> | all]} [profile_id <value 1-255>]**
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

create access_profile

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

Parameters

ethernet – Specifies that the switch will examine the layer 2 part of each packet header.

- *vlan* – Specifies that the switch will examine the VLAN part of each packet header.
- *source_mac <macmask>* – Specifies a MAC address mask for the source MAC address. This mask is entered in the following hexadecimal format:
- *destination_mac <macmask>* – Specifies a MAC address mask for the destination MAC address.
- *802.1p* – Specifies that the switch will examine the 802.1p priority value in the frame's header.
- *ethernet_type* – Specifies that the switch will examine the Ethernet type value in each frame's header.

ip – Specifies that the switch will examine the IP address in each frame's header.

- *vlan* – Specifies a VLAN mask.
- *source_ip_mask <netmask>* – Specifies an IP address mask for the source IP address.
- *destination_ip_mask <netmask>* – Specifies an IP address mask for the destination IP address.
- *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.

create access_profile	
	• *flag_mask [all | {urg | ack | psh | rst | syn | fin}]* – Enter the appropriate flag_mask parameter. All incoming packets have TCP port numbers contained in them as the forwarding criterion. These numbers have flag bits associated with them which are parts of a packet that determine what to do with the packet. The user may deny packets by denying certain flag bits within the packets. The user may choose between **all**, **urg** (urgent), **ack** (acknowledgement), **psh** (push), **rst** (reset), **syn** (synchronize) and **fin** (finish). • *udp* – Specifies that the switch will examine each frame's Universal Datagram Protocol (UDP) field. • *src_port_mask <hex 0x0-0xffff>* – Specifies a UDP port mask for the source port. • *dst_port_mask <hex 0x0-0xffff>* – Specifies a UDP port mask for the destination port. • *protocol_id* – Specifies that the switch will examine each frame's Protocol ID field. • *user_define_mask <hex 0x0-0xffffffff>* – Specifies that the rule applies to the IP protocol ID and the mask options behind the IP header. • *packet_content_mask* – Specifies that the switch will mask the packet header beginning with the offset value specified as follows: • *offset_0-15* – Enter a value in hex form to mask the packet from the beginning of the packet to the 16th byte. • *offset_16-31* - Enter a value in hex form to mask the packet from byte 16 to byte 31. • *offset_32-47* - Enter a value in hex form to mask the packet from byte 32 to byte 47. • *offset_48-63* - Enter a value in hex form to mask the packet from byte 48 to byte 63. • *offset_64-79* - Enter a value in hex form to mask the packet from byte 64 to byte 79. *port <portlist>* - Specifies a port or range of ports to be configured. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3-2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. *all* – denotes all ports on the switch. *profile_id <value 1-255>* – Specifies an index number that will identify the access profile being created with this command.
Restrictions	Only administrator-level users can issue this command.

Example usage:

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

```
DGS-3312SR:4#create access_profile ip vlan source_ip_mask 20.0.0.0
destination_ip_mask 10.0.0.0 dscp icmp type code permit profile_id 101

Command: create access_profile ip vlan source_ip_mask 20.0.0.0
destination_ip_mask 10.0.0.0 dscp icmp type code permit profile_id 101


Success.


DGS-3312SR
```

delete access_profile

Purpose	Used to delete a previously created access profile.
Syntax	**delete access_profile [profile_id <value 1-255>]**
Description	The **delete access_profile** command is used to delete a previously created access profile on the switch.
Parameters	*profile_id <value 1-255>* – Enter 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-3312SR:4# delete access_profile profile_id 1

Command: delete access_profile profile_id 1


Success.


DGS-3312SR: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	**<value 1-255>[add access_id <value 1-255> [ethernet {vlan <vlan_name 32> | source_mac <macaddr> | destination_mac <macaddr> | 802.1p <value 0-7> | ethernet_type <hex 0x0-0xffff> [permit {priority <value 0-7> {replace_priority }} | deny] | ip {vlan <vlan_name 32> | source_ip <ipaddr> | destination_ip <ipaddr> | dscp <value 0-63> | [icmp {type <value 0-255> code <value 0-255>} | igmp {type <value 0-255>} | tcp {src_port <value 0-65535>**

config access_profile

	| dst_port <value 0-65535> | flag_mask [all | {urg | ack | psh | rst | syn | fin}]} | udp {src_port <value 0-65535> | dst_port <value 0-65535>} | protocol_id <value 0 - 255> {user_define <hex 0x0-0xffffffff>}]} [permit {priority <value 0-7> {replace_priority }} | deny] | packet_content {offset_0-15 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_16-31 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_32-47 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_48-63 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_64-79 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff>}] [permit {priority <value 0-7> {replace_priority} | deny] | delete access_id <value 1-255>]
Description	The **config access_profile** command is used to configure an access profile on the switch and to enter specific values that will be combined, using a logical AND operation, with masks entered with the **create access_profile** command, above.
Parameters	*profile_id <value 1-255>* – Enter 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. *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. The 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 hexadecimal 802.1Q Ethernet type value in the packet header. *ip* – Specifies that the switch will look into the IP fields in each packet. • *vlan <vlan_name 32>* – Specifies that the access profile will apply to only to this VLAN. • *source_ip <ipaddr>* – Specifies that the access profile will apply to only packets with this source IP address. • *destination_ip <ipaddr>* – Specifies that the access profile will apply to only packets with this destination IP address.

config access_profile

- *dscp* <*value 0-63*> – Specifies that the access profile will apply only to packets that have this value in their Type-of-Service (DiffServ code point, DSCP) field in their IP packet header.
- *icmp* – Specifies that the switch will examine the Internet Control Message Protocol (ICMP) field within each packet.
  - *type* <*value 0-255*> – Specifies that the access profile will apply to this ICMP type value.
  - *code* <*value 0-255*> – Specifies that the access profile will apply to this ICMP code.
- *igmp* – Specifies that the switch will examine the Internet Group Management Protocol (IGMP) field within each packet.
  - *type* <*value 0-255*> – Specifies that the access profile will apply to packets that have this IGMP type value.
- *tcp* – Specifies that the switch will examine the Transmission Control Protocol (TCP) field within each packet.
  - *src_port* <*value 0-65535*> – Specifies that the access profile will apply only to packets that have this TCP source port in their TCP header.
  - *dst_port* <*value 0-65535*> – Specifies that the access profile will apply only to packets that have this TCP destination port in their TCP header.
- *flag_mask* – Enter the type of TCP flag to be masked. The choices are:
  - *urg*: TCP control flag (urgent)
  - *ack*: TCP control flag (acknowledgement)
  - *psh*: TCP control flag (push)
  - *rst*: TCP control flag (reset)
  - *syn*: TCP control flag (synchronize)
  - *fin*: TCP control flag (finish)
- *udp* – Specifies that the switch will examine the Universal Datagram Protocol (UDP) field in each packet.
  - *src_port* <*value 0-65535*> – Specifies that the access profile will apply only to packets that have this UDP source port in their header.
  - *dst_port* <*value 0-65535*> – Specifies that the access profile will apply only to packets that have this UDP destination port in their header.

protocol_id <*value 0-255*> – Specifies that the switch will examine the Protocol field in each packet and if this field contains the value entered here, apply the following rules.

config access_profile	
	user_define <hex 0x0-0xffffffff> – Specifies a mask to be combined with the value found in the frame header using a logical AND operation. • *packet_content* – Specifies that the switch will mask the packet header beginning with the offset value specified as follows: • *offset_0-15* – Enter a value in hex form to mask the packet from the beginning of the packet to the 15th byte. • *offset_16-31* - Enter a value in hex form to mask the packet from byte 16 to byte 32. • *offset_32-47* - Enter a value in hex form to mask the packet from byte 32 to byte 47. • *offset_48-63* - Enter a value in hex form to mask the packet from byte 48 to byte 63. • *offset_64-79* - Enter a value in hex form to mask the packet from byte 64 to byte 79. *permit* – Specifies that packets that match the access profile are permitted to be forwarded by the Switch. • *priority <value 0-7>* – Specify the 802.1p priority value included in the packet that will be forwarded by the Switch. Only packets that have this priority value will be permitted. • *{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 with <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. *deny* – Specifies that packets that do not match the access profile are not permitted to be forwarded by the Switch and will be filtered. *delete access_id <value 1-255>* – Specifies the access ID of a rule to delete.
Restrictions	Only administrator-level users can issue this command.

Example usage:

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

```
DGS-3312SR:4# config access_profile profile_id 2 add access_id 1 ip
source_ip 10.42.73.1 deny
Command: config access_profile profile_id 1 add access_id 1 ip
source_ip 10.42.73.1 deny

Success.

DGS-3312SR:4#
```

show access_profile	
Purpose	Used to display the currently configured access profiles on the switch.
Syntax	**show access_profile {profile_id <value 1-255>}**
Description	The **show access_profile** command is used to display the currently configured access profiles
Parameters	*profile_id <value 1-255>* - Enter this parameter, along with the appropriate value between 1 and 255, to view a specific access profile. Entering this command without a parameter will display all access profiles currently set on the switch.
Restrictions	Only administrator-level users can issue this command.

Example usage:

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

```
DGS-3312SR:4#show access_profile
Command: show access_profile

Access Profile Table

Access Profile ID: 2
TYPE : Ethernet Frame Filter
Ports: 1:1
Masks : VLAN              802.1P
--------------------------------  -------------

ID   Mode
----  ---------  --------------  -------------
3     Permit  0              0-x

DGS-3312SR:4#
```

26

TRAFFIC SEGMENTATION COMMANDS

Traffic segmentation allows you to further sub-divide VLANs into smaller groups of ports that will help to reduce traffic on the VLAN. The VLAN rules take precedence, and then the traffic segmentation rules are applied. The traffic segmentation commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

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

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

NOTE: As a stand-alone switch or as a master switch in a switch stack, the switch number will be referred to as 15 for all configurations, graphs and tables.

config traffic_segmentation

Purpose	Used to configure traffic segmentation on the switch.
Syntax	**config traffic_segmentation <portlist> forward_list [null | <portlist>]**
Description	The **config traffic_segmentation** command is used to configure traffic segmentation on the switch.
Parameters	*<portlist>* – Specifies a range of ports that will be configured for traffic segmentation. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3-2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. *forward_list* – Specifies a range of ports that will receive forwarded frames from the ports specified in the portlist, above. *null* – no ports are specified *<portlist>* – Specifies a range of ports for the forwarding list. This list must be on the same switch previously specified for traffic segmentation (i.e. following the *<portlist>* specified above for config traffic_segmentation).
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure ports 1 through 9 to be able to forward frames to port 10 through 12:

```
DGS-3312SR:4# config traffic_segmentation 1:1-1:9 forward_list 1:10-1:12
Command: config traffic_segmentation 1:1-1:9 forward_list 1:10-1:12

Note:  If a port in forward_list belongs to a different slave form
source_port, all ports on the slave will be added in forward_list.

Success.

DGS-3312SR:4#
```

show traffic_segmentation

Purpose	Used to display the current traffic segmentation configuration on the switch.
Syntax	**show traffic_segmentation <portlist>**
Description	The **show traffic_segmentation** command is used to display the current traffic segmentation configuration on the switch.
Parameters	<*portlist*> – Specifies a range of ports for which the current traffic segmentation configuration on the switch will be displayed. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3-2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order.
Restrictions	The port lists for segmentation and the forward list must be on the same switch.

Example usage:

To display the current traffic segmentation configuration on the switch.

```
DGS-3312SR:4#show traffic_segmentation 1:1-1:12
Command: show traffic_segmentation 1:1-1:12

Traffic Segmentation Table

Port  Forward Portlist
----  ----------------------------
1:1   1:1-1:12,2:1-2:12
1:2   1:1-1:12,2:1-2:12
1:3   1:1-1:12,2:1-2:12
1:4   1:1-1:12,2:1-2:12
1:5   1:1-1:12,2:1-2:12
1:6   1:1-1:12,2:1-2:12
1:7   1:1-1:12,2:1-2:12
1:8   1:1-1:12,2:1-2:12
1:9   1:1-1:12,2:1-2:12
1:10  1:1-1:12,2:1-2:12
1:11  1:1-1:12,2:1-2:12
1:12  1:1-1:12,2:1-2:12

DGS-3312SR:4#
```

27

STACKING COMMANDS

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

Command	Parameters
config stacking mode	[disable {ports [<portlist> | <int>]} | enable {ports [<portlist> | <int>]}]
show stacking	mode

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

NOTE: As a stand-alone switch or as a master switch in a switch stack, the switch number will be referred to as 15 for all configurations, graphs and tables.

config stacking mode

Purpose	Used to configure the stacking mode.
Syntax	**config stacking mode [disable {ports [<portlist>]} | enable {ports [<portlist>]}]**
Description	This command is used to configure the stacking function for the switch by enabling or disabling stacking, along with a list of ports.
Parameters	*disable* - To disable the switch to function in a stacked group. The user may disable this stacking function by port, by adding the *ports* parameter along with the appropriate port to be disabled. ▪ *<portlist>* - Specifies a range of ports for which the stacking mode on the switch will be enabled. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3-2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. *enable* – To enable the switch to function in a stacked group. The user may employ this stacking function by port, by adding the *ports* parameter along with the appropriate port to be enabled. ▪ *<portlist>* - Specifies a range of ports for which the stacking mode on the switch will be enabled. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3-2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order.
Restrictions	Only administrator-level users can issue this command.

Usage Example

To globally enable stacking:

```
DGS-3312SR:4#config stacking mode enable

Command: config stacking mode enable


The new stacking mode configuration must be saved and the system
restarted to put the new settings into effect.

If you do not save the changes now,they will be lost.


Do you want to save the new system configuration to NV-RAM and restart
now?(y/n)
```

It is necessary to save the stacking mode settings and restart the system. If you want to save and restart press Y. It will take a few minutes for the system to reboot.

It is also possible to use any of the built-in combination ports for stacking. Follow the example below to enable stacking for a built-in port.

To configure built-n port number 4 to function as a stacking port:

```
DGS-3312SR:4#config stacking mode enable ports 4

Command: config stacking mode enable ports 4


The new stacking mode configuration must be saved and the system
restarted to put the new settings into effect.

If you do not save the changes now, they will be lost.


Do you want to save the new system configuration to NV-RAM and
restart now?(y/n)


Success.


DGS-3312SR:4#
```

It is necessary to save the stacking mode settings and restart the system. If you want to save and restart press Y. It will take a few minutes for the system to reboot.

show stacking

Purpose	Used to display the current stacking mode.
Syntax	**show stacking {mode}**
Description	This command will display the current stacking configurations, and mode, if specified.
Parameters	*mode* – Displays the current stacking mode.
Restrictions	None.

Usage Example:

To show stacking:

```
DGS-3312SR:4#show stacking
Command: show stacking

ID   MAC Address         Port Range  Mode      Version    RPS Status   Model Name
---  ------------------- ----------  ----------  --------  -----------  ---------
*15  00-01-02-03-04-00   1 - 12      MASTER    3.00-B12   Not Present  DGS-3312SR
*2   01-02-03-04-05-00   1 - 12      SLAVE     4.02-B03   Not Present  DES-3226S

Total Entries :1

DGS-3312SR:4#
```

To show stacking mode:

```
DGS-3312SR:4#show stacking mode
Command: show stacking mode

Stacking Topology : Disable
Setting           : STANDALONE
Current           : STANDALONE

DGS-3312SR:4#
```

28

D-LINK SINGLE IP MANAGEMENT COMMANDS

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

- SIM is an optional feature on the switch and can easily be enabled or disabled. SIM grouping has no effect on the normal operation of the switch in the user's network.
- There are three classifications for switches using SIM. The **Commander Switch (CS)**, which is the master switch of the group, **Member Switch (MS)**, which is a switch that is recognized by the CS a member of a SIM group, and a **Candidate Switch (CaS)**, which is a switch that has a physical link to the SIM group but has not been recognized by the CS as a member of the SIM group.
- A SIM group can only have one Commander Switch (CS).
- All switches in a particular SIM group must be in the same IP subnet (broadcast domain). Members of a SIM group cannot cross a router.
- A SIM group accepts up to 32 switches (numbered 0-31), including the Commander Switch (numbered 0).
- There is no limit to the number of SIM groups in the same IP subnet (broadcast domain), however a single switch can only belong to one group.
- If multiple VLANs are configured, the SIM group will only utilize the default VLAN on any switch.
- SIM allows intermediate devices that do not support SIM. This enables the user to manage a switch that is more than one hop away from the CS.

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

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

- It has an IP Address.
- It is not a command switch or member switch of another Single IP group.
- It is connected to the member switches through its management VLAN.

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

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

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

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

The following rules also apply to the above roles:

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

6. The CaS can be configured through the CS to become a MS.

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

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

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

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

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

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

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

Example usage:

To enable SIM on the switch:

```
DGS-3312SR:4#enable sim
Command: enable sim

Success.

DGS-3312SR:4#
```

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

Example usage:

To disable SIM on the switch:

```
DGS-3312SR:4#disable sim
Command: disable sim

Success.

DGS-3312SR:4#
```

show sim	
Purpose	Used to view the current information regarding the SIM group on the switch.
Syntax	**show sim {[candidates {<candidate_id 1-32>} | members {<member_id 1-32>} | group {commander_mac <macaddr>} neighbor]}**
Description	This command will display the current information regarding the SIM group on the switch, including the following: SIM Version - Displays the current Single IP Management version on the switch. Firmware Version - Displays the current Firmware version on the switch. Device Name - Displays the user-defined device name on the switch. MAC Address - Displays the MAC Address of the switch. Capabilities – Displays the type of switch, be it Layer 2 (L2) or Layer 3 (L3). Platform – Switch Description including name and model number. SIM State –Displays the current Single IP Management State of the switch, whether it be enabled or disabled. Role State – Displays the current role the switch is taking, including Commander, Member or Candidate. A stand-alone switch will always have the candidate role. Discovery Interval - Time in seconds the switch will send discovery packets out over the network. Hold time – Displays the time in seconds the switch will hold discovery results before dropping it or utilizing it.
Parameters	*candidates <candidate_id 1-32>* - Entering this parameter will display information concerning candidates of the SIM group. To view a specific candidate, include that candidate's ID number, listed from 1 to 32.

show sim	
	members <member_id 1-32> - Entering this parameter will display information concerning members of the SIM group. To view a specific member, include that member's id number, listed from 1 to 32. *group commander_mac <macaddr>* - Entering this parameter will display information concerning the SIM group of a commander device, identified by its MAC address. *neighbor* – Entering this parameter will display neighboring devices of the switch. A SIM neighbor is defined as a switch that is physically connected to the switch but is not part of the SIM group. This screen will produce the following results: ▪ Port – Displays the physical port number of the commander switch where the uplink to the neighbor switch is located. ▪ MAC Address – Displays the MAC Address of the neighbor switch. ▪ Role – Displays the role (CS, CaS, MS) of the neighbor switch.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To show the SIM information in detail:

```
DGS-3312SR:4#show sim
Command: show sim

SIM Version          : VER-1
Firmware Version     : Build 2.00-B17
Device Name          :
MAC Address          : 00-35-26-11-11-00
Capabilities         : L3
Platform             : DGS-3312SR L3 Switch
SIM State            : Enabled
Role State           : Commander
Discovery Interval   : 30 sec
Hold Time            : 100 sec

DGS-3312SR:4#
```

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

```
DGS-3312SR:4#show sim candidates
Command: show sim candidates

ID   MAC Address        Platform /              Hold   Firmware   Device Name
                        Capability              Time   Version
---  -----------------  ----------------------  -----  ---------  ----------------
1    00-01-02-03-04-00  DGS-3212SR L2 Switch    40     3.00-B09   The Man
2    00-55-55-00-55-00  DGS-3212SR L2 Switch    140    3.00-B09   default master

Total Entries: 2

DGS-3312SR:4#
```

To show the member information in summary, if the member id is specified:

```
DGS-3312SR:4#show sim member
Command: show sim  member

ID  MAC Address        Platform /                 Hold    Firmware   Device Name
                       Capability                 Time    Version
---  -----------------  ------------------------  ----    ---------  ----------------
1   00-01-04-03-04-00  DGS-3212SR L2 Switch      40      3.00-B09   The Man
2   00-55-35-00-55-00  DGS-3212SR L2 Switch      140     3.00-B09   default master

Total Entries: 2

DGS-3312SR:4#
```

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

```
DGS-3312SR:4#show sim group
Command: show sim group

SIM Group Name : default

ID  MAC Address        Platform /                 Hold   Firmware   Device Name
                       Capability                 Time   Version
---  -----------------  ------------------------  -----  ---------  ----------------
*1  00-01-02-03-04-00  DGS-3212SR L2 Switch      40     3.00-B09   Trinity

SIM Group Name : default

ID  MAC Address        Platform /                 Hold   Firmware   Device Name
                       Capability                 Time   Version
---  -----------------  ------------------------  -----  ---------  ----------------
 2  00-55-55-00-55-00  DGS-3212SR L2 Switch      140    3.00-B09   Enrico

SIM Group Name : SIM2

ID  MAC Address        Platform /                 Hold   Firmware   Device Name
                       Capability                 Time   Version
---  -----------------  ------------------------  ------  ---------  ----------------
*1  00-01-02-03-04-00  DGS-3212SR L2 Switch      40     3.00-B09   Neo
 2  00-55-55-00-55-00  DGS-3212SR L2 Switch      140    3.00-B09   default master

'*' means commander switch.

DGS-3312SR:4#
```

Example usage:

To view SIM neighbors:

```
DGS-3312SR:4#show sim neighbor
Command: show sim neighbor

Neighbor Info Table

Port   MAC Address        Role
------  ------------------------  ---------
23     00-35-26-00-11-99  Commander
23     00-35-26-00-11-91  Member
24     00-35-26-00-11-90  Candidate

Total Entries: 3
```

```
DGS-3312SR:4#
```

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

Example usage:

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

```
DGS-3312SR:4#reconfig member_id 2
Command: reconfig member_id 2


DGS-3312SR:4#
Login:
```

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

Example usage:

To add a member:

```
DGS-3312SR:4#config sim_group add 2
Command: config sim_group add 2

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

Success.

DGS-3312SR:4#
```

To delete a member:

```
DGS-3312SR:4#config sim delete 1
Command: config sim delete 1

Please wait for ACK...

Success.

DGS-3312SR:4#
```

config sim

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

config sim	
	interval from 30 to 90 seconds. ▪ *hold time <sec 100-255>*– Using this parameter, the user may set the time, in seconds, the switch will hold information sent to it from other switches, utilizing the discovery interval protocol. The user may set the hold time from 100 to 300 seconds.
Restrictions	Only administrator-level users can issue this command.

To change the time interval of the discovery protocol:

```
DGS-3312SR:4#config sim commander dp_interval 30
Command:config sim commander dp_interval 30

Success.

DGS-3312SR:4#
```

To change the hold time of the discovery protocol:

```
DGS-3312SR:4# config sim commander hold_time 120
Command: config sim commander hold_time 120

Success.

DGS-3312SR:4#
```

To transfer the switch to be a commander:

```
DGS-3312SR:4#config sim commander
Command: config sim commander

Success.

DGS-3312SR:4#
```

To update the name of a group:

```
DGS-3312SR:4#config sim commander group_name Trinity
Command: config sim commander group_name Trinity

Success.

DGS-3312SR:4#
```

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

Example usage:

To download firmware:

```
DGS-3312SR:4# download sim_ms firmware 10.53.13.94
c:/dgssri.had members all
Command: download sim_ms firmware 10.53.13.94 c:/dgssri.had
members all

This device is updating firmware.  Please wait...

Download Status :

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

DGS-3312SR:4#
```

To download configuration files:

```
DGS-3312SR:4#download sim_ms configuration 10.53.13.94
c:/dgssri.txt members all
Command: download sim_ms configuration 10.53.13.94
c:/dgssri.txt members all

This device is updating configuration.  Please wait...

Download Status :

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

DGS-3312SR:4#
```

upload sim_ms

Purpose	User to upload a configuration file to a TFTP server from a specified member of a SIM group.
Syntax	**upload sim_ms [configuration] <ipaddr> <path_filename> <member_id 1-32>**
Description	This command will upload a configuration file to a TFTP server from a specified member of a SIM group.
Parameters	*<ipaddr>* Enter the IP address of the TFTP server the user wishes to upload a configuration file to. *<path_filename>* – Enter a user-defined path and file name on the TFTP server the user wishes to upload configuration files to. *<member_id 1-32>* Enter this parameter to specify the member the user prefers to upload a switch configuration file to. The user may specify a member or members by adding the ID number of the specified member.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To upload configuration files to a TFTP server:

```
DGS-3312SR:4#upload sim_ms configuration 10.55.47.1 D:\configuration.txt 1
Command: upload sim_ms configuration 10.55.47.1 D:\configuration.txt 1

Success.

DGS-3312SR:4#
```

29

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

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

config sntp

Purpose	Used to setup SNTP service.
Syntax	**config sntp {primary <ipaddr> | secondary <ipaddr> | poll-interval <int 30-99999>}**
Description	Use this command to configure SNTP service from an SNTP server. SNTP must be enabled for this command to function (See enable sntp).
Parameters	*primary* – This is the primary server the SNTP information will be taken from. ▪ <*ipaddr*> – The IP address of the primary server. *secondary* – This is the secondary server the SNTP information will be taken from in the event the primary server is unavailable. ▪ <*ipaddr*> – The IP address for the secondary server. *poll-interval <int 30-99999>* – This is the interval between requests for updated SNTP information. The polling interval ranges from 30 to 99,999 seconds.
Restrictions	Only administrator-level users can issue this command. SNTP service must be enabled for this command to function (enable sntp).

Example usage:

To configure SNTP settings:

```
DGS-3312SR:4#config sntp primary 10.1.1.1 secondary 10.1.1.2 poll-interval 30
Command: config sntp primary 10.1.1.1 secondary 10.1.1.2 poll-interval 30

Success.

DGS-3312SR:4#
```

show sntp

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

Example usage:

To display SNTP configuration information:

```
DGS-3312SR:4#show sntp
Command: show sntp

Current Time Source  : System Clock
SNTP : Disabled
SNTP Primary Server     : 10.1.1.1
SNTP Secondary Server : 10.1.1.2
SNTP Poll Interval    : 720 sec


DGS-3312SR:4#
```

enable sntp

Purpose	Enables SNTP server support.
Syntax	**enable sntp**
Description	This will enable SNTP support. SNTP service must be separately configured (see **config sntp**).Enabling and configuring SNTP support will override any manually configured system time settings.
Parameters	None.
Restrictions	Only administrator-level users can issue this command. SNTP settings must be configured for SNTP to function (config sntp).

Example usage:

To enable the SNTP function:

```
DGS-3312SR:4#enable sntp
Command: enable sntp

Success.

DGS-3312SR:4#
```

disable sntp

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

Example:

To stop SNTP support:

```
DGS-3312SR:4#disable sntp
Command: disable sntp

Success.

DGS-3312SR:4#
```

config time

Purpose	Used to manually configure system time and date settings.
Syntax	**config time date <date ddmmmyyyy> <time hh:mm:ss>**
Description	This will configure the system time and date settings. These will be overridden if SNTP is configured and enabled.
Parameters	*date* – Express the date using two numerical characters for the day of the month, three alphabetical characters for the name of the month, and four numerical characters for the year. For example: 03aug2003. *time* – Express the system time using the format hh:mm:ss, that is, two numerical characters each for the hour using a 24-hour clock, the minute and second. For example: 19:42:30.
Restrictions	Only administrator-level users can issue this command. Manually configured system time and date settings are overridden if SNTP support is enabled.

Example usage:

To manually set system time and date settings:

```
DGS-3312SR:4#config time 30jun2003 16:30:30
Command: config time 30jun2003 16:30:30

Success.

DGS-3312SR:4#
```

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

Example usage:

To configure time zone settings:

```
DGS-3312SR:4#config time_zone operator + hour 2 min 30
Command: config time_zone operator + hour 2 min 30

Success.

DGS-3312SR:4#
```

config dst	
Purpose	Used to enable and configure time adjustments to allow for the use of Daylight Savings Time (DST).
Syntax	**config dst [disable | repeating {s_week <start_week 1-4,last> | s_day <start_day sun-sat>| s_mth <start_mth 1-12> | s_time <start_time hh:mm> | e_week <end_week 1-4,last> | e-day <end_day sun-sat> | e_mth <end_mth 1-12> | e_time <end_time hh:mm> | offset [30 | 60 | 90 | 120]} | annual {s_date <start_date 1-31> | s_mth <start_mth 1-12> | s_time <start_time hh:mm> | e_date <end_date 1-31> | e_mth <end_mth 1-12> | e_time <end_time hh:mm> | offset [30 | 60 | 90 | 120]}]**
Description	DST can be enabled and configured using this command. When enabled this will adjust the system clock to comply with any DST requirement. DST adjustment effects system time for both manually configured time and time set using SNTP service.

config dst

Parameters

disable – Disable the DST seasonal time adjustment for the Switch.

repeating - Using repeating mode will enable DST seasonal time adjustment. Repeating mode requires that the DST beginning and ending date be specified using a formula. For example, specify to begin DST on Saturday during the second week of April and end DST on Sunday during the last week of October.

annual - Using annual mode will enable DST seasonal time adjustment. Annual mode requires that the DST beginning and ending date be specified concisely. For example, specify to begin DST on April 3 and end DST on October 14.

s_week - Configure the week of the month in which DST begins.

- <*start_week 1-4,last*> - The number of the week during the month in which DST begins where 1 is the first week, 2 is the second week and so on, last is the last week of the month.

e_week - Configure the week of the month in which DST ends.

- <*end_week 1-4,last*> - The number of the week during the month in which DST ends where 1 is the first week, 2 is the second week and so on, last is the last week of the month.

s_day – Configure the day of the week in which DST begins.

- <*start_day sun-sat*> - The day of the week in which DST begins expressed using a three character abbreviation (sun, mon, tue, wed, thu, fri, sat)

e_day - Configure the day of the week in which DST ends.

- <*end_day sun-sat*> - The day of the week in which DST ends expressed using a three character abbreviation (sun, mon, tue, wed, thu, fri, sat)

s_mth - Configure the month in which DST begins.

- <*start_mth 1-12*> - The month to begin DST expressed as a number.

e_mth - Configure the month in which DST ends.

- <*end_mth 1-12*> - The month to end DST expressed as a number.

s_time – Configure the time of day to begin DST.

- <*start_time hh:mm*> - Time is expressed using a 24-hour clock, in hours and minutes.

e_time - Configure the time of day to end DST.

- <*end_time hh:mm*> - Time is expressed using a 24-hour clock, in hours and minutes.

s_date - Configure the specific date (day of the month) to begin DST.

- <*start_date 1-31*> - The start date is expressed numerically.

e_date - Configure the specific date (day of the month) to begin DST.

- <*end_date 1-31*> - The end date is expressed numerically.

offset [30 | *60* | *90* | *120]* - Indicates number of minutes to add or to subtract during the summertime. The possible offset times are 30,60,90,120. The default value is 60.

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

Example usage:

To configure daylight savings time on the switch:

```
DGS-3312SR:4#config dst repeating s_week 2 s_day tue s_mth 4
s_time 15:00 e_week 2 e_day wed e_mth 10 e_time 15:30 offset 30

Command: config dst repeating s_week 2 s_day tue s_mth 4 s_time
15:00 e_week 2 e_day wed e_mth 10 e_time 15:30 offset 30


Success.


DGS-3312SR:4#
```

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

Example usage:

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

```
DGS-3312SR:4#show time
Command: show time


Current Time Source     : System Clock
Current Time            : 10 Jul 2003 01:43:41
Time Zone               : GMT +02:30
Daylight Saving Time    : Repeating
Offset in Minutes       : 60
  Repeating From        : Apr 2nd Tue 15:00
            To          : Oct 2nd Wed 15:30
  Annual    From        : 29 Apr 00:00
            To          : 012 Oct 00:00


DGS-3312SR:4#
```

30

ARP COMMANDS

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

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

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

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

Example Usage:

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

```
DGS-3312SR:4#create arpentry 10.48.74.121 00-50-BA-00-07-36
Command: create arpentry 10.48.74.121 00-50-BA-00-07-36

Success.

DGS-3312SR:4#
```

delete arpentry	
Purpose	Used to delete a static entry into the ARP table.
Syntax	**delete arpentry {<ipaddr> | all}**
Description	This command is used to delete a static ARP entry, made using the **create arpentry** command above, by specifying either the IP address of the entry or all. Specifying *all* clears the switch's ARP table.
Parameters	<*ipaddr*> – The IP address of the end node or station.

delete arpentry	
	all – Deletes all ARP entries.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

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

```
DGS-3312SR:4#delete arpentry 10.48.74.121
Command: delete arpentry 10.48.74.121

Success.

DGS-3312SR:4#
```

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 an ARP entry can remain in the switch's ARP table, without being accessed, before it is dropped from the table.
Parameters	*time <value 0-65535>* – The ARP age-out time, in minutes. The value may be set in the range of 0-65535 minutes with a default setting of 20 minutes.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To configure ARP aging time:

```
DGS-3312SR:4#config arp_aging time 30
Command: config arp_aging time 30

Success.

DGS-3312SR:4#
```

show arpentry	
Purpose	Used to display the ARP table.
Syntax	**show arpentry {ipif <ipif_name 12> | ipaddress <ipaddr> | static}**

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

Example Usage:

To display the ARP table**:**

```
DGS-3312SR: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          10.1.1.169      00-50-BA-70-E4-4E   Dynamic
System          10.1.1.254      00-01-30-FA-5F-00   Dynamic
System          10.9.68.1       00-A0-C9-A4-22-5B   Dynamic
System          10.9.68.4       00-80-C8-2E-C7-45   Dynamic
System          10.10.27.51     00-80-C8-48-DF-AB   Dynamic
System          10.11.22.145    00-80-C8-93-05-6B   Dynamic
System          10.11.94.10     00-10-83-F9-37-6E   Dynamic
System          10.14.82.24     00-50-BA-90-37-10   Dynamic
System          10.15.1.60      00-80-C8-17-42-55   Dynamic
System          10.17.42.153    00-80-C8-4D-4E-0A   Dynamic
System          10.19.72.100    00-50-BA-38-7D-5E   Dynamic
System          10.21.32.203    00-80-C8-40-C1-06   Dynamic
System          10.40.44.60     00-50-BA-6B-2A-1E   Dynamic
System          10.42.73.221    00-01-02-03-04-00   Dynamic
System          10.44.67.1      00-50-BA-DA-02-51   Dynamic
System          10.47.65.25     00-50-BA-DA-03-2B   Dynamic
System          10.50.8.7       00-E0-18-45-C7-28   Dynamic
System          10.90.90.90     00-01-02-03-04-00   Local
System          10.255.255.255  FF-FF-FF-FF-FF-FF   Local/Broadcast

Total Entries = 20

DGS-3312SR:4#
```

clear arptable	
Purpose	Used to remove all dynamic ARP table entries.
Syntax	**clear arptable**
Description	This command is used to remove dynamic ARP table entries from the switch's ARP table. Static ARP table entries are not affected.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To remove dynamic entries in the ARP table:

```
DGS-3312SR:4#clear arptable
Command: clear arptable

Success.

DGS-3312SR:4#
```

31

VRRP COMMANDS

VRRP or *Virtual Routing Redundancy Protocol* is a function on the switch that dynamically assigns responsibility for a virtual router to one of the VRRP routers on a LAN. The VRRP router that controls the IP address associated with a virtual router is called the Master, and will forward packets sent to this IP address. This will allow any Virtual Router IP address on the LAN to be used as the default first hop router by end hosts. Utilizing VRRP, the administrator can achieve a higher available default path cost without needing to configure every end host for dynamic routing or routing discovery protocols.

Statically configured default routes on the LAN are prone to a single point of failure. VRRP is designed to eliminate these failures by setting an election protocol that will assign a responsibility for a virtual router to one of the VRRP routers on the LAN. When a virtual router fails, the election protocol will select a virtual router with the highest priority to be the Master router on the LAN. This retains the link and the connection is kept alive, regardless of the point of failure.

To configure VRRP for virtual routers on the switch, an IP interface must be present on the system and it must be a part of a VLAN. VRRP IP interfaces may be assigned to every VLAN, and therefore IP interface, on the switch. VRRP routers within the same VRRP group must be consistent in configuration settings for this protocol to function optimally.

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

Command	Parameters
enable vrrp	{ping}
disable vrrp	{ping}
create vrrp ipif	<ipif_name 12> vrid <vrid 1-255> ipaddress <ipaddr> {state [enable | disable] | priority <int 1-254> | advertisement_interval <int 1-255> | preempt [true | false] | critical_ip <ipaddr> | critical_ip_state [enable | disable]}
config vrrp ipif	<ipif_name 12> | vrid <vrid 1-255> {state [enable | disable] | priority <int 1-254> | ipaddress <ipaddr> | advertisement_interval <int 1-255> | preempt [true | false] | critical_ip <ipaddr> | critical_ip_state [enable | disable]}
config vrrp ipif authtype	<ipif_name 12> [authtype [none | simple authdata <string 8> | ip authdata <string 16>]
show vrrp	{ipif <ipif_name 12> {vrid <vrid 1-255>}
delete vrrp	{ipif <ipif_name 12> {vrid <vrid 1-255>}

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

enable vrrp	
Purpose	To enable a VRRP interface configuration.
Syntax	**enable vrrp {ping}**
Description	This command will enable the VRRP interface configuration on the switch.
Parameters	*{ping}* – Adding this parameter to the command will allow the virtual IP address to be pinged from other host end nodes to verify connectivity. This will only enable the ping connectivity check function. To enable the VRRP protocol on the switch, omit this parameter. This command is disabled by default.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To enable VRRP globally on the switch:

```
DGS-3312SR:4#enable vrrp
Command: enable vrrp

Success.

DGS-3312SR:4#
```

Example usage:

To enable the virtual IP address to be pinged:

```
DGS-3312SR:4#enable vrrp ping
Command: enable vrrp ping

Success.

DGS-3312SR:4#
```

disable vrrp

Purpose	To disable a VRRP interface configuration.
Syntax	**disable vrrp {ping}**
Description	This command will disable the VRRP interface configuration on the switch.
Parameters	*{ping}* - Adding this parameter to the command will stop the virtual IP address from being pinged from other host end nodes to verify connectivity. This will only disable the ping connectivity check function. To disable the VRRP protocol on the switch, omit this parameter.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To disable the VRRP function globally on the switch:

```
DGS-3312SR:4#disable vrrp
Command: disable vrrp

Success.

DGS-3312SR:4#
```

Example usage:

To disable the virtual IP address from being pinged:

```
DGS-3312SR:4#disable vrrp ping
Command: disable vrrp ping

Success.

DGS-3312SR:4#
```

create vrrp ipif

Purpose	To create a VRRP IP interface on the switch.
Syntax	**<ipif_name 12> vrid <vrid 1-255> ipaddress <ipaddr> {state [enable | disable] | priority <int 1-254> | advertisement_interval <int 1-255> | preempt [true | false] | critical_ip <ipaddr> | critical_ip_state [enable | disable]}**
Description	This command is used to create a VRRP interface on the switch.
Parameters	*<ipif_name 12>* - Enter the name of a previously configured IP interface that you wish to create a VRRP entry for. This IP interface must be assigned to a VLAN on the switch. *vrid <vrid 1-255>* - Enter a value between *1* and *255* to uniquely identify this VRRP group on the switch. All routers participating in this group must be assigned the same *vrid* value. This value MUST be different from other VRRP groups set on the switch. *ipaddress <ipaddr>* - Enter the virtual IP address that will be assigned to the VRRP entry. This IP address is also the default gateway that will be statically assigned to end hosts and must be set for all routers that participate in this group. *state [enable | disable]* – Used to enable and disable the VRRP IP interface on the switch. *priority <int 1-254>* - Enter a value between 1 and 254 to indicate the router priority. The VRRP Priority value may determine if a higher priority VRRP router overrides a lower priority VRRP router. A higher priority will increase the probability that this router will become the Master router of the group. A lower priority will increase the probability that this router will become the backup router. VRRP routers that are assigned the same priority value will elect the highest physical IP address as the Master router. The default value is 100. (The value of 255 is reserved for the router that owns the IP address associated with the virtual router and is therefore set automatically.) *advertisement_interval <int 1-255>* - Enter a time interval value, in seconds, for sending VRRP message packets. This value must be consistent with all routers participating within the same VRRP group and is used to troubleshoot poorly configured routers. The default is 1 second. *preempt [true | false]* – This entry will determine the behavior of backup routers within the VRRP group by controlling whether a higher priority backup router will preempt a lower priority Master router. A *true* entry, along with having the backup router's priority set higher than the masters priority, will set the backup router as the Master router. A *false* entry will disable the backup router from becoming the Master router. This setting must be consistent with all routers participating within the same VRRP group. The default setting is *true*.

create vrrp ipif	
	critical_ip <ipaddr> - Enter the IP address of the physical device that will provide the most direct route to the Internet or other critical network connections from this virtual router. This must be a real IP address of a real device on the network. If the connection from the virtual router to this IP address fails, a new Master will be elected from the backup routers participating in the VRRP group. If the connection to the backup fails, this backup router cannot assume the Master router role. Different critical IP addresses may be assigned to different routers participating in the VRRP group, and can therefore define multiple routes to the Internet or other critical network connections. c*ritical_ip_state [enable* | *disable]* – This parameter is used to enable or disable the critical IP address entered above. The default is *disable*.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To create a VRRP entry:

```
DGS-3312SR:4#create vrrp ipif Darren vrid ipaddress 11.1.1.1 state enable
priority 200 advertisement_interval 1 preempt true critical_ip 10.53.13.224
critical_ip_state enable
Command: create vrrp ipif Darren vrid ipaddress 11.1.1.1 state enable
priority 200 advertisement_interval 1 preempt true critical_ip 10.53.13.224
critical_ip_state enable

Success.

DGS-3312SR:4#
```

config vrrp ipif	
Purpose	To configure a VRRP IP interface on the switch.
Syntax	**<ipif_name 12> [authtype [none | simple authdata <string 8> | ip authdata <string 16>] | vrid <vrid 1-255> {state [enable | disable] | priority <int 1-254> | ipaddress <ipaddr> | advertisement_interval <int 1-255> | preempt [true | false] | critical_ip <ipaddr> | critical_ip_state [enable | disable]}**
Description	This command is used to configure a previously configured VRRP interface on the switch.
Parameters	*<ipif_name 12>* - Enter the name of a previously configured IP interface that you wish to configure the VRRP entry for. This IP interface must be assigned to a VLAN on the switch. *vrid <vrid 1-255>* - Enter a value between *1* and *255* that uniquely identifies the VRRP group you wish to configure. All routers participating in this group must be assigned the same *vrid* value. This value MUST be different from other VRRP groups set on the switch. *state [enable* | *disable]* – Used to enable and disable the VRRP IP interface on the switch. *priority <int 1-254>* - Enter a value between 1 and 254 to indicate the

config vrrp ipif	
	router priority. The VRRP Priority value may determine if a higher priority VRRP router overrides a lower priority VRRP router. A higher priority will increase the probability that this router will become the Master router of the group. A lower priority will increase the probability that this router will become the backup router. VRRP routers that are assigned the same priority value will elect the highest physical IP address as the Master router. The default value is 100. (The value of 255 is reserved for the router that owns the IP address associated with the virtual router and is therefore set automatically.) *ipaddress <ipaddr>* - Enter the virtual IP address that will be assigned to the VRRP entry. This IP address is also the default gateway that will be statically assigned to end hosts and must be set for all routers that participate in this group. *advertisement_interval <int 1-255>* - Enter a time interval value, in seconds, for sending VRRP message packets. This value must be consistent with all routers participating within the same VRRP group and is used to troubleshoot misconfigured routers. The default is 1 second. *preempt [true | false]* – This entry will determine the behavior of backup routers within the VRRP group by controlling whether a higher priority backup router will preempt a lower priority Master router. A *true* entry, along with having the backup router's priority set higher than the masters priority, will set the backup router as the Master router. A *false* entry will disable the backup router from becoming the Master router. This setting must be consistent with all routers participating within the same VRRP group. The default setting is *true*. *critical_ip <ipaddr>* - Enter the IP address of the physical device that will provide the most direct route to the Internet or other critical network connections from this virtual router. This must be a real IP address of a real device on the network. If the connection from the virtual router to this IP address fails, a new Master will be elected from the backup routers participating in the VRRP group. If the connection to the backup fails, this backup router cannot assume the Master router role. Different critical IP addresses may be assigned to different routers participating in the VRRP group, and can therefore define multiple routes to the Internet or other critical network connections. c*ritical_ip_state [enable | disable]* – This parameter is used to enable or disable the critical IP address entered above. The default is *disable*.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure a VRRP entry:

```
DGS-3312SR:4#config vrrp ipif Trinity vrid 1 state enable priority
100 advertisement_interval 2
Command: config vrrp ipif Trinity vrid 1 state enable priority 100
advertisement_interval 2

Success.

DGS-3312SR:4#
```

config vrrp ipif authtype

Purpose	To configure the authentication type for a VRRP entry.
Syntax	**config vrrp ipif authtype <ipif_name 12> [none | simple authdata <string 8> | ip authdata <string 16>]**
Description	This command is used to set the authentication type for a VRRP entry on the switch.
Parameters	*<ipif_name 12>* - Enter the name of a previously configured IP interface that you wish to configure the VRRP entry for. This IP interface must be assigned to a VLAN on the switch. *authtype* – Specifies the type of authentication used. The authtype must be consistent with all routers participating within the VRRP group. The user may choose between: ▪ *none* – Entering this parameter indicates that VRRP protocol exchanges will not be authenticated. ▪ *simple authdata <string 8>* - This parameter, along with an alphanumeric string of no more than eight characters, to set a simple password for comparing VRRP message packets received by a router. If the two passwords are not exactly the same, the packet will be dropped. ▪ *ip authdata <string 16>* - This parameter will require the user to set an alphanumeric authentication string of no more than 16 characters to generate a MD5 message digest for authentication in comparing VRRP messages received by the router. If the two values are inconsistent, the packet will be dropped.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To set the authentication type for a VRRP entry:

```
DGS-3312SR:4#config vrrp ipif Trinity authtype simple authdata tomato
Command: config vrrp ipif Trinity authtype simple authdata tomato

Success.

DGS-3312SR:4#
```

delete vrrp	
Purpose	Used to delete a vrrp entry from the switch.
Syntax	**delete vrrp {ipif <ipif_name 12> vrid <vrid 1-255>}**
Description	This command is used to remove a VRRP router running on a local device.
Parameters	*ipif <ipif_name 12>* - Enter the name of the IP interface which holds the VRRP router to delete. *vrid <vrid 1-255>* - Enter the VRRP ID of the virtual router to be deleted.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To delete a VRRP entry:

```
DGS-3312SR:4#delete vrrp ipif Trinity vrid 2
Command: delete vrrp ipif Trinity vrid 2


Success.


DGS-3312SR:4#
```

32

ROUTING TABLE COMMANDS

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

Command	Parameters
create iproute	<network_address> <ipaddr> {<metric 1-65535>} {[primary | backup]}
create iproute default	<ipaddr> {<metric 1-65535>}
delete iproute default	
delete iproute	<network_address> <ipaddr> {[primary | backup]}
show iproute	{<network_address>} {[static | rip | ospf]}

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

create iproute	
Purpose	Used to create IP route entries to the switch's IP routing table.
Syntax	**create iproute <network_address> <ipaddr> {<metric 1-65535>} {[primary | backup]}**
Description	This command is used to create a primary and backup IP route entry to the switch's IP routing table.
Parameters	*<network_address>* – IP address and netmask of the IP interface that is the destination of the route. You can specify the address and mask information using the traditional format (for example, 10.1.2.3/255.0.0.0 or in CIDR format, 10.1.2.3/8). *<ipaddr>* – The gateway IP address for the next hop router. *<metric 1-65535>* – Allows the entry of a routing protocol metric entry, representing the number of routers between the Switch and the IP address above. The default setting is 1. *[primary | backup]* - The user may choose between *Primary* and *Backup.* If the Primary Static/Default Route fails, the Backup Route will support the entry. Please take note that the Primary and Backup entries cannot have the same Gateway.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

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

```
DGS-3312SR:4#create iproute 10.48.74.121/255.0.0.0 10.1.1.254 1
Command: create iproute 10.48.74.121/8 10.1.1.254 1

Success.

DGS-3312SR:4#
```

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

Example Usage:

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

```
DGS-3312SR:4#create iproute default 10.48.74.121 1
Command: create iproute default 10.48.74.121 1

Success.

DGS-3312SR:4#
```

delete iproute	
Purpose	Used to delete an IP route entry from the switch's IP routing table.
Syntax	**delete iproute <network_address> <ipaddr> [primary | backup]**
Description	This command will delete an existing entry from the switch's IP routing table.
Parameters	*<network_address>* – IP address and netmask of the IP interface that is the destination of the route. You can specify the address and mask information using the traditional format (for example, 10.1.2.3/255.0.0.0 or in CIDR format, 10.1.2.3/8). *<ipaddr>* – The gateway IP address for the next hop router. *[primary | backup]* – The user may choose between *Primary* and *Backup.* If the Primary Static/Default Route fails, the Backup Route will support the entry. Please take note that the Primary and Backup entries cannot have the same Gateway.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To delete a backup static address 10.48.75.121, mask 255.0.0.0 and gateway (ipaddr) entry of 10.1.1.254 from the routing table:

```
DGS-3312SR:4#delete iproute 10.48.74.121/8 10.1.1.254
Command: delete iproute 10.48.74.121/8 10.1.1.254

Success.

DGS-3312SR:4#
```

delete iproute default

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

Example usage:

To delete the default IP route 10.53.13.254:

```
DGS-3312SR:4#delete iproute default
Command: delete iproute default

Success.

DGS-3312SR:4#
```

show iproute

Purpose	Used to display the switch's current IP routing table.
Syntax	**show iproute {<network_address>} {[static | rip | ospf]}**
Description	This command will display the switch's current IP routing table.
Parameters	*<network_address>* – IP address and netmask of the IP interface that is the destination of the route. You can specify the address and mask information using the traditional format (for example, 10.1.2.3/255.0.0.0 or in CIDR format, 10.1.2.3/8). *static* – Use this parameter to display static iproute entries. *rip* – Use this parameter to display RIP iproute entries. *ospf* – Use this parameter to display OSPF iproute entries.
Restrictions	None.

Example Usage:

To display the contents of the IP routing table:

```
DGS-3312SR:4#show iproute
Command: show iproute

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

Total Entries: 2

DGS-3312SR:4#
```

33

ROUTE REDISTRIBUTION COMMANDS

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

Command	Parameters
create route redistribute dst ospf src	[static | rip | local] {mettype [1 | 2] |metric <value>}
create route redistribute dst rip src	[local | static | ospf {all | internal | external | type_1 | type_2 | inter+e1 | inter+e2}] {metric <value>}
config route redistribute dst ospf src	[static | rip | local] {mettype [1 | 2] |metric <value>}
config route redistribute dst rip src	[local | static | ospf {all | internal | external | type_1 | type_2 | inter+e1 | inter+e2}] {metric <value>}
delete route redistribute	{dst [rip | ospf] src [rip | local | static | ospf]}
show route redistribute	{dst [rip | ospf] | src [rip | static | local | ospf]

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

create route redistribute dst ospf src

Purpose	Used to add route redistribution settings for the exchange of RIP routes to OSPF routes on the switch.
Syntax	**create route redistribute dst ospf src [static | rip | local] {mettype [1 | 2] | metric <value>}**
Description	This command will redistribute routing information between the OSPF and RIP routing protocols to all routers on the network that are running OSPF or RIP. Routing information entered into the Static Routing Table on the local DGS-3312SR switch is also redistributed.
Parameters	*src [static | rip | local]* – Allows for the selection of the protocol for the source device. *mettype [1 | 2]* – Allows for the selection of one of two methods of calculating the metric value. Type-1 calculates (for RIP to OSPF) by adding the destination's interface cost to the metric entered in the Metric field. Type-2 uses the metric entered in the Metric field without change. This field applies only when the destination field is OSPF. *metric <value>* – Allows the entry of an OSPF interface cost. This is analogous to a Hop Count in the RIP routing protocol.
Restrictions	Only administrator-level users can issue this command.

Routing information source – RIP. the Static Route table, and the Local interface routing information. Routing information will be redistributed to OSPF.

Route Source	Metric	Metric Type
RIP	0 to 16777214	mettype 1 mettype 2
Static	0 to 16777214	mettype 1 mettype 2
Local	0 to 16777214	mettype 1 mettype 2

Allowed Metric Type combinations are **mettype 1** or **mettype 2**. The metric value **0** above will be redistributed in OSPF as the metric **20**.

Example Usage:

To add route redistribution settings:

```
DGS-3312SR:4#create route redistribute dst ospf src rip
Command: create route redistribute dst ospf src rip

Success.

DGS-3312SR:4#
```

create route redistribute dst rip src

Purpose	Used to add route redistribution settings for the exchange of OSPF routes to RIP routes on the switch.
Syntax	**create route redistribute dst rip src {all | internal | external | type_1 | type_2 | inter+e1 | inter+e2}] {metric <value>}**
Description	This command will redistribute routing information between the OSPF and RIP routing protocols to all routers on the network that are running OSPF or RIP. Routing information entered into the Static Routing Table on the local DGS-3312SR switch is also redistributed
Parameters	*src {all | internal | external | type_1 | type_2 | inter+e1 | inter+e2}* – Allows the selection of the protocol of the source device. *metric <value>* – Allows the entry of an OSPF interface cost. This is analogous to a HOP Count in the RIP routing protocol.
Restrictions	Only administrator-level users can issue this command.

Routing information source – OSPF and the Static Route table. Routing information will be redistributed to RIP. The following table lists the allowed values for the routing metrics and the types (or forms) of the routing information that will be redistributed.

Route Source	Metric	Type
OSPF	0 to 16	all type_1 type_2 inter+e1 inter+e2 external internal
Static	0 to 16	not applicable

Entering the **Type** combination – **internal type_1 type_2** is functionally equivalent to **all**. Entering the combination **type_1 type_2** is functionally equivalent to **external**. Entering the combination **internal external** is functionally equivalent to **all**.

Entering the metric **0** specifies transparency.

Example Usage:

To add route redistribution settings:

```
DGS-3312SR:4#create route redistribute dst rip src ospf all metric 2
Command: create route redistribute dst rip src ospf all metric 2

Success.

DGS-3312SR:4#
```

config route redistribute dst ospf src

Purpose	Used configure route redistribution settings for the exchange of RIP routes to OSPF routes on the switch.
Syntax	**config route redistribute dst ospf src [static | rip | local] {mettype [1 | 2] | metric <value>}**
Description	Route redistribution allows routers on the network – that are running different routing protocols to exchange routing information. This is accomplished by comparing the routes stored in the various router's routing tables and assigning appropriate metrics. This information is then exchanged among the various routers according to the individual routers current routing protocol. The switch can redistribute routing information between the OSPF and RIP routing protocols to all routers on the network that are running OSPF or RIP. Routing information entered into the Static Routing Table on the local switch is also redistributed.
Parameters	*src [static | rip | local]* – Allows the selection of the protocol of the source device. *mettype* – Allows the selection of one of the methods for calculating the metric value. Type-1 calculates the metric (for RIP to OSPF) by adding the destination's interface cost to the metric entered in the Metric field. Type-2 uses the metric entered in the Metric field without change. This field applies only when the destination field is OSPF. *metric <value>* – Allows the entry of an OSPF interface cost. This is analogous to a Hop Count in the RIP routing protocol.
Restrictions	Only administrator-level users can issue this command.

Routing information source – RIP: the Static Route table, and the Local interface routing information. Routing information will be redistributed to OSPF. The following table lists the allowed values for the routing metrics and the types (or forms) of the routing information that will be redistributed.

Route Source	Metric	Metric Type
RIP	0 to 16777214	mettype 1 mettype 2
Static	0 to 16777214	mettype 1 mettype 2
Local	0 to 16777214	mettype 1 mettype 2

Allowed Metric Type combinations are **mettype 1** or **mettype 2**. The metric value **0** above will be redistributed in OSPF as the metric **20**.

Example Usage:

To configure route redistributions:

```
DGS-3312SR:4#config route redistribute dst ospf src all metric 2
Command: config route redistribute dst ospf src all metric 2

Success.

DGS-3312SR:4#
```

config route redistribute dst rip src

Purpose	Used configure route redistribution settings for the exchange of RIP routes to OSPF routes on the switch.
Syntax	**config route redistribute dst rip src [local | static | ospf | [all | internal | external | type_1 | type_2 | inter+e1 | inter+e2]] {metric <value>}**
Description	Route redistribution allows routers on the network that are running different routing protocols to exchange routing information. This is accomplished by comparing the routes stored in the various router's routing tables and assigning appropriate metrics. This information is then exchanged among the various routers according to the individual routers current routing protocol. The switch can redistribute routing information between the OSPF and RIP routing protocols to all routers on the network that are running OSPF or RIP. Routing information entered into the Static Routing Table on the local switch is also redistributed.
Parameters	*src {all | internal | external | type_1 | type_2 | inter+e1 | inter+e2}* – Allows the selection of the protocol of the source device. *metric <value>* – Allows the entry of an OSPF interface cost. This is analogous to a Hop Count in the RIP routing protocol.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To configure route redistributions:

```
DGS-3312SR:4#config route redistribute dst ospf src rip mettype
type_1 metric 2

Command: config route redistribute dst ospf src rip mettype
type_1 metric 2


Success.


DGS-3312SR:4#
```

delete route redistribute	
Purpose	Used to delete an existing route redistribute configuration on the switch.
Syntax	**delete route redistribute {dst [rip | ospf] src [rip | static | local | ospf]}**
Description	This command will delete the route redistribution settings on this switch.
Parameters	*dst [rip | ospf]* – Allows the selection of the protocol on the destination device. *src [rip | static | local | ospf]* – Allows the selection of the protocol on the source device.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To delete route redistribution settings:

```
DGS-3312SR:4#delete route redistribute dst rip src ospf
Command: delete route redistribute dst rip src ospf

 Success.

DGS-3312SR:4#
```

show route redistribute	
Purpose	Used to display the route redistribution on the switch.
Syntax	**show route redistribute {dst [rip | ospf] | src [rip | static | local | ospf]}**
Description	Displays the current route redistribution settings on the switch.
Parameters	*src [rip | static | local | ospf]* – Allows the selection of the routing protocol on the source device. *dst [rip | ospf]* – Allows the selection of the routing protocol on the destination device.
Restrictions	none.

Example Usage:

To display route redistributions:

```
DGS-3312SR:4#show route redistribute
Command: show route redistribute

Source      Destination  Type        Metric
Protocol    Protocol
--------    -----------  --------    --------
STATIC      RIP          All         1
LOCAL       OSPF         Type-2      20

Total Entries : 2

DGS-3312SR:4#
```

34

BOOTP RELAY COMMANDS

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

Command	Parameters
config bootp_relay	{hops <value 1-16> | time <sec 0-65535>}
config bootp_relay add ipif	<ipif_name 12> <ipaddr>
config bootp_relay delete ipif	<ipif_name 12> <ipaddr>
enable bootp_relay	
disable bootp_relay	
show bootp_relay	{ipif <ipif_name 12>}

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

config bootp_relay

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

Example Usage:

To configure bootp relay status.

```
DGS-3312SR:4#config bootp_relay hops 4 time 2
Command: config bootp_relay hops 4 time 2

Success.

DGS-3312SR:4#
```

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

Example Usage:

To add a BOOTP relay.

```
DGS-3312SR:4#config bootp_relay add ipif System 10.43.21.12
Command: config bootp_relay add ipif System 10.43.21.12

Success.

DGS-3312SR:4#
```

config bootp_relay delete	
Purpose	Used to delete an IP destination addresses from the switch's BOOTP relay table.
Syntax	**config bootp_relay delete ipif <ipif_name 12> <ipaddr>**
Description	This command is used to delete an IP destination addresses in the switch's BOOTP relay table.
Parameters	<*ipif_name 12*> – The name of the IP interface that contains the IP address below. <*ipaddr*> – The BOOTP server IP address.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To delete a BOOTP relay:

```
DGS-3312SR:4#config bootp_relay delete ipif System 10.43.21.12
Command: config bootp_relay delete ipif System 10.43.21.12

Success.

DGS-3312SR:4#
```

enable bootp_relay	
Purpose	Used to enable the BOOTP relay function on the switch.
Syntax	**enable bootp_relay**
Description	This command, in combination with the **disable bootp_relay** command below, is used to enable and disable the BOOTP relay function on the switch.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To enable the BOOTP relay function:

```
DGS-3312SR:4#enable bootp_relay
Command: enable bootp_relay

Success.

DGS-3312SR:4#
```

disable bootp_relay	
Purpose	Used to disable the BOOTP relay function on the switch.
Syntax	**disable bootp_relay**
Description	This command, in combination with the **enable bootp_relay** command above, is used to enable and disable the BOOTP relay function on the switch.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To disable the BOOTP relay function:

```
DGS-3312SR:4#disable bootp_relay
Command: disable bootp_relay

Success.

DGS-3312SR:4#
```

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

Example Usage:

To display bootp relay status:

```
DGS-3312SR:4#show bootp_relay
Command: show bootp_relay

Bootp Relay Status              : Disabled
Bootp Hops Count Limit          : 4
Bootp Relay Time Threshold      : 0

Interface    Server 1        Server 2        Server 3        Server 4
-----------  --------------  --------------  --------------  --------------
System       10.48.74.122    10.23.12.34     10.12.34.12     10.48.75.121

Total Entries: 1

DGS-3312SR:4#
```

35

DNS RELAY COMMANDS

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

Command	Parameters
config dnsr	{[primary | secondary] nameserver <ipaddr> | [add | delete] static <domain_name 32> <ipaddr>}
enable dnsr	{cache | static}
disable dnsr	{cache | static}
show dnsr	{static}

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

config dnsr

Purpose	Used to configure the DNS relay function.
Syntax	**config dnsr {[primary | secondary] nameserver <ipaddr> | [add | delete] static <domain_name 32> <ipaddr>}**
Description	This command is used to configure the DNS relay function on the switch.
Parameters	*primary* – Indicates that the IP address below is the address of the primary DNS server. *secondary* – Indicates that the IP address below is the address of the secondary DNS server. *nameserver <ipaddr>* – The IP address of the DNS nameserver. *[add | delete]* – Indicates if the user wishes to add or delete the DNS relay function. *<domain_name 32>* – The domain name of the entry. *<ipaddr>* – The IP address of the entry.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To set IP address 10.43.21.12 of primary.

```
DGS-3312SR:4#config dnsr primary 10.43.21.12
Command: config dnsr primary 10.43.21.12

Success

DGS-3312SR:4#
```

Example Usage:

To add an entry domain name dns1, IP address 10.43.21.12 to DNS static table:

```
DGS-3312SR:4#config dnsr add static dns1 10.43.21.12
Command: config dnsr add static dns1 10.43.21.12

Success.
DGS-3312SR:4#
```

Example Usage:

To delete an entry domain name dns1, IP address 10.43.21.12 from DNS static table.

```
DGS-3312SR:4#config dnsr delete static dns1 10.43.21.12
Command: config dnsr delete static dns1 10.43.21.12

Success.

DGS-3312SR:4#
```

enable dnsr

Purpose	Used to enable DNS relay.
Syntax	**enable dnsr {cache | static}**
Description	This command is used, in combination with the **disable dnsr** command below, to enable and disable DNS Relay on the switch.
Parameters	*cache* - This parameter will allow the user to enable the cache lookup for the DNS rely on the switch. *static* - This parameter will allow the user to enable the static table lookup for the DNS rely on the switch.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To enable status of DNS relay:

```
DGS-3312SR:4#enable dnsr
Command: enable dnsr

Success.

DGS-3312SR:4#
```

Example Usage:

To enable cache lookup for DNS relay.

```
DGS-3312SR:4#enable dnsr cache
Command: enable dnsr cache

Success.

DGS-3312SR:4#
```

Example Usage:

To enable static table lookup for DNS relay.

```
DGS-3312SR:4#enable dnsr static
Command: enable dnsr static

Success.

DGS-3312SR:4#
```

disable dnsr

Purpose	Used to disable DNS relay on the switch.
Syntax	**disable dnsr {cache | static}**
Description	This command is used, in combination with the **enable dnsr** command above, to enable and disable DNS Relay on the switch.
Parameters	*cache* – This parameter will allow the user to disable the cache lookup for the DNS rely on the switch. *static* - This parameter will allow the user to disable the static table lookup for the DNS rely on the switch.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To disable status of DNS relay.

```
DGS-3312SR:4#disable dnsr
Command: disable dnsr

Success.

DGS-3312SR:4#
```

Example Usage:

To disable cache lookup for DNS relay.

```
DGS-3312SR:4#disable dnsr cache
Command: disable dnsr cache

Success.

DGS-3312SR:4#
```

Example Usage:

To disable static table lookup for DNS relay.

```
DGS-3312SR:4#disable dnsr static
Command: disable dnsr static

Success.

DGS-3312SR:4#
```

show dnsr

Purpose	Used to display the current DNS relay status.
Syntax	**show dnsr {static}**
Description	This command is used to display the current DNS relay status.
Parameters	*static* – Allows the display of only the static entries into the DNS relay table. If this parameter is omitted, the entire DNS relay table will be displayed.
Restrictions	None.

Example Usage:

To display DNS relay status:

```
DGS-3312SR:4#show dnsr
Command: show dnsr

DNSR Status                      : Disabled
Primary Name Server              : 0.0.0.0
Secondary Name Server            : 0.0.0.0
DNSR Cache Status                : Disabled
DNSR Static Cache Table Status   : Disabled

DNS Relay Static Table

Domain Name                      IP Address
-------------------------------- ---------------
www.123.com.tw                   10.12.12.123
bbs.ntu.edu.tw                   140.112.1.23

Total Entries: 2

DGS-3312SR:4#
```

36

RIP COMMANDS

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

Command	Parameters
config rip	[ipif <ipif_name 12> | all] {authentication [enable <password 16> | disable] | tx_mode [disable | v1_only | v1_compatible | v2_only] | rx_mode [v1_only | v2_only | v1_or_v2 | disable] state [enable | disable]}
enable rip	
disable rip	
show rip	ipif <ipif_name 12>

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

config rip

Purpose	Used to configure RIP on the switch.
Syntax	**config rip [ipif <ipif_name 12> | all] {authentication [enable <password 16> | disable] | tx_mode [disable | v1_only | v1_compatible | v2_only] | rx_mode [v1_only | v2_only | v1_or_v2 | disable] state [enable | disable]}**
Description	This command is used to configure RIP on the switch.
Parameters	*<ipif_name 12>* – The name of the IP interface. *all* – To configure all RIP receiving mode for all IP interfaces. *authentication [enable | disable]* – Enables or disables authentication for RIP on the switch. ▪ *<password 16>* – Allows the specification of a case-sensitive password. *tx_mode* – Determines how received RIP packets will be interpreted – as RIP version **V1 only, V2 Only,** or **V1 Compatible (V1 and V2).** This entry specifies which version of the RIP protocol will be used to transfer RIP packets. The Disabled entry prevents the reception of RIP packets. ▪ *disable* – Prevents the transmission of RIP packets. ▪ *v1_only* – Specifies that only RIP v1 packets will be transmitted. ▪ *v1_compatible* – Specifies that only RIP v1 compatible packets will be transmitted. ▪ *v2_only* - Specifies that only RIP v2 packets will be transmitted. *rx_mode* – Determines how received RIP packets will be interpreted – as RIP version **V1 only, V2 Only,** or **V1 or V2.** This entry specifies which version of the RIP protocol will be used to receive RIP packets. The Disabled entry prevents the

config rip	
	reception of RIP packets. ▪ *v1_only* – Specifies that only RIP v1 packets will be transmitted. ▪ *v2_only* - Specifies that only RIP v2 packets will be transmitted. ▪ *v1_or_v2* - Specifies that only RIP v1 or v2 packets will be transmitted. *state [enable | disable]* – Allows RIP to be enabled and disabled on the switch.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To change the RIP receive mode for the IP interface System:

```
DGS-3312SR:4#config rip ipif System rx_mode v1_only
Command: config rip ipif System rx_mode v1_only

Success.

DGS-3312SR:4#
```

enable rip	
Purpose	Used to enable RIP.
Syntax	**enable rip**
Description	This command is used to enable RIP on the switch.
Parameters	none.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To enable RIP:

```
DGS-3312SR:4#enable rip
Command: enable rip

Success.

DGS-3312SR:4#
```

disable rip

Purpose	Used to disable RIP.
Syntax	**disable rip**
Description	This command is used to disable RIP on the switch.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To disable rip:

```
DGS-3312SR:4#disable rip
Command: disable rip

Success.

DGS-3312SR:4#
```

show rip

Purpose	Used to display the RIP configuration and statistics for the switch.
Syntax	**show rip {ipif <ipif_name 12>}**
Description	This command will display the RIP configuration and statistics for a given IP interface or for all IP interfaces.
Parameters	*ipif <ipif_name 12>* – The name of the IP interface for which you want to display the RIP configuration and settings. If this parameter is not specified, the **show rip** command will display the global RIP configuration for the switch.
Restrictions	None.

Example Usage:

To display RIP configuration:

```
DGS-3312SR:4#show rip
Command: show rip

RIP Global State : Disabled

RIP Interface Settings

Interface    IP Address       TX Mode    RX Mode     Authen-   State
                                                     tication
-------------  ------------------  ----------  -------------  ----------  -----
System       10.41.44.33/8    Disabled   Disabled    Disabled   Disabled

Total Entries : 1

DGS-3312SR:4#
```

37

DVMRP COMMANDS

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

Command	Parameters
config dvmrp	[ipif <ipif_name 12> | all] {metric <value 1-31> | probe <sec 1-65535> | neighbor_timeout <sec 1-65535> | state [enable | disable]}
enable dvmrp	
disable dvmrp	
show dvmrp neighbor	{ipif <ipif_name 12> | ipaddress <network_address>}
show dvmrp nexthop	{ipaddress <network_address> | ipif <ipif_name 12>}
show dvmrp routing_table	{ipaddress <network_address>}
show dvmrp	{ipif <ipif_name 12>}

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

NOTE: Due to a switch limitation, DVMRP cannot function for Secondary IP interfaces, although the DVMRP settings for the Secondary IP Interface will be displayed. For more information regarding configuring Primary and Secondary IP Interfaces, see the *IP Interface Settings and IP Multinetting* section of the DGS-3312SR Manual.

config dvmrp

Purpose	Used to configure DVMRP on the switch.
Syntax	**config dvmrp [ipif <ipif_name 12> | all] {metric <value 1-31> | probe <sec 1-65535> | neighbor_timeout <sec 1-65535> | state [enable | disable]}**
Description	This command is used to configure DVMRP on the switch.
Parameters	*<ipif_name 12>* – The name of the IP interface for which DVMRP is to be configured. *all* – Specifies that DVMRP is to be configured for all IP interfaces on the switch. *metric <value 1-31>* – Allows the assignment of a DVMRP route cost to the above IP interface. A DVMRP route cost is a relative number that represents the real cost of using this route in the construction of a multicast delivery tree. It is similar to, but not defined as, the hop count in RIP. The default is 1. *probe <second 1-65535>* – DVMRP defined an extension to IGMP that allows routers to query other routers to determine if a DVMRP neighbor is present on a given subnetwork or not. This is referred to as a 'probe'. This entry will set an intermittent probe (in seconds) on the device that will transmit dvmrp messages, depending on the time specified. This

config dvmrp	
	probe is also used to “keep alive” the connection between DVMRP enabled devices. The default value is 10 seconds. *neighbor_timeout <second 1-65535>* – The time period for which DVMRP will hold Neighbor Router reports before issuing poison route messages. The default value is 35 seconds. *state [enable | disable]* – Allows DVMRP to be enabled or disabled.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To configure DVMRP configurations of IP interface System:

```
DGS-3312SR:4#config dvmrp ipif System neighbor_timeout 30 metric 1 probe 5
Command: config dvmrp ipif System neighbor_timeout 30 metric 1 probe 5

Success

DGS-3312SR:4#
```

enable dvmrp	
Purpose	Used to enable DVMRP.
Syntax	**enable dvmrp**
Description	This command, in combination with the **disable dvmrp** below, to enable and disable DVMRP on the switch.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To enable DVMRP:

```
DGS-3312SR:4#enable dvmrp
Command: enable dvmrp

Success.

DGS-3312SR:4#
```

disable dvmrp	
Purpose	Used to disable DVMRP.
Syntax	**disable dvmrp**
Description	This command, in combination with the **enable dvmrp** above, to enable and disable DVMRP on the switch.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To disable DVMRP:

```
DGS-3312SR:4#disable dvmrp
Command: disable dvmrp

Success.

DGS-3312SR:4#
```

show dvmrp routing_table	
Purpose	Used to display the current DVMRP routing table.
Syntax	**show dvmrp routing table [ipaddress <network_address>]**
Description	The command is used to display the current DVMRP routing table.
Parameters	*ipaddress <network_address>* – The IP address and netmask of the destination. You can specify the IP address and netmask information using the traditional format or the CIDR format. For example, 10.1.2.3/255.255.0.0 or 10.2.3.4/16.
Restrictions	None.

Example Usage:

To display DVMRP routing table:

```
DGS-3312SR:4#show dvmrp routing_table
Command: show dvmrp routing_table

DVMRP Routing Table
Source Address/Netmask  Upstream Neighbor  Metric  Learned   Interface   Expire
----------------------  -----------------  ------  --------  ----------  ------
10.0.0.0/8              10.90.90.90        2       Local     System      -
20.0.0.0/8              20.1.1.1           2       Local     ip2         117
30.0.0.0/8              30.1.1.1           2       Dynamic   ip3         106

Total Entries: 3

DGS-3312SR:4#
```

show dvmrp neighbor

Purpose	Used to display the DVMRP neighbor table.
Syntax	**show dvmrp neighbor {ipif <ipif_name 12> | ipaddress <network_address>}**
Description	This command will display the current DVMRP neighbor table.
Parameters	*<ipif_name 12>* – The name of the IP interface for which you want to display the DVMRP neighbor table. *ipaddress <network_address>* – The IP address and netmask of the destination. You can specify the IP address and netmask information using the traditional format or the CIDR format. For example, 10.1.2.3/255.255.0.0 or 10.2.3.4/16.
Restrictions	None.

Example Usage:

To display DVMRP neighbor table:

```
DGS-3312SR:4#show dvmrp neighbor
Command: show dvmrp neighbor

DVMRP Neighbor Address Table

Interface       Neighbor Address      Generation ID      Expire Time
---------------  ----------------------  -------------------  ---------
System          10.2.1.123            2                  250

Total Entries: 1

DGS-3312SR:4#
```

show dvmrp nexthop

Purpose	Used to display the current DVMRP routing next hop table.
Syntax	**show dvmrp nexthop {ipaddress <network_address> | ipif <ipif_name 12>}**
Description	This command will display the DVMRP routing next hop table.
Parameters	*<ipif_name 12>* – The name of the IP interface for which you want to display the current DVMRP routing next hop table. *ipaddress <network_address>* – The IP address and netmask of the destination. You can specify the IP address and netmask information using the traditional format or the CIDR format. For example, 10.1.2.3/255.255.0.0 or 10.2.3.4/16.
Restrictions	None.

Example Usage:

To display DVMRP routing next hop table:

```
DGS-3312SR:4#show dvmrp nexthop
Command: show dvmrp nexthop

Source IP Address/Netmask  Interface Name   Type
-----------------          ---------------  ------
10.0.0.0/8                 ip2              Leaf
10.0.0.0/8                 ip3              Leaf
20.0.0.0/8                 System           Leaf
20.0.0.0/8                 ip3              Leaf
30.0.0.0/8                 System           Leaf
30.0.0.0/8                 ip2              Leaf

Total Entries: 6

DGS-3312SR:4#
```

show dvmrp

Purpose	Used to display the current DVMRP routing table.
Syntax	**show dvmrp {<ipif_name 12>}**
Description	The command will display the current DVMRP routing table.
Parameters	*<ipif_name 12>* – The name of the IP interface for which you want to display the DVMRP routing table.
Restrictions	None.

Example Usage:

To show DVMRP configurations:

```
DGS-3312SR:4#show dvmrp
Command: show dvmrp

DVMRP Global State : Disabled

Interface   IP Address       Neighbor Timeout  Probe  Metric  State
----------  ---------------  ----------------  -----  ------  -------
System      10.90.90.90/8    35                10     1       Disabled

Total Entries: 1

DGS-3312SR:4#
```

38

PIM COMMANDS

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

Command	Parameters
config pim	[ipif <ipif_name 12> | all] {hello <sec 1-18724> | jp_interval <sec 1-18724> | state [enable | disable]}
enable pim	
disable pim	
show pim neighbor	{ipif <ipif_name 12> | ipaddress <network_address>}
show pim	{ipif <ipif_name 12>}

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

NOTE: Due to a switch limitation, PIM-DM cannot function for Secondary IP interfaces, although the PIM-DM settings for the Secondary IP Interface will be displayed. For more information regarding configuring Primary and Secondary IP Interfaces, see the *IP Interface Settings and IP Multinetting* section of the DGS-3312SR Manual.

config pim

Purpose	Used to configure PIM settings for the switch or for specified IP interfaces.
Syntax	**config pim [ipif <ipif_name 12> | all] { hello <sec 1-18724> | jp_interval <sec 1-18724> | state [enable | disable]}**
Description	The config pim command is used to configure PIM settings and enable or disable PIM settings for specified IP interfaces. PIM must also be globally enabled to function (see **enable pim**).
Parameters	*ipif <ipif_name 12>* – Name assigned to the specific IP interface being configured for PIM settings. *all* – Used to configure PIM settings for all IP interfaces. *hello <sec 1-18724>* - The time, in seconds, between issuing hello packets to find neighboring routers. *jp_interval <sec 1-18724>* – The join/prune interval is the time value (seconds) between transmitting (flooding to all interfaces) multicast messages to downstream routers, and automatically 'pruning' a branch from the multicast delivery tree. The *jp_interval* is also the interval used by the router to automatically remove prune information from a branch of a multicast delivery tree and begin to flood multicast messages to all branches of that delivery tree. These two actions are equivalent. The range is between 1 and 18724 seconds. The default is 60 seconds.

config pim	
	state [enable | *disable]* – This can enable or disable PIM for the specified IP interface. The default is disabled. Note that PIM settings must also be enabled globally for the switch with the **enable pim** described below for PIM to operate on any configured IP interfaces.
Restrictions	Only administrator-level users can issue this command.

Usage Example:

To configure PIM settings for IP interface "System":

```
DGS-3312SR:4#config pim ipif System hello 35 jp_interval 70 state enable
Command: config pim ipif System hello 35 jp_interval 70 state enable

Success.

DGS-3312SR:4#
```

enable pim	
Purpose	Used to enable PIM function on the switch.
Syntax	**enable pim**
Description	This command will enable PIM for the switch. PIM settings must first be configured for specific IP interfaces using the **config pim** command.
Parameters	None.
Restrictions	Only administrator-level users can use this command.

Usage Example:

To enable PIM as previously configured on the switch:

```
DGS-3312SR:4#enable pim
Command: enable pim

Success.

DGS-3312SR:4#
```

disable pim	
Purpose	Used to disable PIM function on the switch.
Syntax	**disable pim**

disable pim	
Description	This command will disable PIM for the switch. Any previously configured PIM settings will remain unchanged and may be enabled at a later time with the **enable pim** command.
Parameters	None.
Restrictions	Only administrator-level users can use this command.

Usage Example:

To disable PIM on the switch:

```
DGS-3312SR:4#disable pim
Command: disable pim

Success.

DGS-3312SR:4#
```

show pim neighbor	
Purpose	Used to display PIM neighbor router table entries.
Syntax	**show pim neighbor {ipif <ipif_name 12> | ipaddress <network_address>}**
Description	This command will list current entries in the PIM neighbor table for a specified IP interface or destination router IP address.
Parameters	*ipif <ipif_name 12>* – The name of an IP interface for which you want to view the PIM neighbor router table. *ipaddress <network_address>*- The IP address and netmask of the destination routing device for which you want to view the neighbor router table. You can specify the IP address and netmask information using the traditional format or the CIDR format. For example, 10.1.2.3/255.255.0.0 or 10.2.3.4/16. If no parameters are specified, all PIM neighbor router tables are displayed.
Restrictions	None.

Example usage:

To display PIM settings as configured on the switch:

```
DGS-3312SR:4#show pim neighbor
Command: show pim neighbor

PIM Neighbor Address Table

Interface Name   Neighbor Address  Expire Time
---------------  ----------------  -----------
System           10.48.74.122      5

Total Entries : 1

DGS-3312SR:4#
```

show pim

Purpose	Used to display current PIM configuration.
Syntax	**show pim {ipif <ipif_name 12>}**
Description	This command will list current PIM configuration settings for a specified IP interface or all IP interfaces.
Parameters	*ipif <ipif_name 12>* – The name of an IP interface for which PIM settings are listed. If no parameters are specified, all PIM settings are displayed for all interfaces.
Restrictions	None.

Usage Example:

To display PIM settings as configured on the switch:

```
DGS-3312SR:4#show pim
Command: show pim

PIM Global State : Disabled

PIM-DM Interface Table
                                 Hello     Join/Prune
Interface    IP Address          Interval  Interval    State
-----------  ---------------     --------  ----------  --------
System       10.90.90.90/8       35        60          Enabled

Total Entries : 1

DGS-3312SR:4#
```

39

IP MULTICASTING COMMANDS

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

Command	Parameters
show ipmc cache	{group <group>} {ipaddress <network_address>}
show ipmc	{ipif <ipif_name 12> | protocol [dvmrp | pim]}

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

show ipmc cache

Purpose	Used to display the current IP multicast forwarding cache.
Syntax	**show ipmc cache {group <group>} {ipaddress <network_address>}**
Description	This command will display the current IP multicast forwarding cache.
Parameters	*<group>* – The multicast group ID. *ipaddress <network_address>* – The IP address and netmask of the destination. You can specify the IP address and netmask information using the traditional format or the CIDR format. For example, 10.1.2.3/255.255.0.0 or 10.2.3.4/16.
Restrictions	None.

Usage Example:

To display the current IP multicast forwarding cache:

```
DGS-3312SR:4#show ipmc cache
Command: show ipmc cache

Multicast Group   Source Address/Netmask   Upstream Neighbor   Expire Time   Routing Protocol
---------------   ----------------         ---------------     ----------    ---------
224.1.1.1         10.48.74.121/32          10.48.75.63         30            dvmrp
224.1.1.1         20.48.74.25 /32          20.48.75.25         20            dvmrp
224.1.2.3         10.48.75.3 /3            10.48.76.6          30            dvmrp

Total Entries: 3

DGS-3312SR:4#
```

show ipmc	
Purpose	Used to display the IP multicast interface table.
Syntax	**show ipmc {ipif <ipif_name 12> | protocol [dvmrp | pim]}**
Description	This command will display the current IP multicast interface table.
Parameters	*<ipif_name 12>* – The name of the IP interface for which you want to display the IP multicast interface table for. *protocol [dvmrp | pim]* – Allows the user to specify whether or not to use the DVMRP or PIM protocol to display the IP multicast interface table. For example, if DVMRP is specified, the table will display only those entries that are related to the DVMRP protocol.
Restrictions	None.

Usage Example

To display the current IP multicast interface table by DVMRP entry:

```
DGS-3312SR:4#show ipmc ipif System protocol dvmrp
Command: show ipmc ipif System protocol dvmrp

Interface Name    IP Address      Multicast Routing
---------------   ---------------  ----------------
System            10.90.90.90     DVMRP

Total Entries: 1

DGS-3312SR:4#
```

40

MD5 CONFIGURATION COMMANDS

The MD5 configuration commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameters
create md5 key	<key_id 1-255> <password 16>
config md5 key	<key_id 1-255> <password 16>
delete md5 key	<key_id 1-255>
show md5 key	<key_id 1-255>

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

create md5 key

Purpose	Used to create a new entry in the MD5 key table.
Syntax	**create md5 key <key_id 1-255> <password 16>**
Description	This command is used to create an entry for the MD5 key table.
Parameters	*<key_id 1-255>* – The MD5 key ID. The user may enter a key ranging from 1 to 255. *<password>* – An MD5 password of up to 16 bytes.
Restrictions	Only administrator-level users can issue this command.

Usage Example

To create an entry in the MD5 key table:

```
DGS-3312SR:4# create md5 key 1 dlink
Command: create md5 key 1 dlink

Success.

DGS-3312SR:4#
```

config md5 key

Purpose	Used to enter configure the password for an MD5 key.
Syntax	**config md5 key <key_id 1-255> <password 16>**
Description	This command is used to configure an MD5 key and password.
Parameters	*<key_id 1-255>* – The previously defined MD5 key ID. *<password 16>* – The user may change the MD5 password for the md5 key. A new password of up to 16 characters can be created.
Restrictions	Only administrator-level users can issue this command.

Usage Example

To configure an MD5 Key password:

```
DGS-3312SR:4#config md5 key 1 taboo
Command: config md5 key 1 taboo

Success.

DGS-3312SR:4#
```

delete md5 key	
Purpose	Used to delete an entry in the MD5 key table.
Syntax	**delete md5 key <key_id 1-255>**
Description	This command is used to delete a specific entry in the MD5 key table.
Parameters	*<key_id 1-255>* – The MD5 key ID the user wishes to delete.
Restrictions	Only administrator-level users can issue this command.

Usage Example

The delete an entry in the MD5 key table:

```
DGS-3312SR:4# delete md5 key 1
Command: delete md5 key 1

Success.

DGS-3312SR:4#
```

show md5 key	
Purpose	Used to display an MD5 key table.
Syntax	**show md5 {key <key_id 1-255>}**
Description	This command will display the current MD5 key table.
Parameters	*<key_id 1-255>* – The MD5 key ID.
Restrictions	None.

Usage Example

To display the current MD5 key:

```
DGS-3312SR:4#show md5
Command: show md5

MD5 Key Table Configurations

Key-ID      Key
------      ----------
1           dlink
2           develop
3           fireball
4           intelligent

Total Entries: 4

DGS-3312SR:4#
```

41

OSPF CONFIGURATION COMMANDS

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

Command	Parameters
config ospf router_id	<ipaddr>
enable ospf	
disable ospf	
show ospf	
create ospf area	<area_id> type [normal | stub {stub_summary [enable | disable] | metric <value 0-65535>}]
delete ospf area	<area_id>
config ospf area	<area_id> type [normal | stub {stub_summary [enable | disable] | metric <value 0-65535>}]
show ospf area	{<area_id>}
create ospf host_route	<ipaddr> {area <area_id> | metric <value 1-65535>}
delete ospf host_route	<ipaddr>
config ospf host_route	<ipaddr> {area <area_id> | metric <value 1-65535>}
show ospf host_route	<ipaddr>
create ospf aggregation	<area_id> <network_address> lsdb_type summary {advertise [enable | disable]}
delete ospf aggregation	<area_id> <network_address> lsdb_type summary
config ospf aggregation	<area_id> <network_address> lsdb_type summary {advertise [enable | disable]}
show ospf aggregation	<area_id>
show ospf lsdb	{area <area_id> | advertise_router <ipaddr> | type [rtrlink | netlink | summary | assummary | asextlink]}
show ospf neighbor	<ipaddr>
show ospf virtual_neighbor	{<area_id> <neighbor_id>}
config ospf ipif	<ipif_name 12> {area <area_id> | priority <value> | hello_interval <sec 1-65535 > | dead_interval <sec 1-65535> | authentication [none | simple <password 8> | md5 <key_id 1-255>] | metric <value 1-65535> state [enable | disable]
config ospf all	{area <area_id> | priority <value> | hello_interval <1-65535 sec> | dead_interval <1-65535 sec> | authentication [none | simple <password 8> | md5 <key_id 1-255>] | metric <value 1-65535> state [enable | disable]}
show ospf ipif	<ipif_name 12>

Command	Parameters
show ospf all	
create ospf virtual_link	<area_id> <neighbor_id> {hello_interval <sec 1-65535> | dead_interval <sec 1-65535> | authentication [none | simple <password 8> | md5 <key_id 1-255>]}
config ospf virtual_link	<area_id> <neighbor_id> {hello_interval <sec 1-65535> | dead_interval <sec 1-65535> | authentication [none | simple <password 8> | md5 <key_id 1-255>]}
delete ospf virtual_link	<area_id> <neighbor_id>
show ospf virtual_link	<area_id> <neighbor_id>

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

config ospf router_id

Purpose	Used to configure the OSPF router ID.
Syntax	**config ospf router_id <ipaddr>**
Description	This command is used to configure the OSPF router ID.
Parameters	*<ipaddr>* – The IP address of the OSPF router.
Restrictions	Only administrator-level users can issue this command.

Usage Example

To configure the OSPF router ID:

```
DGS-3312SR:4#config ospf router_id 10.48.74.122
Command: config ospf router_id 10.48.74.122

Success.

DGS-3312SR:4#
```

enable ospf

Purpose	Used to enable OSPF on the switch.
Syntax	**enable ospf**
Description	This command, in combination with the **disable ospf** command below, is used to enable and disable OSPF on the switch.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Usage Example

To enable OSPF on the switch:

```
DGS-3312SR:4#enable ospf
Command: enable ospf

Success.

DGS-3312SR:4#
```

disable ospf

Purpose	Used to disable OSPF on the switch.
Syntax	**disable ospf**
Description	This command, in combination with the **enable ospf** command above, is used to enable and disable OSPF on the switch.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Usage Example

To disable OSPF on the switch:

```
DGS-3312SR:4#disable ospf
Command: disable ospf

Success.

DGS-3312SR:4#
```

show ospf

Purpose	Used to display the current OSPF state on the switch.
Syntax	**show ospf**
Description	This command will display the current state of OSPF on the switch, divided into the following categories: General OSPF settings OSPF Interface settings OSPF Area settings OSPF Virtual Interface settings OSPF Area Aggregation settings OSPF Host Route settings
Parameters	None.
Restrictions	None.

Usage Example:

To show OSPF state:

```
DGS-3312SR:4#show ospf
Command: show ospf

OSPF Router ID    : 10.1.1.2
State             : Enabled
OSPF Interface Settings
Interface   IP Address      Area ID   State      Link          Metric
                                                 Status
------------  ------------------  ---------  --------  ---------  ---------
System      10.90.90.90/8   0.0.0.0    Disabled   Link DOWN   1
ip2         20.1.1.1/8      0.0.0.0    Disabled   Link DOWN   1
ip3         30.1.1.1/8      0.0.0.0    Disabled   Link DOWN   1

Total Entries : 3

OSPF Area Settings
Area ID       Type      Stub Import Summary LSA   Stub Default Cost
---------------  ------    ----------------------    -----------------
0.0.0.0       Normal    None                      None
10.0.0.0      Normal    None                      None
10.1.1.1      Normal    None                      None
20.1.1.1      Stub      Enabled                    1

Total Entries : 4

Virtual Interface Configuration
Transit    Virtual              Hello     Dead      Authentication   Link
Area ID    Neighbor Router      Interval  Interval                   Status
-----------  ---------------      --------  --------  --------------   ------
10.0.0.0   20.0.0.0            10        60        None             DOWN
10.1.1.1   20.1.1.1            10        60        None             DOWN

Total Entries : 2

OSPF Area Aggregation Settings
Area ID        Aggregated          LSDB    Advertise
               Network Address     Type
---------------  ------------------    --------  ---------

Total Entries : 0
OSPF Host Route Settings
Host Address    Metric  Area ID       TOS
---------------    ------  ------------    ------
10.3.3.3           1       10.1.1.1

Total Entries : 1

DGS-3312SR:4#
```

create ospf area	
Purpose	Used to configure OSPF area settings.
Syntax	**create ospf area <area_id> type [normal | stub {stub_summary [enable | disable] | metric <value 0-65535>}]**
Description	This command is used to create an OSPF area and configure its settings.
Parameters	*<area_id>* – The OSPF area ID. The user may enter a 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain. *type [normal | stub]* – The OSPF area mode of operation – stub or normal. *stub_summary [enable | disable]* – Enables or disables the OSPF area to import summary LSA advertisements. *metric <value 0-65535>* – The OSPF area cost between 0 and 65535. *0* denotes that the value will be automatically assigned. The default setting is 0.
Restrictions	Only administrator-level users can issue this command.

Usage Example:

To create an OSPF area:

```
DGS-3312SR:4#create ospf area 10.48.74.122 type normal
Command: create ospf area 10.48.74.122 type normal

Success.

DGS-3312SR:4#
```

delete ospf area	
Purpose	Used to delete an OSPF area.
Syntax	**delete ospf area <area_id>**
Description	This command is used to delete an OSPF area.
Parameters	*<area_id>* – A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.
Restrictions	Only administrator-level users can issue this command.

Usage Example:

To delete an OSPF area:

```
DGS-3312SR:4#delete ospf area 10.48.74.122
Command: delete ospf area 10.48.74.122

Success.

DGS-3312SR:4#
```

config ospf area

Purpose	Used to configure an OSPF area's settings.
Syntax	**config ospf area <area_id> type [normal | stub {stub_summary [enable | disable] | metric <value 0-65535>}]**
Description	This command is used to configure an OSPF area's settings.
Parameters	*<area_id>* – The OSPF area ID. The user may enter a 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain. *type [normal | stub]* – Allows the specification of the OSPF mode of operation – stub or normal. *stub_summary [enable | disable]* – Allows the OSPF area import of LSA advertisements to be enabled or disabled. *metric <value 0-65535>* – The OSPF area stub default cost.
Restrictions	Only administrator-level users can issue this command.

Usage Example

To configure an OSPF area's settings:

```
DGS-3312SR:4#config ospf area 10.48.74.122 type stub stub_summary
enable metric 1
Command: config ospf area 10.48.74.122 type stub stub_summary enable
metric 1

Success.

DGS-3312SR:4#
```

show ospf area

Purpose	Used to display an OSPF area's configuration.
Syntax	**show ospf area {<area_id>}**
Description	This command will display the current OSPF area configuration.
Parameters	*<area_id>* – A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.
Restrictions	None.

Usage Example

To display an OSPF area's settings:

```
DGS-3312SR:4#show ospf area
Command: show ospf area

Area ID          Type       Stub  Import Summary LSA   Stub       Default Cost
---------------  ---------- ----------------------------------- ---------- --------
0.0.0.0          Normal     None                        None       None
10.48.74.122     Stub       Enabled                     Enabled    1

Total Entries: 2

DGS-3312SR:4#
```

create ospf host_route

Purpose	Used to configure OSPF host route settings.
Syntax	**create ospf host_route <ipaddr> {area <area_id> | metric <value 1-65535>}**
Description	This command is used to configure the OSPF host route settings.
Parameters	*<ipaddr>* – The host's IP address. *<area_id>* – A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain. *metric <value 1-65535>* – A metric between 1 and 65535, which will be advertised.
Restrictions	Only administrator-level users can issue this command.

Usage Example

To configure the OSPF host route settings:

```
DGS-3312SR:4#create ospf host_route 10.48.74.122 area 10.1.1.1 metric 2
Command: create ospf host_route 10.48.74.122 area 10.1.1.1 metric 2

Success.

DGS-3312SR:4#
```

delete ospf host_route

Purpose	Used to delete an OSPF host route.
Syntax	**delete ospf host_route <ipaddr>**
Description	This command is used to delete an OSPF host route.
Parameters	*<ipaddr>* – The IP address of the OSPF host.
Restrictions	Only administrator-level users can issue this command.

Usage Example

To delete an OSPF host route:

```
DGS-3312SR:4#delete ospf host_route 10.48.74.122
Command: delete ospf host_route 10.48.74.122

Success.

DGS-3312SR:4#
```

config ospf host_route

Purpose	Used to configure OSPF host route settings.
Syntax	**config ospf host_route <ipaddr> {area <area_id> | metric <value>}**
Description	This command is used to configure an OSPF host route settings.
Parameters	*<ipaddr>* – The IP address of the host. *<area_id>* – A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain. *<value>* – A metric value between 1 and 65535 that will be advertised for the route.
Restrictions	Only administrator-level users can issue this command.

Usage Example

To configure an OSPF host route:

```
DGS-3312SR:4#config ospf host_route 10.48.74.122 area 10.1.1.1 metric 2
Command: config ospf host_route 10.48.74.122 area 10.1.1.1 metric 2

Success.

DGS-3312SR:4#
```

show ospf host_route

Purpose	Used to display the current OSPF host route table.
Syntax	**show ospf host_route {<ipaddr>}**
Description	This command will display the current OSPF host route table.
Parameters	*<ipaddr>* – The IP address of the host.

show ospf host_route

Restrictions	None.

Usage Example:

To display the current OSPF host route table:

```
DGS-3312SR:4#show ospf host_route
Command: show ospf host_route

Host Address    Metric          Area_ID     TOS
---------------  ---------------  -----------  ------
10.48.73.21     2               10.1.1.1
10.48.74.122    1               10.1.1.1

Total Entries: 2

DGS-3312SR:4#
```

create ospf aggregation

Purpose	Used to configure OSPF area aggregation settings.
Syntax	**create ospf aggregation <area_id> <network_address> lsdb_type summary {advertise [enable | disable]}**
Description	This command is used to create an OSPF area aggregation.
Parameters	*<area_id>* – A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain. *<network_address>* – The 32-bit number in the form of an IP address that uniquely identifies the network that corresponds to the OSPF Area. *lsdb_type summary* – The type of address aggregation. *advertise [enable | disable]* – Allows for the advertisement trigger to be enabled or disabled.
Restrictions	Only administrator-level users can issue this command.

Usage Example:

To create an OSPF area aggregation:

```
DGS-3312SR:4#create ospf aggregation 10.1.1.1 10.48.76.122/16
lsdb_type summary advertise enable

Command: create ospf aggregation 10.1.1.1 10.48.76.122/16
lsdb_type summary advertise enable


Success.


DGS-3312SR:4#
```

delete ospf aggregation	
Purpose	Used to delete an OSPF area aggregation configuration.
Syntax	**delete ospf aggregation <area_id> <network_address> lsdb_type summary**
Description	This command is used to delete an OSPF area aggregation configuration.
Parameters	*<area_id>* – A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain. *<network_address>* – The 32-bit number in the form of an IP address that uniquely identifies the network that corresponds to the OSPF Area. *lsdb_type summary* – Specifies the type of address aggregation.
Restrictions	Only administrator-level users can issue this command.

Usage Example

To configure the OSPF area aggregation settings:

```
DGS-3312SR:4#delete ospf aggregation 10.1.1.1 10.48.76.122/16 lsdb_type
summary
Command:  delete ospf aggregation 10.1.1.1 10.48.76..122/16 lsdb_type
summary

Success.

DGS-3312SR:4#
```

config ospf aggregation	
Purpose	Used to configure the OSPF area aggregation settings.
Syntax	**config ospf aggregation <area_id> <network_address> lsdb_type summary {advertise [enable | disable]}**
Description	This command is used to configure the OSPF area aggregation settings.
Parameters	*<area_id>* – A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain. *<network_address>* – The 32-bit number in the form of an IP address that uniquely identifies the network that corresponds to the OSPF Area. *lsdb_type summary* – Specifies the type of address aggregation. *advertise [enable | disable]* – Allows for the advertisement trigger to be enabled or disabled.
Restrictions	Only administrator-level users can issue this command.

Usage Example

To configure the OSPF area aggregation settings:

```
DGS-3312SR:4#config ospf aggregation 10.1.1.1 10.48.76.122/16
lsdb_type summary advertise enable
Command: config ospf aggregation 10.1.1.1 10.48.76.122/16 lsdb_type
summary advertise enable

Success.

DGS-3312SR:4#
```

show ospf aggregation

Purpose	Used to display the current OSPF area aggregation settings.
Syntax	**show ospf aggregation {<area_id>}**
Description	This command will display the current OSPF area aggregation settings.
Parameters	*<area_id>* – Enter this parameter if you wish to view this table by a specific OSPF area ID.
Restrictions	None.

Usage Example

To display OSPF area aggregation settings:

```
DGS-3312SR:4#show ospf aggregation
Command: show ospf aggregation

OSPF Area Aggregation Settings

Area ID    Aggregated          LSDB          Advertise
           Network Address     Type
---------- ------------------- ------------- -------------
10.1.1.1   10.0.0.0/8          Summary       Enabled
10.1.1.1   20.2.0.0/16         Summary       Enabled

Total Entries: 2

DGS-3312SR:4#
```

show ospf lsdb

Purpose	Used to display the OSPF Link State Database (LSDB).
Syntax	**show ospf lsdb {area_id <area_id> | advertise_router <ipaddr> | type [rtrlink | netlink | summary | assummary | asextlink]}**
Description	This command will display the current OSPF Link State Database (LSDB).
Parameters	*area_id <area_id>* – A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the

show ospf lsdb

	OSPF domain. *advertise_router <ipaddr>* – The router ID of the advertising router. *type [rtrlink | netlink | summary | assummary | asextlink]* – The type of link.
Restrictions	None.

NOTE: When this command displays a "*" (a star symbol) in the OSPF LSDB table for the *area_id* or the *Cost*, this is interpreted as "no area ID" for external LSAs, and as "no cost given" for the advertised link.

Usage Example:

To display the link state database of OSPF:

```
DGS-3312SR:4#show ospf lsdb
Command: show ospf lsdb

Area      LSDB      Advertising   Link State   Cost   Sequence
ID        Type      Router ID     ID                  Number
----------  -------------  ----------------  ----------------  -------  ----------------
0.0.0.0   RTRLink   50.48.75.73   50.48.75.73   *      0x80000002
0.0.0.0   Summary   50.48.75.73   10.0.0.0/8    1      0x80000001
1.0.0.0   RTRLink   50.48.75.73   50.48.75.73   *      0x80000001
1.0.0.0   Summary   50.48.75.73   40.0.0.0/8    1      0x80000001
1.0.0.0   Summary   50.48.75.73   50.0.0.0/8    1      0x80000001
*         ASExtLink 50.48.75.73   1.2.0.0/16    20     0x80000001

Total Entries: 5

DGS-3312SR:4#
```

show ospf neighbor

Purpose	Used to display the current OSPF neighbor router table.
Syntax	**show ospf neighbor {<ipaddr>}**
Description	This command will display the current OSPF neighbor router table.
Parameters	*<ipaddr>* – The IP address of the neighbor router.
Restrictions	None.

Usage Example

To display the current OSPF neighbor router table:

```
DGS-3312SR:4#show ospf neighbor
Command: show ospf neighbor

IP Address of    Router ID of    Neighbor   Neighbor
Neighbor         Neighbor        Priority   State
---------------  --------------  --------   ------------
10.48.74.122     10.2.2.2        1          Initial

DGS-3312SR:4#
```

show ospf virtual_neighbor

Purpose	Used to display the current OSPF virtual neighbor router table.
Syntax	**show ospf virtual_neighbor {<area_id> <neighbor id>}**
Description	This command will display the current OSPF virtual neighbor router table.
Parameters	<*area_id*> – A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain. <*neighbor_id*> – The OSPF router ID for the neighbor. This is a 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the remote area's Area Border Router.
Restrictions	None.

Usage Example

To display the current OSPF virtual neighbor table:

```
DGS-3312SR:4#show ospf virtual_neighbor
Command: show ospf virtual_neighbor

Transit      Router ID of      IP Address of     Virtual Neighbor
Area ID      Virtual Neighbor  Virtual Neighbor  State
-----------  ----------------  ----------------  ----------------
10.1.1.1     10.2.3.4          10.48.74.111      Exchange

Total Entries : 1

DGS-3312SR:4#
```

config ospf ipif	
Purpose	Used to configure the OSPF interface settings.
Syntax	**config ospf ipif <ipif_name 12> {area <area_id> | priority <value> | hello_interval <sec 1-65535>| dead_interval <sec 1-65535> | authentication [none | simple <password 8> | md5 <key_id 1-255>] | metric <value 1-65535> | state [enable | disable]}**
Description	This command is used to configure the OSPF interface settings.
Parameters	*<ipif_name 12>* – The name of the IP interface. *area <area_id>* - A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain. *priority <value>* – The priority used in the election of the Designated Router (DR). A number between 0 and 255. *hello_interval <sec 1-65535>* – Allows the specification of the interval between the transmission of OSPF Hello packets, in seconds. Between 1 and 65535 seconds can be specified. The Hello Interval, Dead Interval, Authorization Type, and Authorization Key should be the same for all routers on the same network. *dead_interval <sec 1-65535>* – Allows the specification of the length of time between the receipt of Hello packets from a neighbor router before the selected area declares that router down. An interval between 1 and 65535 seconds can be specified. The *dead interval* must be evenly divisible by the Hello Interval. *metric <value 1-65535 >* – The interface metric (1 to 65535). Entering a 0 will allow automatic calculation of the metric. *authentication* – Enter the type of authentication preferred. The user may choose between: ▪ *none* – Choosing this parameter will require no authentication. ▪ *simple <password 8>* – Choosing this parameter will set a simple authentication which includes a case-sensitive password of no more than 8 characters. ▪ *md5 <key_id 1-255>* – Choosing this parameter will set authentication based on md5 encryption. A previously configured MD5 key ID (1 to 255) is required. *metric <value 1-65535>* – This field allows the entry of a number between 1 and 65,535 that is representative of the OSPF cost of reaching the selected OSPF interface. The default metric is 1. *state [enable | disable]* – Used to enable or disable this function.
Restrictions	Only administrator-level users can issue this command.

Usage Example

To configure OSPF interface settings:

```
DGS-3312SR:4#config ospf ipif System priority 2 hello_interval 15
metric 2 state enable
Command: config ospf ipif System priority 2 hello_interval 15
metric 2 state enable

Success.

DGS-3312SR:4#
```

config ospf all

Purpose	Used to configure all of the OSPF interfaces on the switch at one time.
Syntax	**config ospf all {area <area_id> | priority <value> | hello_interval <sec 1-65535> | dead_interval <sec 1-65535> | authentication [none | simple <password 8> | md5 <key_id 1-255>] | metric <value 1-65535> | state [enable | disable]}**
Description	This command is used to configure all of the OSPF interfaces on the switch, using a single group of parameters, at one time.
Parameters	*area <area_id>* - A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain. *priority <value>* – The priority used in the election of the Designated Router (DR). A number between 0 and 255. *hello_interval <sec 1-65535>* – Allows the specification of the interval between the transmission of OSPF Hello packets, in seconds. Between 1 and 65535 seconds can be specified. The Hello Interval, Dead Interval, Authorization Type, and Authorization Key should be the same for all routers on the same network. *dead_interval <sec 1-65535>* – Allows the specification of the length of time between the receipt of Hello packets from a neighbor router before the selected area declares that router down. An interval between 1 and 65535 seconds can be specified. The Dead Interval must be evenly divisible by the Hello Interval. *metric <value 1-65535 >* – The interface metric (1 to 65535). Entering a 0 will allow automatic calculation of the metric. *authentication* – Enter the type of authentication preferred. The user may choose between: ▪ *none* – Choosing this parameter will require no authentication. ▪ *simple <password 8>* – Choosing this parameter will set a simple authentication which includes a case-sensitive password of no more than 8 characters. ▪ *md5 <key_id 1-255>* – Choosing this parameter will set authentication based on md5 encryption. A previously configured MD5 key ID (1 to 255) is required. *metric <value 1-65535>* – This field allows the entry of a number between 1 and 65,535 that is representative of the OSPF cost of reaching the selected OSPF interface. The default metric is 1. *state [enable | disable]* – Used to enable or disable this function.
Restrictions	Only administrator-level users can issue this command.

Usage Example

To configure all of the OSPF interfaces on the switch with a single group of parameters:

```
DGS-3312SR:4#config ospf all state enable
Command: config ospf all state enable

Success.

DGS-3312SR:4#
```

show ospf ipif

Purpose	Used to display the current OSPF interface settings for the specified interface name.
Syntax	**show ospf ipif {<ipif_name 12> | all}**
Description	This command will display the current OSPF interface settings for the specified interface name.
Parameters	*<ipif_name 12>* – The IP interface name for which you want to display the current OSPF interface settings. *all* – Entering this parameter will display all ospf Interface settings.
Restrictions	None.

Usage Example

To display the current OSPF interface settings, for a specific OSPF interface:

```
DGS-3312SR:4#show ospf ipif ipif2
Command: show ospf ipif ipif2

Interface Name:  ipif2                    IP Address:  123.234.12.34/24 ((Link Up)
Network Medium Type: BROADCAST            Metric:  1
Area ID:  1.0.0.0                         Administrative State:  Enabled
Priority:  1                              DR State:  DR
DR Address:  123.234.12.34                Backup DR Address:  None
Hello Interval:  10                       Dead Interval:  40
Transmit Delay:  1                        Retransmit Time:  5
Authentication:  None

Total Entries: 1

DGS-3312SR:4#
```

Usage Example:

To display the current OSPF interface settings, for all OSPF interfaces on the switch:

```
DGS-3312SR:4#show ospf all
Command: show ospf all

Interface Name: System                    IP Address:  10.42.73.10/8 (Link Up)
Network Medium Type: BROADCAST            Metric:  1
Area ID:  0.0.0.0                         Administrative State:  Enabled
Priority:  1                              DR State:  DR
DR Address:  10.42.73.10                  Backup DR Address:  None
Hello Interval:  10                       Dead Interval:  40
Transmit Delay:  1                        Retransmit Time:  5
Authentication:  None
```

```
Interface Name:  ipif2                    IP Address:  123.234.12.34/24 ((Link Up)
Network Medium Type: BROADCAST            Metric:  1
Area ID:  1.0.0.0                         Administrative State:  Enabled
Priority:  1                              DR State:  DR
DR Address:  123.234.12.34                Backup DR Address:  None
Hello Interval:  10                       Dead Interval:  40
Transmit Delay:  1                        Retransmit Time:  5
Authentication:  None

Total Entries: 2

DGS-3312SR:4#
```

create ospf virtual_link

Purpose	Used to create an OSPF virtual interface.
Syntax	**create ospf virtual_link <area_id> <neighbor_id> {hello_interval <sec 1-65535> | dead_interval <sec 1-65535> | authentication [none | simple <password 8> | md5 <key_id 1-255>]}**
Description	This command is used to create an OSPF virtual interface.
Parameters	*<area_id>* – A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain. *<neighbor_id>* – The OSPF router ID for the remote area. This is a 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the remote area's Area Border Router. The router ID of the neighbor router. *hello_interval <sec 1-65535>* – Allows the specification of the interval between the transmission of OSPF Hello packets, in seconds. Between 1 and 65535 seconds can be specified. The Hello Interval, Dead Interval, Authorization Type, and Authorization Key should be the same for all routers on the same network. *dead_interval <sec 1-65535>* – Allows the specification of the length of time between the receipt of Hello packets from a neighbor router before the selected area declares that router down. An interval between 1 and 65535 seconds can be specified. The Dead Interval must be evenly divisible by the Hello Interval. *authentication* – Enter the type of authentication preferred. The user may choose between: ▪ *none* – Choosing this parameter will require no authentication. ▪ *simple <password 8>* – Choosing this parameter will set a simple authentication which includes a case-sensitive password of no more than 8 characters. ▪ *md5 <key_id 1-255>* – Choosing this parameter will set authentication based on md5 encryption. A previously configured MD5 key ID (1 to 255) is required.
Restrictions	Only administrator-level users can issue this command.

Usage Example

To create an OSPF virtual interface:

```
DGS-3312SR:4#create ospf virtual_link 10.1.12 20.1.1.1 hello_interval 10
Command: create ospf virtual_link 10.1.12 20.1.1.1 hello_interval 10

Success.

DGS-3312SR:4#
```

config ospf virtual_link

Purpose	Used to configure the OSPF virtual interface settings.
Syntax	**config ospf virtual_link <area_id> <neighbor_id> {hello_interval <sec 1-65535> | dead_interval <sec 1-65535> | authentication [none | simple <password 8> | md5 <key_id 1-255>]}**
Description	This command is used to configure the OSPF virtual interface settings.
Parameters	*<area_id>* – A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain. *<neighbor_id>* – The OSPF router ID for the remote area. This is a 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the remote area's Area Border Router. *hello_interval <sec 1-65535>* – Allows the specification of the interval between the transmission of OSPF Hello packets, in seconds. Between 1 and 65535 seconds can be specified. The Hello Interval, Dead Interval, Authorization Type, and Authorization Key should be the same for all routers on the same network. *dead_interval <sec 1-65535>* – Allows the specification of the length of time between the receipt of Hello packets from a neighbor router before the selected area declares that router down. An interval between 1 and 65535 seconds can be specified. The Dead Interval must be evenly divisible by the Hello Interval. *authentication* – Enter the type of authentication preferred. The user may choose between: ▪ *none* – Choosing this parameter will require no authentication. ▪ *simple <password 8>* – Choosing this parameter will set a simple authentication which includes a case-sensitive password of no more than 8 characters. ▪ *md5 <key_id 1-255>* – Choosing this parameter will set authentication based on md5 encryption A previously configured MD5 key ID (1 to 255) is required.
Restrictions	Only administrator-level users can issue this command.

Usage Example

To configure the OSPF virtual interface settings:

```
DGS-3312SR:4#config ospf virtual_link 10.1.1.2 20.1.1.1 hello_interval 10
Command: config ospf virtual_link 10.1.1.2 20.1.1.1 hello_interval 10

Success.

DGS-3312SR:4#
```

delete ospf virtual_link

Purpose	Used to delete an OSPF virtual interface.
Syntax	**delete ospf virtual_link <area_id> <neighbor_id>**
Description	This command will delete an OSPF virtual interface from the switch.
Parameters	*<area_id>* – A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain. *<neighbor_id>* – The OSPF router ID for the remote area. This is a 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the remote area's Area Border Router. The router ID of the neighbor router.
Restrictions	Only administrator-level users can issue this command.

Usage Example:

To delete an OSPF virtual interface from the switch:

```
DGS-3312SR:4#delete ospf virtual_link 10.1.12 20.1.1.1
Command: delete ospf virtual_link 10.1.12 20.1.1.1

Success.

DGS-3312SR:4#
```

show ospf virtual_link

Purpose	Used to display the current OSPF virtual interface configuration.
Syntax	**show ospf virtual_link {<area_id> <neighbor_id>}**
Description	This command will display the current OSPF virtual interface configuration.

show ospf virtual_link	
Parameters	*<area_id>* – A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain. *<neighbor_id>* – The OSPF router ID for the remote area. This is a 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the remote area's Area Border Router. This is the router ID of the neighbor router.
Restrictions	None.

Usage Example:

To display the current OSPF virtual interface configuration:

```
DGS-3312SR:4#show ospf virtual_link
Command: show ospf virtual_link

Transit      Virtual         Hello     Dead      Authentication     Link
Area ID      Neighbor Router Interval  Interval                     Status
------------ --------------- --------- --------- ------------------ ----------
10.0.0.0     20.0.0.0        10        60        None               DOWN

Total Entries: 1

DGS-3312SR:4#
```

42

COMMAND HISTORY LIST

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

Command	Parameters
?	
show command_history	
config command_history	<value 1-40>

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

?	
Purpose	Used to display all commands in the Command Line Interface (CLI).
Syntax	**?**
Description	This command will display all of the commands available through the Command Line Interface (CLI).
Parameters	None.
Restrictions	None.

Example usage

To display all of the commands in the CLI:

```
DGS-3312SR:4#?

Command:?

..
?
clear
clear arptable
clear counters
clear fdb
clear log
config 802.1p default_priority
config 802.1p user_priority
config 802.1x auth_mode
config 802.1x auth_parameter ports
config 802.1x auth_protocol
config 802.1x capability ports
config 802.1x init
config 802.1x reauth
config access profile profile_id
config account
config admin local_enable
config all_boxes_id
config arp_aging time
config authen_application

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

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

Example usage

To display the command history:

```
DGS-3312SR:4#show command_history
Command: show command_history

?
? show
show vlan
config router_ports vlan2 add 1:1-1:10
config router_ports vlan2 add
config router_ports vlan2
config router_ports
show vlan
create vlan vlan2 tag 3
create vlan vlan2 tag 2
show router_ports
show router ports
login

DGS-3312SR:4#
```

config command_history	
Purpose	Used to configure the command history.
Syntax	**config command_history <value 1-40>**
Description	This command is used to configure the command history.
Parameters	*<value 1-40>* – The number of previously executed commands maintained in the buffer. Up to 40 of the latest executed commands may be viewed.
Restrictions	None.

Example usage

To configure the command history:

```
DGS-3312SR:4#config command_history 20
Command: config command_history 20


Success.


DGS-3312SR:4#
```

A

TECHNICAL SPECIFICATIONS

Physical and Environmental	
AC input & External Redundant Power Supply	100 – 120; 200 - 240 VAC, 50/60 Hz (internal universal power supply)
Power Consumption	90 watts maximum
DC fans	2 built-in 40 x 40 x10 mm fans
Operating Temperature	0 to 40 degrees Celsius
Storage Temperature	-25 to 55 degrees Celsius
Humidity	Operating: 5% to 95% RH non-condensing; Storage: 0% to 95% RH non-condensing
Dimensions	441 mm x 207 mm x 44 mm (1U), 19 inch rack-mount width
Weight	3.15 kg
EMC	FCC Class A CE Mark C-Tick
Safety	CSA International

General		
Standards:	IEEE 802.3u 100BASE-TX Fast Ethernet IEEE 802.3ab 1000BASE-T Gigabit Ethernet IEEE 802.1 P/Q VLAN IEEE 802.3x Full-duplex Flow Control IEEE 802.3 Nway auto-negotiation IEEE 802.3z SFP ports IEEE 1394.b Stacking IEEE 802.1D/w/s Spanning trees. IEEE 802.1p QoS (Priority Bits) IEEE 802.1X Access Control	
Protocols:	CSMA/CD	
Data Transfer Rates:	Half-duplex	Full-duplex
Ethernet	10 Mbps	20Mbps

General	
Fast Ethernet	100Mbps 200Mbps
Gigabit Ethernet	n/a 2000Mbps
Fiber Optic	SFP (Mini GBIC) Support IEEE 802.3z 1000BASE-LX (DEM-310GT transceiver) IEEE 802.3z 1000BASE-SX (DEM-311GT transceiver) IEEE 802.3z 1000BASE-LH (DEM-314GT transceiver) IEEE 802.3z 1000BASE-ZX (DEM-315GT transceiver)
Network Cables:	
10BASE-T:	UTP Cat.5, Cat.5 Enhanced for 1000Mbps UTP Cat.5 for 100Mbps UTP Cat.3, 4, 5 for 10Mbps
100BASE-TX	EIA/TIA-568 100-ohm screened twisted-pair (STP)(100m)
Number of Ports	12 x 10/100/1000 Gigabit Ethernet ports

Performance	
Transmission Method	Store-and-forward
RAM Buffer	1 MB per device
Filtering Address Table	16K MAC address per device
Packet Filtering/Forwarding Rate:	Full-wire speed for all connections. 148,810 pps per port (for 100Mbps) 1,488,100 pps per port (for 1000Mbps)
MAC Address Learning	Automatic update.
Forwarding Table Age Time	Max age: 10 - 1000000 seconds. Default = 300.

FCC Warning

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with this manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

CE Mark Warning

This is a Class A product. In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.

Warnung!

Dies ist ein Produkt der Klasse A. Im Wohnbereich kann dieses Produkt Funkstoerungen verursachen. In diesem Fall kann vom Benutzer verlangt werden, angemessene Massnahmen zu ergreifen.

Precaución!

Este es un producto de Clase A. En un entorno doméstico, puede causar interferencias de radio, en cuyo case, puede requerirse al usuario para que adopte las medidas adecuadas.

Attention!

Ceci est un produit de classe A. Dans un environnement domestique, ce produit pourrait causer des interférences radio, auquel cas l`utilisateur devrait prendre les mesures adéquates.

Attenzione!

Il presente prodotto appartiene alla classe A. Se utilizzato in ambiente domestico il prodotto può causare interferenze radio, nel cui caso è possibile che l`utente debba assumere provvedimenti adeguati.

VCCI Warning

この装置は、クラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

BSMI Warning

警告使用者

這是甲類的資訊產品,在居住的環境中使用時,可能會造成射頻干擾,
在這種情況下使用者會被要求採取某些適當的對策

Warranty and Registration Information

(All countries and regions excluding USA)

Wichtige Sicherheitshinweise

1. Bitte lesen Sie sich diese Hinweise sorgfältig durch.
2. Heben Sie diese Anleitung für den spätern Gebrauch auf.
3. Vor jedem Reinigen ist das Gerät vom Stromnetz zu trennen. Vervenden Sie keine Flüssig- oder Aerosolreiniger. Am besten dient ein angefeuchtetes Tuch zur Reinigung.
4. Um eine Beschädigung des Gerätes zu vermeiden sollten Sie nur Zubehörteile verwenden, die vom Hersteller zugelassen sind.
5. Das Gerät is vor Feuchtigkeit zu schützen.
6. Bei der Aufstellung des Gerätes ist auf sichern Stand zu achten. Ein Kippen oder Fallen könnte Verletzungen hervorrufen. Verwenden Sie nur sichere Standorte und beachten Sie die Aufstellhinweise des Herstellers.
7. Die Belüftungsöffnungen dienen zur Luftzirkulation die das Gerät vor Überhitzung schützt. Sorgen Sie dafür, daß diese Öffnungen nicht abgedeckt werden.
8. Beachten Sie beim Anschluß an das Stromnetz die Anschlußwerte.
9. Die Netzanschlußsteckdose muß aus Gründen der elektrischen Sicherheit einen Schutzleiterkontakt haben.
10. Verlegen Sie die Netzanschlußleitung so, daß niemand darüber fallen kann. Es sollete auch nichts auf der Leitung abgestellt werden.
11. Alle Hinweise und Warnungen die sich am Geräten befinden sind zu beachten.
12. Wird das Gerät über einen längeren Zeitraum nicht benutzt, sollten Sie es vom Stromnetz trennen. Somit wird im Falle einer Überspannung eine Beschädigung vermieden.
13. Durch die Lüftungsöffnungen dürfen niemals Gegenstände oder Flüssigkeiten in das Gerät gelangen. Dies könnte einen Brand bzw. Elektrischen Schlag auslösen.
14. Öffnen Sie niemals das Gerät. Das Gerät darf aus Gründen der elektrischen Sicherheit nur von authorisiertem Servicepersonal geöffnet werden.
15. Wenn folgende Situationen auftreten ist das Gerät vom Stromnetz zu trennen und von einer qualifizierten Servicestelle zu überprüfen:
    a. Netzkabel oder Netzstecker sint beschädigt.
    b. Flüssigkeit ist in das Gerät eingedrungen.
    c. Das Gerät war Feuchtigkeit ausgesetzt.
    d. Wenn das Gerät nicht der Bedienungsanleitung ensprechend funktioniert oder Sie mit Hilfe dieser Anleitung keine Verbesserung erzielen.
    e. Das Gerät ist gefallen und/oder das Gehäuse ist beschädigt.
    f. Wenn das Gerät deutliche Anzeichen eines Defektes aufweist.
16. Bei Reparaturen dürfen nur Orginalersatzteile bzw. den Orginalteilen entsprechende Teile verwendet werden. Der Einsatz von ungeeigneten Ersatzteilen kann eine weitere Beschädigung hervorrufen.
17. Wenden Sie sich mit allen Fragen die Service und Repartur betreffen an Ihren Servicepartner. Somit stellen Sie die Betriebssicherheit des Gerätes sicher.
18. Zum Netzanschluß dieses Gerätes ist eine geprüfte Leitung zu verwenden, Für einen Nennstrom bis 6A und einem Gerätegewicht größer 3kg ist eine Leitung nicht leichter als H05VV-F, 3G, 0.75mm2 einzusetzen.

WARRANTIES EXCLUSIVE

IF THE D-LINK PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, THE CUSTOMER'S SOLE REMEDY SHALL BE, AT D-LINK'S OPTION, REPAIR OR REPLACEMENT. THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESSED OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. D-LINK NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION MAINTENANCE OR USE OF D-LINK'S PRODUCTS.

D-LINK SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THAT THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY THE CUSTOMER'S OR ANY THIRD PERSON'S MISUSE, NEGLECT, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING OR OTHER HAZARD.

LIMITATION OF LIABILITY

IN NO EVENT WILL D-LINK BE LIABLE FOR ANY DAMAGES, INCLUDING LOSS OF DATA, LOSS OF PROFITS, COST OF COVER OR OTHER INCIDENTAL, CONSEQUENTIAL OR INDIRECT DAMAGES ARISING OUT THE INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE OR INTERRUPTION OF A D- LINK PRODUCT, HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY. THIS LIMITATION WILL APPLY EVEN IF D-LINK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

IF YOU PURCHASED A D-LINK PRODUCT IN THE UNITED STATES, SOME STATES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

Limited Warranty

Hardware:

D-Link warrants each of its hardware products to be free from defects in workmanship and materials under normal use and service for a period commencing on the date of purchase from D-Link or its Authorized Reseller and extending for the length of time stipulated by the Authorized Reseller or D-Link Branch Office nearest to the place of purchase.

This Warranty applies on the condition that the product Registration Card is filled out and returned to a D-Link office within ninety (90) days of purchase. A list of D-Link offices is provided at the back of this manual, together with a copy of the Registration Card.

If the product proves defective within the applicable warranty period, D-Link will provide repair or replacement of the product. D-Link shall have the sole discretion whether to repair or replace, and replacement product may be new or reconditioned. Replacement product shall be of equivalent or better specifications, relative to the defective product, but need not be identical. Any product or part repaired by D-Link pursuant to this warranty shall have a warranty period of not less than 90 days, from date of such repair, irrespective of any earlier expiration of original warranty period. When D-Link provides replacement, then the defective product becomes the property of D-Link.

Warranty service may be obtained by contacting a D-Link office within the applicable warranty period, and requesting a Return Material Authorization (RMA) number. If a Registration Card for the product in question has not been returned to D-Link, then a proof of purchase (such as a copy of the dated purchase invoice) must be provided. If Purchaser's circumstances require special handling of warranty correction, then at the time of requesting RMA number, Purchaser may also propose special procedure as may be suitable to the case.

After an RMA number is issued, the defective product must be packaged securely in the original or other suitable shipping package to ensure that it will not be damaged in transit, and the RMA number must be prominently marked on the outside of the package. The package must be mailed or otherwise shipped to D-Link with all costs of mailing/shipping/insurance prepaid. D-Link shall never be responsible for any software, firmware, information, or memory data of Purchaser contained in, stored on, or integrated with any product returned to D-Link pursuant to this warranty.

Any package returned to D-Link without an RMA number will be rejected and shipped back to Purchaser at Purchaser's expense, and D-Link reserves the right in such a case to levy a reasonable handling charge in addition mailing or shipping costs.

Software:

Warranty service for software products may be obtained by contacting a D-Link office within the applicable warranty period. A list of D-Link offices is provided at the back of this manual, together with a copy of the Registration Card. If a Registration Card for the product in question has not been returned to a D-Link office, then a proof of purchase (such as a copy of the dated purchase invoice) must be provided when requesting warranty service. The term "purchase" in this software warranty refers to the purchase transaction and resulting license to use such software.

D-Link warrants that its software products will perform in substantial conformance with the applicable product documentation provided by D-Link with such software product, for a period of ninety (90) days from the date of purchase from D-Link or its Authorized Reseller. D-Link warrants the magnetic media, on which D-Link provides its software product, against failure during the same warranty period. This warranty applies to purchased software, and to replacement software provided by D-Link pursuant to this warranty, but shall not apply to any update or replacement which may be provided for download via the Internet, or to any update which may otherwise be provided free of charge.

D-Link's sole obligation under this software warranty shall be to replace any defective software product with product which substantially conforms to D-Link's applicable product documentation. Purchaser assumes responsibility for the selection of appropriate application and system/platform software and associated reference materials. D-Link makes no warranty that its software products will work in combination with any hardware, or any application or system/platform software product provided by any third party, excepting only such products as are expressly represented, in D-Link's applicable product documentation as being compatible. D-Link's obligation under this warranty shall be a reasonable effort to provide compatibility, but D-Link shall have no obligation to provide compatibility when there is fault in the third-party hardware or software. D-Link makes no warranty that operation of its software products will be uninterrupted or absolutely error-free, and no warranty that all defects in the software product, within or without the scope of D-Link's applicable product documentation, will be corrected.

D-Link®
Building Networks for People

Limited Warranty (USA Only)

Subject to the terms and conditions set forth herein, D-Link Systems, Inc. ("D-Link") provides this Limited Warranty:

- Only to the person or entity that originally purchased the product from D-Link or its authorized reseller or distributor, and
- Only for products purchased and delivered within the fifty states of the United States, the District of Columbia, U.S. Possessions or Protectorates, U.S. Military Installations, or addresses with an APO or FPO.

Limited Warranty: D-Link warrants that the hardware portion of the D-Link product described below ("Hardware") will be free from material defects in workmanship and materials under normal use from the date of original retail purchase of the product, for the period set forth below ("Warranty Period"), except as otherwise stated herein.

- Hardware (excluding power supplies and fans): Five (5) Years
- Power supplies and fans: One (1) Year
- Spare parts and spare kits: Ninety (90) days

The customer's sole and exclusive remedy and the entire liability of D-Link and its suppliers under this Limited Warranty will be, at D-Link's option, to repair or replace the defective Hardware during the Warranty Period at no charge to the original owner or to refund the actual purchase price paid. Any repair or replacement will be rendered by D-Link at an Authorized D-Link Service Office. The replacement hardware need not be new or have an identical make, model or part. D-Link may, at its option, replace the defective Hardware or any part thereof with any reconditioned product that D-Link reasonably determines is substantially equivalent (or superior) in all material respects to the defective Hardware. Repaired or replacement hardware will be warranted for the remainder of the original Warranty Period or ninety (90) days, whichever is longer, and is subject to the same limitations and exclusions. If a material defect is incapable of correction, or if D-Link determines that it is not practical to repair or replace the defective Hardware, the actual price paid by the original purchaser for the defective Hardware will be refunded by D-Link upon return to D-Link of the defective Hardware. All Hardware or part thereof that is replaced by D-Link, or for which the purchase price is refunded, shall become the property of D-Link upon replacement or refund.

Limited Software Warranty: D-Link warrants that the software portion of the product ("Software") will substantially conform to D-Link's then current functional specifications for the Software, as set forth in the applicable documentation, from the date of original retail purchase of the Software for a period of ninety (90) days ("Software Warranty Period"), provided that the Software is properly installed on approved hardware and operated as contemplated in its documentation. D-Link further warrants that, during the Software Warranty Period, the magnetic media on which D-Link delivers the Software will be free of physical defects. The customer's sole and exclusive remedy and the entire liability of D-Link and its suppliers under this Limited Warranty will be, at D-Link's option, to replace the non-conforming Software (or defective media) with software that substantially conforms to D-Link's functional specifications for the Software or to refund the portion of the actual purchase price paid that is attributable to the Software. Except as otherwise agreed by D-Link in writing, the replacement Software is provided only to the original licensee, and is subject to the terms and conditions of the license granted by D-Link for the Software. Replacement Software will be warranted for the remainder of the original Warranty Period and is subject to the same limitations and exclusions. If a material non-conformance is incapable of correction, or if D-Link determines in its sole discretion that it is not practical to replace the non-conforming Software, the price paid by the original licensee for the non-conforming Software will be refunded by D-Link; provided that the non-conforming Software (and all copies thereof) is first returned to D-Link. The license granted respecting any Software for which a refund is given automatically terminates.

Non-Applicability of Warranty: The Limited Warranty provided hereunder for Hardware and Software portions of D-Link's products will not be applied to and does not cover any refurbished product and any product purchased through the inventory clearance or liquidation sale or other sales in which D-Link, the sellers, or the liquidators expressly disclaim their warranty obligation pertaining to the product and in that case, the product is being sold "As-Is" without any warranty whatsoever including, without limitation, the Limited Warranty as described herein, notwithstanding anything stated herein to the contrary.

Submitting A Claim: The customer shall return the product to the original purchase point based on its return policy. In case the return policy period has expired and the product is within warranty, the customer shall submit a claim to D-Link as outlined below:

- The customer must submit with the product as part of the claim a written description of the Hardware defect or Software nonconformance in sufficient detail to allow D-Link to confirm the same, along with proof of purchase of the product (such as a copy of the dated purchase invoice for the product) if the product is not registered.
- The customer must obtain a Case ID Number from D-Link Technical Support at 1-877-453-5465, who will attempt to assist the customer in resolving any suspected defects with the product. If the product is considered defective, the customer must obtain a Return Material Authorization ("RMA") number by completing the RMA form and entering the assigned Case ID Number at https://rma.dlink.com/.
- After an RMA number is issued, the defective product must be packaged securely in the original or other suitable shipping package to ensure that it will not be damaged in transit, and the RMA number must be prominently marked on the outside of the package. Do not include any manuals or accessories in the shipping package. D-Link will only replace the defective portion of the product and will not ship back any accessories.
- The customer is responsible for all in-bound shipping charges to D-Link. No Cash on Delivery ("COD") is allowed. Products sent COD will either be rejected by D-Link or become the property of D-Link. Products shall be fully insured by the customer and shipped to **D-Link Systems, Inc., 17595 Mt. Herrmann, Fountain Valley, CA 92708**. D-Link will not be held responsible for any packages that are lost in transit to D-Link. The repaired or replaced packages will be shipped to the customer via UPS Ground or any common carrier selected by D-Link. Return shipping charges shall be prepaid by D-Link if you use an address in the United States, otherwise we will ship the product to you freight collect. Expedited shipping is available upon request and provided shipping charges are prepaid by the customer.

- D-Link may reject or return any product that is not packaged and shipped in strict compliance with the foregoing requirements, or for which an RMA number is not visible from the outside of the package. The product owner agrees to pay D-Link's reasonable handling and return shipping charges for any product that is not packaged and shipped in accordance with the foregoing requirements, or that is determined by D-Link not to be defective or non-conforming.

What Is Not Covered: The Limited Warranty provided herein by D-Link does not cover: Products that, in D-Link's judgment, have been subjected to abuse, accident, alteration, modification, tampering, negligence, misuse, faulty installation, lack of reasonable care, repair or service in any way that is not contemplated in the documentation for the product, or if the model or serial number has been altered, tampered with, defaced or removed; Initial installation, installation and removal of the product for repair, and shipping costs; Operational adjustments covered in the operating manual for the product, and normal maintenance; Damage that occurs in shipment, due to act of God, failures due to power surge, and cosmetic damage; Any hardware, software, firmware or other products or services provided by anyone other than D-Link; and Products that have been purchased from inventory clearance or liquidation sales or other sales in which D-Link, the sellers, or the liquidators expressly disclaim their warranty obligation pertaining to the product. While necessary maintenance or repairs on your Product can be performed by any company, we recommend that you use only an Authorized D-Link Service Office. Improper or incorrectly performed maintenance or repair voids this Limited Warranty.

Disclaimer of Other Warranties: EXCEPT FOR THE LIMITED WARRANTY SPECIFIED HEREIN, THE PRODUCT IS PROVIDED "AS-IS" WITHOUT ANY WARRANTY OF ANY KIND WHATSOEVER INCLUDING, WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. IF ANY IMPLIED WARRANTY CANNOT BE DISCLAIMED IN ANY TERRITORY WHERE A PRODUCT IS SOLD, THE DURATION OF SUCH IMPLIED WARRANTY SHALL BE LIMITED TO THE DURATION OF THE APPLICABLE WARRANTY PERIOD SET FORTH ABOVE. EXCEPT AS EXPRESSLY COVERED UNDER THE LIMITED WARRANTY PROVIDED HEREIN, THE ENTIRE RISK AS TO THE QUALITY, SELECTION AND PERFORMANCE OF THE PRODUCT IS WITH THE PURCHASER OF THE PRODUCT.

Limitation of Liability: TO THE MAXIMUM EXTENT PERMITTED BY LAW, D-LINK IS NOT LIABLE UNDER ANY CONTRACT, NEGLIGENCE, STRICT LIABILITY OR OTHER LEGAL OR EQUITABLE THEORY FOR ANY LOSS OF USE OF THE PRODUCT, INCONVENIENCE OR DAMAGES OF ANY CHARACTER, WHETHER DIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF GOODWILL, LOSS OF REVENUE OR PROFIT, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, FAILURE OF OTHER EQUIPMENT OR COMPUTER PROGRAMS TO WHICH D-LINK'S PRODUCT IS CONNECTED WITH, LOSS OF INFORMATION OR DATA CONTAINED IN, STORED ON, OR INTEGRATED WITH ANY PRODUCT RETURNED TO D-LINK FOR WARRANTY SERVICE) RESULTING FROM THE USE OF THE PRODUCT, RELATING TO WARRANTY SERVICE, OR ARISING OUT OF ANY BREACH OF THIS LIMITED WARRANTY, EVEN IF D-LINK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE SOLE REMEDY FOR A BREACH OF THE FOREGOING LIMITED WARRANTY IS REPAIR, REPLACEMENT OR REFUND OF THE DEFECTIVE OR NON-CONFORMING PRODUCT. THE MAXIMUM LIABILITY OF D-LINK UNDER THIS WARRANTY IS LIMITED TO THE PURCHASE PRICE OF THE PRODUCT COVERED BY THE WARRANTY. THE FOREGOING EXPRESS WRITTEN WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ANY OTHER WARRANTIES OR REMEDIES, EXPRESS, IMPLIED OR STATUTORY.

Governing Law: This Limited Warranty shall be governed by the laws of the State of California. Some states do not allow exclusion or limitation of incidental or consequential damages, or limitations on how long an implied warranty lasts, so the foregoing limitations and exclusions may not apply. This Limited Warranty provides specific legal rights and you may also have other rights which vary from state to state.

Trademarks: D-Link is a registered trademark of D-Link Systems, Inc. Other trademarks or registered trademarks are the property of their respective owners.

Copyright Statement: No part of this publication or documentation accompanying this product may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from D-Link Corporation/D-Link Systems, Inc., as stipulated by the United States Copyright Act of 1976 and any amendments thereto. Contents are subject to change without prior notice. Copyright 2004 by D-Link Corporation/D-Link Systems, Inc. All rights reserved.

CE Mark Warning: This is a Class A product. In a residential environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

FCC Statement: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communication. However, there is no guarantee that interference will not occur in a particular installation. Operation of this equipment in a residential environment is likely to cause harmful interference to radio or television reception. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

For detailed warranty information applicable to products purchased outside the United States, please contact the corresponding local D-Link office.

Product Registration

Register online your D-Link product at http://support.dlink.com/register/

Product registration is entirely voluntary and failure to complete or return this form will not diminish your warranty rights.

- Trademarks

Copyright 2002 D-Link Corporation. Contents subject to change without prior notice. D-Link is a registered trademark of D-Link Corporation/ D-Link Systems Inc. All other trademarks belong to their respective proprietors.

- Copyright statement

No part of this publication may be reproduced in any form or by any means or used to make an derivative such as translation, transformation, or adaptation without permission from D-Link Corporation/ D-Link Systems Inc as stipulated by the United States Copyright Act of 1976.

CE EMI class A warning

This is a Class A product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

D-Link Europe Limited Product Warranty

General Terms

The Limited Product Warranty set forth below is given by D-LINK (Europe) Ltd. (herein referred to as "D-LINK"). This Limited Product Warranty is only effective upon presentation of the proof of purchase. Upon further request by D-LINK, this warranty card has to be presented, too.

EXCEPT AS EXPRESSLY SET FORTH IN THIS LIMITED WARRANTY, D-LINK MAKES NO OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. D-LINK EXPRESSLY DISCLAIMS ALL WARRANTIES NOT STATED IN THIS LIMITED WARRANTY. ANY IMPLIED WARRANTIES THAT MAY BE IMPOSED BY LAW ARE LIMITED IN DURATION TO THE LIMITED WARRANTY PERIOD. SOME STATES OR COUNTRIES DO NOT ALLOW A LIMITATION ON HOW LONG AN IMPLIED WARRANTY LASTS OR THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES FOR CONSUMER PRODUCTS. IN SUCH STATES OR COUNTRIES, SOME EXCLUSIONS OR LIMITATIONS OF THIS LIMITED WARRANTY MAY NOT APPLY TO YOU. THIS LIMITED WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY ALSO HAVE OTHER RIGHTS THAT MAY VARY FROM STATE TO STATE OR FROM COUNTRY TO COUNTRY. YOU ARE ADVISED TO CONSULT APPLICABLE STATE OR COUNTRY LAWS FOR

A FULL DETERMINATION OF YOUR RIGHTS.

This limited warranty applies to D-LINK branded hardware products (collectively referred to in this limited warranty as “D-LINK Hardware Products”) sold by from D-LINK (Europe) Ltd., its worldwide subsidiaries, affiliates, authorized resellers, or country distributors (collectively referred to in this limited warranty as “D-LINK”) with this limited warranty. The Term “D-LINK Hardware Product” is limited to the hardware components and all its internal components including firmware. The term “D-LINK Hardware Product” DOES NOT include any software applications or programs.

Geographical Scope of the Limited Product Warranty

This Limited Product Warranty is applicable in all European Countries as listed in the addendum “European Countries for D-LINK Limited Product Warranty”. The term “European Countries” in this D-LINK Limited Product Warranty only include the countries as listed in this addendum. The Limited Product Warranty will be honored in any country where D-LINK or its authorized service providers offer warranty service subject to the terms and conditions set forth in this Limited Product Warranty. However, warranty service availability and response times may vary from country to country and may also be subject to registration requirements.

Limitation of Product Warranty

D-LINK warrants that the products described below under normal use are free from material defects in materials and workmanship during the Limited Product Warranty Period set forth below ("Limited Product Warranty Period"), if the product is used and serviced in accordance with the user manual and other documentation provided to the purchaser at the time of purchase (or as amended from time to time). D-LINK does not warrant that the products will operate uninterrupted or error-free or that all deficiencies, errors, defects or non-conformities will be corrected.

This warranty shall not apply to problems resulting from: (a) unauthorised alterations or attachments; (b) negligence, abuse or misuse, including failure to operate the product in accordance with specifications or interface requirements; (c) improper handling; (d) failure of goods or services not obtained from D-LINK or not subject to a then-effective D-LINK warranty or maintenance agreement; (e) improper use or storage; or (f) fire, water, acts of God or other catastrophic events. This warranty shall also not apply to any particular product if any D-LINK serial number has been removed or defaced in any way.

D-LINK IS NOT RESPONSIBLE FOR DAMAGE THAT OCCURS AS A RESULT OF YOUR FAILURE TO FOLLOW THE INSTRUCTIONS FOR THE D-LINK HARDWARE PRODUCT.

Limited Product Warranty Period

The Limited Product Warranty Period starts on the date of purchase from D-LINK. Your dated sales or delivery receipt, showing the date of purchase of the product, is your proof of the purchase date. You may be required to provide proof of purchase as a condition of receiving warranty service. You are entitled to warranty service according to the terms and conditions of this document if a repair to your D-LINK branded hardware is required within the Limited Product Warranty Period.

This Limited Product Warranty extends only to the original end-user purchaser of this D-LINK Hardware Product and is not transferable to anyone who obtains ownership of the D-LINK Hardware Product from the original end-user purchaser.

Product Type	Product Warranty Period
Managed Switches (i.e. switches with built in SNMP agent)(including modules and management software)	Five (5) years
All other products	Two (2) years
Spare parts (i.e. External Power Adapters, Fans)	One (1) year

The warranty periods listed above are effective in respect of all D-LINK products sold in European Countries by D-LINK or one of its authorized resellers or distributors from 1st of January 2004. All products sold in European Countries by D-LINK or one of its authorized resellers or distributors before 1st January 2004 carry 5 years warranty, except power supplies, fans and accessories that are provided with 2 year warranty.

The warranty period stated in this card supersedes and replaces the warranty period as stated in the user's manual or in the purchase contract for the relevant products. For the avoidance of doubt, if you have purchased the relevant D-LINK product as a consumer your statutory rights remain unaffected.

Performance of the Limited Product Warranty

If a product defect occurs, D-LINK's sole obligation shall be to repair or replace any defective product free of charge to the original purchaser provided it is returned to an Authorized D-LINK Service Center during the warranty period. Such repair or replacement will be rendered by D-LINK at an Authorized D-LINK Service Center. All component parts or hardware products removed under this limited warranty become the property of D-LINK. The replacement part or product takes on the remaining limited warranty status of the removed part or product. The replacement product need not be new or of an identical make, model or part; D-LINK may in its discretion replace the defective product (or any part thereof) with any reconditioned equivalent (or superior) product in all material respects to the defective product. Proof of purchase may be required by D-LINK.

Warrantor

D-Link (Europe) Ltd.

4th Floor, Merit House

Edgware Road

Colindale

London NW9 5 AB

United Kingdom

Telephone: +44-020-8731-5555

Facsimile: +44-020-8731-5511

www.dlink.co.uk

D-Link Europe Limited Produktgarantie

Allgemeine Bedingungen

Die hierin beschriebene eingeschränkte Garantie wird durch D-LINK (Europe) Ltd. gewährt (im Folgenden: „D-LINK"). Diese eingeschränkte Garantie setzt voraus, dass der Kauf des Produkts nachgewiesen wird. Auf Verlangen von D-LINK muss auch dieser Garantieschein vorgelegt werden.

AUSSER IN DEM HIER AUSDRÜCKLICH BESCHRIEBENEN UMFANG GEWÄHRT D-LINK KEINE WEITEREN GARANTIEN, WEDER AUSDRÜCKLICH NOCH STILLSCHWEIGEND. INSBESONDERE WIRD NICHT STILLSCHWEIGEND EINE GARANTIE FÜR DIE ALLGEMEINE GEBRAUCHSTAUGLICHKEIT ODER DIE EIGNUNG FÜR EINEN BESTIMMTEN ZWECK ERKLÄRT. D-LINK LEHNT AUSDRÜCKLICH JEDE GARANTIE AB, DIE ÜBER DIESE EINGESCHRÄNKTE GARANTIE HINAUSGEHT. JEDE GESETZLICH ANGEORDNETE GARANTIE IST AUF DIE LAUFZEIT DER EINGESCHRÄNKTEN GARANTIE BESCHRÄNKT. IN EINIGEN STAATEN ODER LÄNDERN IST DIE ZEITLICHE BESCHRÄNKUNG EINER STILLSCHWEIGEND ERKLÄRTEN GARANTIE SOWIE AUSSCHLUSS ODER BESCHRÄNKUNG VON SCHADENERSATZ FÜR NEBEN- ODER FOLGESCHÄDEN BEIM VERBRAUCHSGÜTERKAUF UNTERSAGT. SOWEIT SIE IN SOLCHEN STAATEN ODER LÄNDERN LEBEN, ENTFALTEN MÖGLICHERWEISE EINIGE AUSSCHLÜSSE ODER EINSCHRÄNKUNGEN DIESER EINGESCHRÄNKTEN GARANTIE GEGENÜBER IHNEN KEINE WIRKUNG. DIESE EINGESCHRÄNKTE GARANTIE GEWÄHRT IHNEN SPEZIFISCHE RECHTE. DARÜBER HINAUS STEHEN IHNEN MÖGLICHERWEISE NOCH WEITERE RECHTE ZU, DIE SICH JEDOCH VON STAAT ZU STAAT ODER VON LAND ZU LAND UNTERSCHEIDEN KÖNNEN. UM DEN UMFANG IHRER RECHTE ZU BESTIMMEN, WIRD IHNEN EMPFOHLEN, DIE ANWENDBAREN GESETZE DES JEWEILIGEN STAATES ODER LANDES ZU RATE ZU ZIEHEN.

Diese eingeschränkte Garantie ist auf Hardware-Produkte der Marke D-LINK (insgesamt im Folgenden: „D-LINK Hardware-Produkte") anwendbar, die von D-LINK (Europe) Ltd. oder dessen weltweiten Filialen, Tochtergesellschaften, Fachhändlern oder Länderdistributoren (insgesamt im Folgenden: „D-LINK") mit dieser eingeschränkten Garantie verkauft wurden. Der Begriff „D-LINK Hardware-Produkte" beinhaltet nur Hardwarekomponenten und deren Bestandteile einschließlich Firmware. Der Begriff "D-LINK Hardware-Produkte" umfasst KEINE Software-Anwendungen oder -programme.

Räumlicher Geltungsbereich der eingeschränkten Garantie

Diese eingeschränkte Garantie gilt für alle genannten europäischen Staaten gemäß dem Anhang „Eingeschränkte Garantie von D-LINK in europäischen Staaten". Im Rahmen dieser eingeschränkten Garantie sind mit dem Begriff „europäische Staaten" nur die im Anhang genannten Staaten gemeint. Die eingeschränkte Garantie findet überall Anwendung, wo D-LINK oder dessen autorisierte Servicepartner Garantiedienste gemäß den Bestimmungen dieser eingeschränkten Garantie erbringen. Gleichwohl kann sich die Verfügbarkeit von Garantiediensten und die Bearbeitungszeit von Land zu Land unterscheiden und von Registrierungsanforderungen abhängig sein.

Einschränkung der Garantie

D-LINK gewährleistet, dass die nachstehend aufgeführten Produkte bei gewöhnlicher Verwendung für die unten angegebene Laufzeit der eingeschränkten Garantie („Garantielaufzeit") frei von wesentlichen Verarbeitungs- und Materialfehlern sind. Voraussetzung hierfür ist jedoch, dass das Produkt entsprechend dem Benutzerhandbuch und den weiteren Dokumentationen, die der Benutzer beim Kauf (oder später) erhalten hat, genutzt und gewartet wird. D-LINK garantiert nicht, dass die Produkte störungs- oder fehlerfrei arbeiteten oder dass alle Mängel, Fehler, Defekte oder Kompatibilitätsstörungen beseitigt werden können.

Diese Garantie gilt nicht für Probleme wegen: (a) unerlaubter Veränderung oder Hinzufügung, (b) Fahrlässigkeit, Missbrauch oder Zweckentfremdung, einschließlich des Gebrauchs des Produkts entgegen den Spezifikationen oder den durch Schnittstellen gegebenen Vorgaben, (c) fehlerhafter Bedienung, (d) Versagen von Produkten oder Diensten, die nicht von D-LINK stammen oder nicht Gegenstand einer zum maßgeblichen Zeitpunkt gültigen Garantie- oder

Wartungsvereinbarung sind, (e) Fehlgebrauch oder fehlerhafter Lagerung oder (f) Feuer, Wasser, höherer Gewalt oder anderer Katastrophen. Diese Garantie gilt ebenfalls nicht für Produkte, bei denen eine D-LINK-Seriennummer entfernt oder auf sonstige Weise unkenntlich gemacht wurde.

D-LINK STEHT NICHT FÜR SCHÄDEN EIN, DIE DADURCH ENTSTEHEN, DASS DIE ANLEITUNG FÜR DAS D-LINK HARDWARE-PRODUKT NICHT BEFOLGT WIRD.

Laufzeit der eingeschränkten Garantie

Die Laufzeit der eingeschränkten Garantie beginnt mit dem Zeitpunkt, zu dem das Produkt von D-LINK gekauft wurde. Als Nachweis für den Zeitpunkt des Kaufs gilt der datierte Kauf- oder Lieferbeleg. Es kann von Ihnen verlangt werden, dass Sie zur Inanspruchnahme von Garantiediensten den Kauf des Produkts nachweisen. Wenn Ihre Hardware-Produkte der Marke D-LINK innerhalb der Laufzeit der eingeschränkten Garantie eine Reparatur benötigen, so sind Sie berechtigt, gemäß den Bedingungen dieser eingeschränkten Garantie Garantiedienste in Anspruch zu nehmen.

Diese eingeschränkte Garantie gilt nur für denjenigen, der das D-LINK Hardware-Produkt ursprünglich als originärer Endbenutzer gekauft hat. Sie ist nicht auf Dritte übertragbar, die das D-LINK-Produkt von dem ursprünglichen originären Endbenutzer erworben haben.

Produkttyp	Gewährleistungslaufzeit
Verwaltete Switches (d. h. Switches mit eingebauten SNMP-Agents) (einschließlich Modulen und Verwaltungssoftware)	Fünf (5) Jahre
Alle weiteren Produkte	Zwei (2) Jahre
Ersatzteile (z.B. externe Netzteile, Lüfter)	Ein (1) Jahr

Die oben aufgeführten Garantielaufzeiten gelten für alle D-LINK-Produkte, die in europäischen Staaten ab dem 1. Januar 2004 von D-LINK oder einem autorisierten Fachhändler oder Distributor verkauft werden. Alle vor dem 1. Januar 2004 von D-LINK oder einem autorisierten Vertragshändler oder Distributor verkauften Produkte haben eine Gewährleistung von 5 Jahren; ausgenommen sind Netzteile, Lüfter und Zubehör, diese haben eine Garantie von 2 Jahren.

Die durch diesen Garantieschein festgelegte Garantielaufzeit tritt an die Stelle der im Benutzerhandbuch oder im Kaufvertrag für das jeweilige Produkt angegebenen Laufzeit. Sollten Sie das betreffende D-LINK-Produkt als Verbraucher erworben haben, so sei klargestellt, dass Ihre gesetzlichen Rechte hiervon unberührt bleiben.

Leistungsumfang der eingeschränkten Garantie

Bei Auftreten eines Produktfehlers besteht die einzige Verpflichtung von D-LINK darin, dem ursprünglichen Käufer das defekte Produkt kostenlos zu reparieren oder es auszutauschen. Voraussetzung hierfür ist, dass das Produkt während der Garantielaufzeit einem autorisierten D-LINK-Servicecenter übergeben wird. Reparatur oder Austausch werden von D-LINK durch ein autorisiertes D-LINK-Servicecenter durchgeführt. Bauteile oder Hardware-Produkte, die gemäß dieser eingeschränkten Garantie entfernt werden, gehen in das Eigentum von D-LINK über. Die verbliebene eingeschränkte Garantie des entfernten Teils oder Produkts wird auf das Ersatzteil oder -produkt übertragen. Das Austauschprodukt muss weder neu sein noch dem defekten Produkt ganz oder in Teilen entsprechen. D-LINK darf dieses nach eigenem Ermessen gegen ein entsprechendes wiederaufbereitetes Produkt austauschen, welches dem defekten Produkt im Wesentlichen entspricht (oder höherwertig ist). D-LINK kann verlangen, dass der Kauf des Produkts nachgewiesen wird.

DIE VORSTEHENDE GARANTIE WURDE IN DIE DEUTSCHE SPRACHE AUS DEM ENGLISCHEN ÜBERSETZT. BEI ABWEICHUNGEN ZWISCHEN DER ENGLISCHEN VERSION UND DER DEUTSCHEN ÜBERSETZUNG GELTEN DIE BESTIMMUNGEN DER ENGLISCHEN VERSION.

Garantiegeber

D-Link (Europe) Ltd.

4th Floor, Merit House

Edgware Road

Colindale

London NW9 5 AB

Vereinigtes Königreich

Telefon: +44-020-8731-5555

Fax: +44-020-8731-5511

www.dlink.com

D-Link Europe a limité la garantie des produits

Conditions Générales

La Garantie Produit Limitée énoncée ci-dessous émane de D-LINK (Europe) Ltd. (ci-après « D-LINK »). Cette Garantie Produit Limitée n'est valable que sur présentation de la preuve d'achat. D-LINK peut également exiger la présentation du présent bon de garantie.

SAUF INDICATION EXPLICITE DES PRESENTES, D-LINK NE FOURNIT AUCUNE AUTRE GARANTIE, EXPLICITE OU IMPLICITE, Y COMPRIS UNE GARANTIE IMPLICITE DE VALEUR MARCHANDE OU D'ADAPTATION DU PRODUIT A UN USAGE PRECIS. D-LINK DECLINE EXPLICITEMENT TOUTE GARANTIE NON ENONCEE DANS LES PRESENTES. TOUTE GARANTIE IMPLICITE IMPOSEE PAR LA LOI, LE CAS ECHEANT, EST LIMITEE DANS SA DUREE A CELLE DE LA GARANTIE LIMITEE. CERTAINS ETATS OU PAYS NE PERMETTENT PAS DE LIMITER LA DUREE DE LA GARANTIE IMPLICITE OU INTERDISENT D'EXCLURE OU DE LIMITER LA COUVERTURE DES DOMMAGES

DIRECTS OU INDIRECTS OCCASIONNES AUX PRODUITS GRAND PUBLIC. DANS LES ETATS OU PAYS EN QUESTION, CERTAINES EXCLUSIONS OU LIMITATIONS DE LA PRESENTE GARANTIE PEUVENT NE PAS S'APPLIQUER A VOTRE CAS. LA PRESENTE GARANTIE LIMITEE VOUS OCTROIE CERTAINS DROITS LEGAUX SPECIFIQUES. VOUS POUVEZ EGALEMENT BENEFICIER D'AUTRES DROITS VARIABLES D'UN ETAT OU D'UN PAYS A L'AUTRE. NOUS VOUS RECOMMANDONS DE CONSULTER LA LEGISLATION EN VIGUEUR DANS VOTRE LIEU DE RESIDENCE POUR CONNAITRE L'ETENDUE DE VOS DROITS.

La présente garantie limitée s'applique aux produits matériels commercialisés sous la marque D-LINK (collectivement ici « les Produits Matériels D-LINK) vendus par D-LINK (Europe) Ltd., ses filiales, sociétés affiliées, revendeurs agréés ou distributeurs locaux à travers le monde (collectivement ici « D-LINK ») avec la présente garantie limitée. Le terme de « Produit Matériel D-LINK » se limite aux composants matériels et à l'ensemble de leurs composants internes, notamment le firmware. Le terme de « Produit Matériel D-LINK » N'englobe PAS les applications ou programmes logiciels.

Etendue géographique de la Garantie Produit Limitée

La présente Garantie Produit Limitée s'applique à tous les pays européens figurant dans l'annexe « Pays européens où s'applique la Garantie Produit Limitée D-LINK ». Le terme de « pays européens » utilisé dans la présente Garantie Produit Limitée D-LINK englobe uniquement les pays figurant dans la liste en annexe. La Garantie Produit Limitée sera honorée dans tout pays où D-LINK ou ses prestataires agréés proposent le service de garantie, sous réserve des modalités énoncées dans la présente Garantie Produit Limitée. Cependant, la disponibilité du service de garantie et les temps de réponse varient d'un pays à l'autre et peuvent également être assujettis à un enregistrement.

Limitation de la Garantie Produit

D-LINK garantit que les produits décrits ci-dessous, dans le cadre d'une utilisation normale, sont dénués de défauts conséquents, tant au niveau de leurs composants matériels que de leur fabrication, et ce pendant toute la Période de Garantie Produit Limitée indiquée ci-dessous (« Période de Garantie Produit Limitée »), sous réserve qu'ils soient utilisés et entretenus conformément au manuel utilisateur et aux autres documents remis au client lors de l'achat (ou amendés de temps à autre). D-LINK ne garantit pas le fonctionnement ininterrompu ou sans erreur de ses produits. D-LINK ne s'engage pas non plus à corriger tous les défauts, erreurs ou non conformités.

La présente garantie ne s'applique pas aux problèmes qui sont la conséquence : (a) d'altérations ou d'ajouts non autorisés ; (b) d'une négligence, d'un abus ou d'une mauvaise utilisation, notamment une utilisation du produit non conforme à ses spécifications ou aux interfaces requises ; (c) d'une mauvaise manipulation ; (d) d'une panne de biens ou de services acquis auprès d'une société tierce (non D-LINK) ou qui ne font pas l'objet d'un contrat D-LINK de garantie ou de maintenance en bonne et due forme ; (e) d'une mauvaise utilisation ou d'un rangement dans des conditions inadaptées ; ou (f) du feu, de l'eau, d'une catastrophe naturelle ou autre. La présente garantie ne s'applique pas non plus à un produit dont le numéro de série D-LINK aurait été retiré ou altéré de quelque manière que ce soit.

D-LINK N'EST NULLEMENT RESPONSABLE DE DOMMAGES RESULTANT DE VOTRE INOBSERVATION DES INSTRUCTIONS FOURNIES POUR L'UTILISATION DE SON PRODUIT MATERIEL.

Période de Garantie Produit Limitée

La Période de Garantie Produit Limitée court à compter de la date d'achat auprès de D-LINK. La date de votre reçu ou bon de livraison correspond à la date d'achat du produit et constitue la date de votre preuve d'achat. Il est possible que le service de garantie ne vous soit accordé que sur production de votre preuve d'achat. Vous avez droit à un service de garantie conforme aux modalités énoncées dans les présentes dès lorsque que votre matériel de marque D-LINK nécessite une réparation pendant la Période de Garantie Produit Limitée.

La présente Garantie Produit Limitée s'applique uniquement à l'acheteur utilisateur final initial du Produit Matériel D-LINK. Elle est non cessible à quiconque se procure le Produit Matériel D-LINK auprès de l'acheteur utilisateur final initial.

Type de produit	Période de Garantie
Switches gérés (switches comportant un agent SNMP intégré)(y compris modules et logiciels de gestion)	Cinq (5) ans
Tous autres produits	Deux (2) ans
Pièces détachées (adaptateurs d'alimentation externes, ventilateurs)	Un (1) an

Les périodes de garantie indiquées ci-dessus s'appliquent à tous les produits D-LINK vendus depuis le 1er janvier 2004 dans les pays européens par D-LINK ou l'un de ses revendeurs ou distributeurs agréés. Tous les produits vendus avant le 1er janvier 2004 dans les pays européens par D-LINK ou l'un de ses revendeurs ou distributeurs agréés bénéficient d'une garantie de 5 ans, excepté les fournitures électriques, ventilateurs et accessoires, qui sont couverts par une garantie de 2 ans.

La période de garantie indiquée sur ce bon annule et remplace celle qui figure dans le manuel utilisateur ou dans le contrat d'achat des produits considérés. Pour éviter le doute, si vous avez acheté votre produit D-LINK en tant que consommateur, vos droits légaux demeurent inchangés.

Exécution de la Garantie Produit Limitée

En cas de défaut ou d'erreur d'un produit, l'unique obligation de D-LINK se limite à la réparation ou au remplacement gratuit du produit défectueux, au bénéfice de l'acheteur initial, sous réserve que le produit soit rapporté à un Centre de Service Agréé D-LINK pendant la période de garantie. D-LINK assure la réparation ou le remplacement dans un Centre de Service Agréé D-LINK. Les composants, pièces ou produits retirés dans le cadre de cette garantie limitée deviennent propriété de D-LINK. La pièce ou le produit de remplacement est couvert par la garantie limitée de la pièce ou du produit d'origine pendant la période restante. Le produit de remplacement n'est pas nécessairement neuf, ni d'une marque ou d'un modèle identique ; D-LINK peut décider, de manière discrétionnaire, de remplacer le produit défectueux (ou ses pièces) par un équivalent (ou un article supérieur) reconditionné ayant toutes les fonctionnalités du produit défectueux. D-LINK peut exiger la preuve d'achat.

Garant

D-Link (Europe) Ltd.

4th Floor, Merit House

Edgware Road

Colindale

London NW9 5 AB

Royaume-Uni

Tél : +44-020-8731-5555

Fax : +44-020-8731-5511

www.dlink.co.uk

Garantía limitada del producto D-LINK Europa

Condiciones generales

Esta garantía la ofrece D-LINK (Europe) Ltd. (en este documento, "D-LINK"). La garantía limitada del producto sólo es válida si se acompaña del comprobante de la compra. También deberá presentarse la tarjeta de garantía si D-LINK lo solicita.

EXCEPTO EN LO EXPRESAMENTE INDICADO EN ESTA GARANTÍA LIMITADA, D-LINK NO CONCEDE OTRAS GARANTÍAS, NI EXPLÍCITAS NI IMPLÍCITAS, INCLUIDAS LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIDAD Y APTITUD A UN FIN DETERMINADO. D-LINK RECHAZA EXPLÍCITAMENTE CUALQUIER GARANTÍA QUE NO FIGURE EN ESTA GARANTÍA LIMITADA. LA DURACIÓN DE CUALQUIER GARANTÍA IMPLÍCITA QUE PUEDA SER IMPUESTA POR LEY QUEDA LIMITADA AL PERÍODO DE LA GARANTÍA LIMITADA. ALGUNOS ESTADOS O PAÍSES NO PERMITEN QUE EN LA GARANTÍA LIMITADA DE PRODUCTOS DE CONSUMO SE RESTRINJA LA DURACIÓN TEMPORAL, NI QUE SE EXCLUYAN O LIMITEN LOS DAÑOS INCIDENTALES O RESULTANTES PARA EL CONSUMIDOR DE LOS PRODUCTOS. EN ESTOS ESTADOS O PAÍSES, A USTED NO LE PUEDEN APLICAR ALGUNAS EXCLUSIONES O LIMITACIONES DE LA GARANTÍA LIMITADA. ESTA GARANTÍA LIMITADA LE CONCEDE DETERMINADOS DERECHOS. PUEDE, TAMBIÉN, TENER OTROS DERECHOS, QUE PUEDEN SER DISTINTOS DE UN ESTADO A OTRO O DE UN PAÍS A OTRO. SE RECOMIENDA QUE CONSULTE LAS LEYES PERTINENTES DE UN ESTADO O PAÍS A FIN DE QUE CONOZCA SUS DERECHOS.

Esta garantía limitada se aplica a los productos de hardware de la marca D-LINK (llamados en esta guía “Productos de hardware D-LINK”) comprados a D-LINK (Europe) Ltd., a sus filiales en el mundo, a sus proveedores autorizados o a sus distribuidores locales (llamados en este documento “D-LINK”) con esta garantía limitada. El término “producto de hardware D-LINK” se restringe a los componentes de hardware y a los componentes internos de estos, incluyendo el firmware. El término “producto de hardware D-LINK” NO incluye ni las aplicaciones ni los programas de software.

Cobertura geográfica de la garantía limitada del producto

Esta garantía limitada del producto es válida en todos los países europeos que figuran en el apéndice “Países europeos de la garantía limitada del producto D-LINK”. En esta garantía limitada del producto D-Link, el término “países europeos” sólo incluye los países que figuran en el apéndice. La garantía limitada del producto será válida en cualquier país en el que D-LINK o sus proveedores autorizados de servicios ofrezcan un servicio de garantía sujeto a los términos y condiciones recogidos en esta garantía limitada del producto. Sin embargo, la disponibilidad del servicio de garantía, así como el tiempo de respuesta, pueden variar de un país a otro y pueden estar sujetos a requisitos de registro.

Limitación de la garantía del producto

D-LINK garantiza que los productos descritos más adelante están libres de defectos de fabricación y materiales, en condiciones normales de uso, a lo largo del período de la garantía limitada del producto que se indica en este documento ("período de la garantía limitada del producto"), si el producto se ha utilizado y mantenido conforme a lo recogido en el manual del usuario o en otra documentación que se haya proporcionado al comprador en el momento de la compra (o que se haya corregido). D-LINK no garantiza que los productos funcionarán sin interrupciones o sin errores, ni que se corregirán todas las deficiencias, errores, defectos o disconformidades.

Esta garantía no cubre problemas derivados de: (a) modificaciones o conexiones no autorizadas; (b) negligencia, abuso o mal uso, incluyendo el incumplimiento de las especificaciones y de los requisitos de la interfaz en el funcionamiento del producto; (c) manejo incorrecto; (d) errores en artículos o servicios ajenos a D-LINK o no sujetos a una garantía o un contrato de mantenimiento vigentes de D-LINK; (e) uso o almacenamiento incorrecto; o (f) fuego, agua, casos fortuitos u otros hechos catastróficos. Esta garantía tampoco es válida para aquellos productos a los que se haya eliminado o alterado de algún modo el número de serie D-LINK.

D-LINK NO SE RESPONSABILIZA DE LOS DAÑOS CAUSADOS COMO CONSECUENCIA DEL INCUMPLIMIENTO DE LAS INSTRUCCIONES DEL PRODUCTO DE HARDWARE D-LINK.

Período de la garantía limitada del producto

El período de la garantía limitada del producto se inicia en la fecha en que se realizó la compra a D-LINK. Para el comprador, el comprobante de la fecha de la compra es el recibo de la venta o de la entrega, en el que figura la fecha de la compra del producto. Puede ser necesario tener que presentar el comprobante de la compra a fin de que se preste el servicio de garantía. El comprador tiene derecho al servicio de garantía conforme a los términos y condiciones de este documento, si requiere una reparación del hardware de la marca D-LINK dentro del período de garantía limitada del producto.

Esta garantía limitada del producto cubre sólo al originario comprador-usuario final de este producto de hardware D-LINK, y no es transferible a otras personas que reciban el producto de hardware D-LINK del originario comprador-usuario final.

Tipo de producto	Período de garantía del producto
Conmutadores gestionados (p. ej., conmutadores con agente SNMP integrado) (incluyendo módulos y software de gestión)	Cinco (5) años

Resto de productos	Dos (2) años
Piezas de repuesto (p. ej., adaptadores de alimentación externos, ventiladores)	Un (1) año

Estos períodos de garantía están en vigor para todos los productos D-LINK que hayan sido comprados en países europeos a D-LINK o a alguno de sus proveedores o distribuidores autorizados a partir del 1 de enero del 2004. Todos los productos comprados en países europeos a D-LINK o a uno de sus proveedores o distribuidores autorizados antes del 1 de enero del 2004 cuentan con 5 años de garantía, excepto las fuentes de alimentación, los ventiladores y los accesorios, que cuentan con 2 años de garantía.

El período de garantía que figura en esta tarjeta sustituye y reemplaza al período de garantía que consta en el manual del usuario o en el contrato de compra de los productos correspondientes. Para evitar dudas: si usted ha comprado el producto D-LINK correspondiente como consumidor, sus derechos legales no se ven afectados.

Uso de la garantía limitada del producto

Si un producto presenta algún defecto, la obligación exclusiva de D-LINK será reparar o reemplazar, sin coste alguno para el comprador originario, cualquier producto defectuoso siempre y cuando éste sea entregado en un centro autorizado de servicio D-LINK durante el período de garantía. D-LINK realizará la reparación o sustitución para un centro autorizado de servicio D-LINK. Todos los productos de hardware o componentes que se eliminen bajo esta garantía limitada serán propiedad de D-LINK. La parte o el producto de repuesto adquiere, para el resto de la garantía limitada, el estatus de parte o producto eliminado. El producto de repuesto no ha de ser nuevo o de la misma marca, modelo o parte; D-LINK puede sustituir a discreción el producto defectuoso (o cualquier parte) con un producto equivalente reacondicionado (o superior) en cualquier material respecto al producto defectuoso. D-LINK puede pedir el comprobante de compra.

Garante

D-Link (Europe) Ltd.

4th Floor, Merit House

Edgware Road

Colindale

London NW9 5 AB

United Kingdom

Teléfono: +44-020-8731-5555

Fax: +44-020-8731-5511

www.dlink.co.uk

D-Link Europe Termini di Garanzia dei Prodotti

Generalità

La presente Garanzia viene fornita da D-LINK (Europe) Ltd. (di seguito denominata "D-LINK"). Essa viene riconosciuta solo se accompagnata dalla prova di acquisto. D-LINK può richiedere anche l'esibizione della presente cartolina di garanzia.

SALVO QUANTO ESPRESSAMENTE STABILITO NELLA PRESENTE GARANZIA LIMITATA, D-LINK NON FORNISCE NESSUN'ALTRA GARANZIA NE' ESPRESSA NE' IMPLICITA, COMPRESE EVENTUALI GARANZIE DI COMMERCIABILITÀ O DI IDONEITÀ PER UN PARTICOLARE SCOPO. D-LINK NEGA ESPRESSAMENTE QUALUNQUE ALTRA GARANZIA CHE NON RIENTRI NELLA PRESENTE GARANZIA LIMITATA. QUALSIASI GARANZIA IMPLICITA, CHE DOVESSE ESSERE IMPOSTA PER LEGGE, SARÀ CIRCOSCRITTA ALLA DURATA DELLA PRESENTE GARANZIA. ALCUNI PAESI VIETANO QUALSIASI LIMITAZIONE DEL PERIODO DI VALIDITÀ DELLE GARANZIE IMPLICITE OPPURE L'ESCLUSIONE O LA LIMITAZIONE DEI DANNI INCIDENTALI O CONSEQUENZIALI PER I PRODOTTI. IN TALI PAESI, EVENTUALI ESCLUSIONI O LIMITAZIONI DELLA PRESENTE GARANZIA NON POTRANNO APPLICARSI AL VOSTRO CASO. LA PRESENTE GARANZIA VI CONFERISCE DIRITTI LEGALI SPECIFICI. INOLTRE POTRETE GODERE DI ULTERIORI DIRITTI CHE POSSONO VARIARE A SECONDA DEL PAESE. SIETE INVITATI A CONSULTARE LE LEGGI APPLICABILI DEL VOSTRO PAESE AL FINE DI DETERMINARE CON PRECISIONE I VOSTRI DIRITTI.

La presente garanzia trova applicazione su tutti i prodotti hardware recanti il marchio D-LINK (di seguito denominati collettivamente "Prodotti hardware D-LINK") venduti da D-LINK (Europe) Ltd., dalle sue controllate, dalle sue affiliate, dai rivenditori autorizzati o dai distributori nazionali (di seguito denominati collettivamente "D-LINK"), accompagnati dalla presente garanzia limitata. Il termine "Prodotto hardware D-LINK" si riferisce esclusivamente ai componenti hardware e a tutte le parti interne compreso il firmware. Il termine "Prodotto hardware D-LINK" NON comprende eventuali applicazioni o programmi software.

Ambito geografico della Garanzia limitata

La presente Garanzia è estesa a tutti i Paesi europei elencati nell'appendice "Paesi europei - Garanzia limitata dei prodotti D-LINK". Il termine "Paesi europei" si riferisce esclusivamente ai paesi nominati in questa appendice. La Garanzia verrà riconosciuta in tutti i paesi nei quali D-LINK o i suoi Centri di Assistenza

autorizzati offrono assistenza conformemente alle condizioni e ai termini stabiliti nella presente Garanzia. Tuttavia, la disponibilità all'assistenza e i tempi di intervento variano da paese a paese e possono essere soggetti a eventuali requisiti di registrazione.

Limitazione della Garanzia

D-LINK garantisce che i prodotti sotto descritti in condizioni di normale utilizzo non presentano difetti di fabbricazione o vizi di materiale durante il Periodo di garanzia sotto specificato ("Periodo di garanzia"), a condizione che vengano utilizzati e sottoposti a manutenzione in conformità con il manuale d'uso e con ogni altra documentazione fornita all'acquirente all'atto dell'acquisto (e relativi emendamenti). D-LINK non garantisce che il funzionamento del prodotto sarà ininterrotto o esente da errori né tanto meno che tutti gli eventuali errori, carenze, difetti o non conformità potranno essere corretti.

La presente garanzia non copre eventuali problemi derivanti da: (a) alterazioni o aggiunte non autorizzate; (b) negligenza, abuso o utilizzo improprio, compresa l'incapacità di far funzionare il prodotto in conformità con le specifiche e i requisiti di connessione; (c) movimentazione impropria; (d) guasto di prodotti o servizi non forniti da D-LINK o non soggetti a una garanzia successiva di D-LINK o a un accordo di manutenzione; (e) impiego o conservazione impropri; (f) incendio, inondazione, cause di forza maggiore o altro evento catastrofico accidentale. La presente garanzia non si applica altresì ad alcun prodotto particolare qualora il numero di serie di D-LINK sia stato rimosso o reso illeggibile in altro modo.

D-LINK DECLINA OGNI RESPONSABILITÀ PER EVENTUALI DANNI RISULTANTI DAL MANCATO RISPETTO DELLE ISTRUZIONI RELATIVE AL PRODOTTO HARDWARE D-LINK.

Periodo di garanzia

Il Periodo di garanzia ha decorrenza dalla data dell'acquisto presso D-LINK. Prova della data di acquisto è il documento fiscale (scontrino fiscale o ricevuta) recante la data di acquisto del prodotto. Per avere diritto alla garanzia può esserVi richiesto di esibire la prova di acquisto. Potete beneficiare delle prestazioni di assistenza previste dalla garanzia in conformità con i termini e le condizioni di cui sotto nel momento in cui il Vostro prodotto hardware D-LINK necessiti di una riparazione durante il Periodo di garanzia.

La presente Garanzia si applica esclusivamente al primo acquirente del Prodotto hardware D-LINK e non può essere trasferita a terzi che abbiano ottenuto la proprietà del Prodotto hardware D-LINK dal primo acquirente.

Tipo di prodotto	Periodo di garanzia
Switch (solo switch dotati di agente SNMP incorporato) (inclusi moduli e software di gestione)	5 (cinque) anni
Tutti gli altri prodotti	2 (due) anni
Pezzi di ricambio (es. adattatori esterni di potenza, alimentatori esterni, ventole)	1 (un) anno

Il periodo di garanzia sopra specificato relativamente a tutti i prodotti D-LINK venduti nei Paesi europei da D-LINK o da qualsiasi suo rivenditore o distributore autorizzato decorre dal 1° gennaio 2004. Tutti i prodotti venduti nei Paesi europei da D-LINK o da uno qualsiasi dei suoi rivenditori o distributori autorizzati prima del 1° gennaio 2004 sono coperti da una garanzia di 5 anni fatto salvo per alimentatori, ventole e accessori che hanno 2 anni di garanzia.

Il periodo di garanzia qui menzionato sostituisce qualsiasi altro periodo di garanzia definito nel manuale d'uso o nel contratto di acquisto del prodotto. Se avete acquistato un prodotto D-LINK in qualità di consumatore i Vostri diritti rimangono invariati.

Prestazioni della Garanzia limitata

Qualora comparisse un difetto o una non conformità, D-LINK avrà l'unico obbligo di riparare o sostituire il prodotto non conforme senza alcun costo per l'acquirente a condizione che il prodotto venga restituito a un Centro di Assistenza autorizzato D-LINK entro il periodo di garanzia. La riparazione o la sostituzione verranno eseguite da D-LINK presso un Centro di Assistenza autorizzato D-LINK. Tutti i componenti o i prodotti hardware rimossi conformemente ai termini e alle condizioni della presente garanzia divengono di proprietà di D-LINK. Il pezzo o il prodotto in sostituzione beneficerà della garanzia per il tempo residuo della parte o del prodotto originale. Il prodotto in sostituzione non deve necessariamente essere nuovo o di identica fattura, modello o composizione; D-LINK può a sua discrezione sostituire il prodotto non conforme (o qualsiasi parte di esso) con un prodotto che risulti essere equivalente (o di valore superiore) al prodotto non conforme. D-LINK può richiedere che venga esibita la prova di acquisto.

Garante

D-Link (Europe) Ltd.

4th Floor, Merit House

Edgware Road

Colindale

Londra NW9 5 AB

Regno Unito

Telefono: +44-020-8731-5555

Fax: +44-020-8731-5511

www.dlink.co.uk