



# DGS-3224TGR

Layer 2 Switch

## Command Line Interface Reference Manual

---

---

First Edition (October 2003)

6S24TGRCLI01

Printed In China



RECYCLABLE

## **Trademarks**

Copyright ©2003 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 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.

# Table of Contents

---

Introduction .....	1
Using the Console CLI.....	6
Command Syntax.....	14
Basic Switch Commands .....	19
Switch Port Commands .....	44
Network Management Commands .....	49
Download/Upload Commands .....	66
Network Monitoring Commands .....	70
Spanning Tree Commands .....	78
Layer 2 Forwarding Database Commands .....	87
Broadcast Storm Control Commands .....	97
ARP Commands .....	101
QOS Commands .....	106
Port Mirroring Commands .....	121
VLAN Commands .....	128

Link Aggregation Commands.....	141
IP Interface Commands .....	149
IGMP Snooping Commands.....	154
Routing Table Commands .....	168
802.1X Commands .....	173
Access Control List (ACL) Commands.....	197
SSH Commands .....	213
Command History List .....	224
Technical Specifications .....	230

# 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.

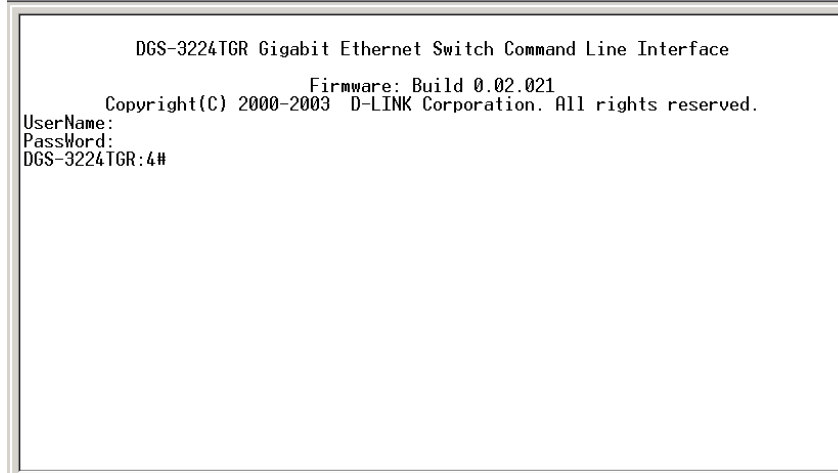
### **Accessing the Switch via the Serial Port**

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.



```
DGS-3224TGR Gigabit Ethernet Switch Command Line Interface
Firmware: Build 0.02.021
Copyright(C) 2000-2003 D-LINK Corporation. All rights reserved.
UserName:
PassWord:
DGS-3224TGR:4#
```

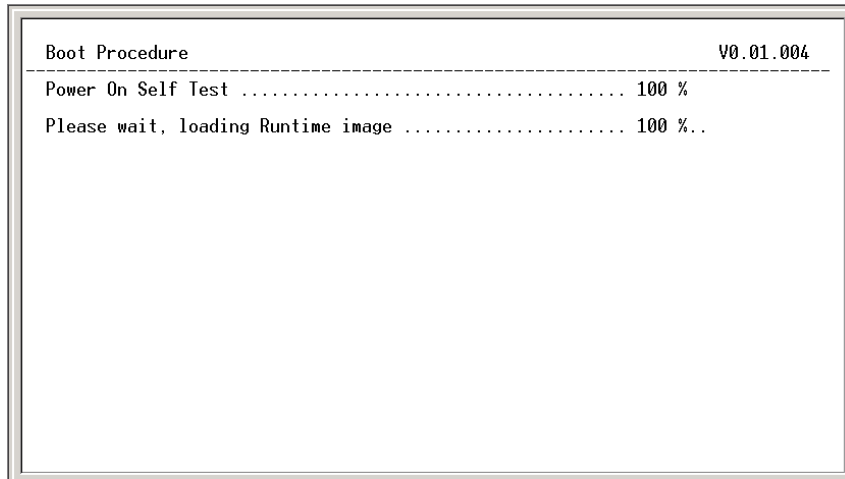
**Figure 1-1. Initial Console screen.**

There is no initial username or password. Just press the **Enter** key twice to display the CLI input cursor – **DGS-3224TGR:4#**. This is the command line where all commands are input.

### **Setting the Switch's IP Address**

Each switch must be assigned its own IP Address, which is used for communication with an SNMP network manager or other TCP/IP application (for example BOOTP or TFTP). The switch's default IP address is 10.90.90.90. You can change the default switch IP address to meet the specification of your networking address scheme.

The switch is also assigned a unique MAC address by the factory that cannot be changed.



**Figure 1-2. Boot Screen**

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

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

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

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

1. Starting at the command line prompt **DGS-3224TGR:4#** – enter the commands **config ipif System ipaddress xxx.xxx.xxx.xxx/yyy.yyy.yyy.yyy**. Where the **x**'s represent the IP address to be assigned to the IP interface named **System** and the **y**'s represent the corresponding subnet mask.
2. Alternatively, you can enter **DGS3224TGR:4#** – enter the commands **config ipif System ipaddress xxx.xxx.xxx.xxx/z**. Where the **x**'s represent the IP address to be assigned to the IP interface named **System** and the **z** represents the corresponding number of subnets in CIDR notation.

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



```
DGS-3224TGR Gigabit Ethernet Switch Command Line Interface
                          Firmware: Build 0.02.021
                          Copyright(C) 2000-2003 D-LINK Corporation. All rights reserved.
UserName:
PassWord:
DGS-3224TGR:4#config ipif System ipaddress 10.24.22.9/255.0.0.0
Command: config ipif System ipaddress 10.24.22.9/8

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

**Figure 1-3. Assigning the Switch an IP Address**

In the above example, the switch was assigned an IP address of 10.24.22.9 with a subnet mask of 255.0.0.0. The system message “Success” indicates that the command was executed successfully. The switch can now be configured and managed via Telnet and the CLI or via the Web-based management agent using the above IP address to connect to the switch.

# 2

---

## ***USING THE CONSOLE CLI***

The DGS-3224TGR supports a console management interface that allows the user to connect to the switch's management agent via a serial port and a terminal or a computer running a terminal emulation program. The console can also be used over the network using the TCP/IP Telnet protocol. The console program can be used to configure the switch to use an SNMP-based network management software over the network.

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



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

### **Connecting to the Switch**

The console interface is used by connecting the switch to a VT100-compatible terminal or a computer running an ordinary

terminal emulator program (e.g., the HyperTerminal program included with the Windows operating system) using an RS-232C serial cable. Your terminal parameters will need to be set to:

- VT-100 compatible
- 9,600 baud
- 8 data bits
- No parity
- One stop bit
- No flow control

You can also access the same functions over a Telnet interface. Once you have set an IP address for your switch, you can use a Telnet program (in VT-100 compatible terminal mode) to access and control the switch. All of the screens are identical, whether accessed from the console port or from a Telnet interface.

After the switch reboots and you have logged in, the console looks like this:

```
DGS-3224TGR Gigabit Ethernet Switch Command Line Interface
                               Firmware: Build 0.02.021
                               Copyright(C) 2000-2003 D-LINK Corporation. All rights reserved.
UserName:
Password:
DGS-3224TGR:4#
```

**Figure 2-1. Initial Console Screen**

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

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

```
..
?
clear
clear arptable
clear counters
clear fdb
clear log
config 802.1p default_priority
config 802.1p user_priority
config 802.1x auth_parameter ports
config 802.1x auth_protocol
config 802.1x capability ports
config 802.1x init ports
config 802.1x reauth ports
config access_profile profile_id
config account
config arp_aging time
config bandwidth_control
config command_history
config fdb aging_time
config gvrp
config igmp_snooping
CTRL+C ESC Quit SPACE Next Page ENTER Next Entry All
```

**Figure 2-2. The ? Command**

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

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

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

Next possible completions:
  <username>

DGS-3224TGR:4#
```

**Figure 2-3. Example Command Parameter Help**

In this case, the command **config account** was entered with the parameter **<username>**. The CLI will then prompt you to enter the **<username>** with the message, **Next possible completions:**. Every command in the CLI has this feature, and complex commands have several layers of parameter prompting.

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

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

Next possible completions:
  <username>

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

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

In the above example, the command **config account** was entered without the required parameter **<username>**, the CLI returned the **Next possible completions: <username>** prompt. The up arrow cursor control key was pressed to re-enter the previous command (**config account**) at the command prompt. Now the appropriate 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-3224TGR:4#help
Available commands:
.. ? clear config create delete
dir disable download enable login logout
ping reboot reset save show upload

DGS-3224TGR:4#
```

**Figure 2-5. The Available Commands Prompt**

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

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



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

Next possible completions:
 802.1p 802.1x access_profile account arpentry auth_diagnostics
auth_session_statistics auth_statistics bandwidth_control command_histor
y error fdb
gvrp hol_prevention igmp_snooping ipif iproute link_aggregation
log_mirror multicast_fdb packet port_security ports
radius realtime router_ports scheduling scheduling_mechanism serial_port

session snmp ssh stp switch syslog
traffic trusted_host utilization vlan

DGS-3224TGR: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 in this manual to describe how command entries are made and values and arguments are specified in this manual. The online help contained in the CLI and available through the console interface uses the same syntax.

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

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

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

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

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

<b>Line Editing Key Usage</b>	
	line to the left.
<b>Insert</b>	Can be toggled on or off. When toggled on, inserts text at the current cursor position and shifts the remainder of the line to the left.
<b>Left Arrow</b>	Moves the cursor to the left.
<b>Right Arrow</b>	Moves the cursor to the right.
<b>Tab</b>	Shifts the cursor to the next field to the left.
<b><i>Multiple Page Display Control Keys</i></b>	
<b>Space</b>	Displays the next page.
<b>CTRL+c</b>	Stops the display of remaining pages when multiple pages are to be displayed.
<b>ESC</b>	Stops the display of remaining pages when multiple pages are to be displayed.
<b>n</b>	Displays the next page.
<b>p</b>	Displays the previous page.
<b>q</b>	Stops the display of remaining pages when multiple pages are to be displayed.
<b>r</b>	Refreshes the pages currently displaying.
<b>a</b>	Displays the remaining pages without pausing between pages.

<b>Line Editing Key Usage</b>	
-------------------------------	--

<b>Enter</b>	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.

<b>Command</b>	<b>Parameters</b>
create account	[admin user] <username 15>
config account	<username>
show account	
delete account	<username>
show session	
show switch	
show serial_port	
config serial_port	{baud_rate [9600 19200 38400 115200] auto_logout(2) [never(0) 2_minutes(2) 5_minutes(5)  10_minutes(10) 15_minutes(15)]}(1)
enable jumbo_frame	
disable jumbo_frame	

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

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

### **create account**

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



## **create account**

Parameters	Admin <username> User <username>
Restrictions	Only Administrator-level users can issue this command.  Usernames can be between 1 and 15 characters.  Passwords can be between 0 and 15 characters.

### Example Usage:

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

```
DGS-3224TGR:4#create account admin dlink
Command: create account admin dlink

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

DGS-3224TGR:4#
```

## **config account**

Purpose	Used to configure user accounts
---------	---------------------------------

## **config account**

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

### Example Usage:

To configure the user password of “dlink” account:

```
DGS-3224TGR:4#config account dlink
Command: config account dlink

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

DGS-3224TGR:4#
```

## **show account**

## **show account**

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

Example Usage:

To display the accounts that have been created:

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

```
Command: show account
```

```
Current Accounts:
```

Username	Access Level
-----	-----
System	user
dlink	Admin

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

## **delete account**

Purpose	Used to delete an existing user account
Syntax	<b>delete account &lt;username&gt;</b>

## **delete account**

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

### Example Usage:

To delete the user account "System":

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

Success.

DGS-3224TGR:4#
```

## **show session**

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

**show session**

Restrictions      None.

Example Usage:

To display the way that the users logged in:

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

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

**show switch**

Purpose            Used to display information about the switch.

Syntax            **show switch**

Description       This command displays information about the switch.

Parameters       None.

Restrictions      None.

Example Usage:

To display the switch information:

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

Device Type       : DGS-3224TGR Gigabit-Ethernet Switch
MAC Address       : 00-01-02-03-04-00
IP Address        : 10.90.90.90 (Manual)
VLAN Name         : default
Subnet Mask       : 255.0.0.0
Default Gateway   : 0.0.0.0
Boot PROM Version : Build 0.01.004
Firmware Version  : Build 0.02.021
Hardware Version  : 1A1
System Name       :
System Location   :
System Contact    :
Spanning Tree     : Disabled
GVRP              : Disabled
IGMP Snooping     : Disabled
TELNET            : Enabled(TCP 23)
SSH               : Enabled(TCP 22)
WEB               : Enabled(TCP 80)
RMON              : Disabled
RPS State         : Disabled

DGS-3224TGR:4#
```

### **show serial\_port**

Purpose Used to display the current serial port settings

**show serial\_port**

settings.

Syntax	<b>show serial_port</b>
Description	This command displays the current serial port settings.
Parameters	None.
Restrictions	None

## Example Usage:

To display the serial port setting:

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

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

DGS-3224TGR:4#
```

**config serial\_port**

Purpose	Used to configure the serial port.
Syntax	<b>config serial_port</b> <b>{baud_rate[9600   19200   38400   115200]   au</b> <b>to_logout</b>

**config serial\_port****[never | 2\_minutes | 5\_minutes | 10\_minutes | 15\_minutes]**

Description	This command is used to configure the serial port's baud rate and auto logout settings.
Parameters	<p>[9600   19200   38400   115200] – The serial bit rate that will be used to communicate with the management host.</p> <p>never – No time limit on the length of time the console can be open with no user input.</p> <p>2_minutes – The console will log out the current user if there is no user input for 2 minutes.</p> <p>5_minutes – The console will log out the current user if there is no user input for 5 minutes.</p> <p>10_minutes – The console will log out the current user if there is no user input for 10 minutes.</p> <p>15_minutes – The console will log out the current user if there is no user input for 15 minutes.</p>
Restrictions	Only administrator-level users can issue this command.

## Example Usage:

To configure baud rate:



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

Success.

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

## **enable jumbo\_frame**

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

### Example Usage:

To enable jumbo frame support on the switch:

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

Success.

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

## **disable jumbo\_frame**

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

Example Usage:

To disable jumbo frame support on the switch:

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

```
Success.
```

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

## **show jumbo\_frame**

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

## **show jumbo\_frame**

bytes is enabled.

Parameters        None.

Restrictions      Only administrator-level users can issue this command.

Example Usage:

To display jumbo frame support on the switch:

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

```
On.
```

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

## **enable clipaging**

Purpose            Used to pause the scrolling of the console screen when the show command displays more than one page.

Syntax            **enable clipaging**

Description      This command is used when issuing the show command will cause the console screen to rapidly scroll through several pages. This command will cause the console to pause at the end of each page. The default setting is enabled.

## **enable clipaging**

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

### Example Usage:

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

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

```
Success.
```

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

## **disable clipaging**

Purpose	Used to disable the pausing of the console screen scrolling at the end of each page when the show command would display more than one screen of information.
Syntax	<b>disable clipaging</b>
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.

**disable clipaging**

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

```
Success.
```

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

**enable telnet**

Purpose	Used to enable communication with and management of the switch using the Telnet protocol.
Syntax	<b>enable telnet &lt;tcp_port_number&gt;</b>
Description	This command is used to enable the Telnet protocol on the switch. The user can specify the TCP or UDP port number the switch will use to listen for Telnet requests.
Parameters	<tcp_port_number> - the TCP port number. TCP ports are numbered between

## **enable telnet**

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

```
Success.
```

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

## **disable telnet**

**Purpose** Used to disable the Telnet protocol on the switch.

**Syntax** **disable telnet**

**Description** This command is used to disable the Telnet protocol on the switch.

**Parameters** None.

**Restrictions** Only administrator-level users can issue this command.

Example Usage:

To disable the Telnet protocol on the switch:

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

```
Success.
```

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

## **enable web**

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

Example Usage:

To enable HTTP and configure port number:

**DGS-3224TGR:4#enable web 80**

**Command: enable web 80**

**Success.**

**DGS-3224TGR:4#**

## **disable web**

**Purpose** Used to disable the HTTP-based management software on the switch.

**Syntax** **disable web**

**Description** This command disables the Web-based management software on the switch.

**Parameters** None.

**Restrictions** Only administrator-level users can issue this command.

Example Usage:

To disable HTTP:

**DGS-3224TGR:4#disable web**

**Command: disable web**

**Success.**



**DGS-3224TGR:4#**

## **save**

Purpose	Used to save changes in the switch's configuration to non-volatile RAM.
Syntax	<b>save</b>
Description	This command is used to enter the current switch configuration into non-volatile RAM. The saved switch configuration will be loaded into the switch's memory each time the switch is restarted.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

### Example Usage:

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

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

## reboot

Purpose	Used to restart the switch.
Syntax	<b>reboot</b>
Description	This command is used to restart the switch.
Parameters	None.
Restrictions	None.

Example Usage:

To restart the switch:

```
DGS-3224TGR:4#reboot
Command: reboot
Are you sure want to proceed with the
system reboot? (y|n)
Please wait, the switch is rebooting...
```

## reset

Purpose	Used to reset the switch to the factory default settings.
Syntax	<b>reset {config system}</b>
Description	This command is used to restore the switch's configuration to the default

## **reset**

settings assigned from the factory.

### Parameters

**config** – If **config** is specified, all of the factory default settings are restored on the switch except for the IP address, user accounts, and the switch history log.

**system** – If **system** is specified all of the factory default settings are restored on the switch.

If no parameter is specified, the switch's current IP address, user accounts, and switch history log are retained. All other parameters are restored to their factory default settings.

### Restrictions

Only administrator-level users can issue this command.

### Example Usage:

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

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

```
Success.
```

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

## login

Purpose	Used to log in a user to the switch's console.
Syntax	<b>login</b>
Description	This command is used to initiate the login procedure. The user will be prompted for his Username and Password.
Parameters	None.
Restrictions	None.

Example Usage:

To initiate the login procedure:

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

## logout

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

**logout**

Parameters	None.
Restrictions	None.

Example Usage:

To terminate the current user's console session:

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

**config realtime date**

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

Example Usage:

---

To configure the date:

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

Success.

DGS-3224TGR:4#
```

## show realtime

Purpose	Used to display the date and time on the switch.
Syntax	<b>show realtime</b>
Description	This command is used to display the date and time on the switch.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To display the date:

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

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

DGS-3224TGR:4#

**5**

---

# ***SWITCH PORT COMMANDS***

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

<b>Command</b>	<b>Parameters</b>
<b>config ports</b>	<portlist all> speed [auto 10_half 10_full 100_half 100_full   1000_full] flow_control [enabled disabled] learning [enabled disabled] state [enabled disabled]
<b>show ports</b>	<portlist>

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



**config ports**

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

## **config ports**

slower speeds.

[half|full] – Configures the specified range of ports as either full- or half-duplex.

flow\_control [enable|disable] – Enables or disables flow control for the specified range of ports.

learning [enable|disable] – Enables or disables the MAC address learning on the specified range of ports.

state [enable|disable] – Enables or disables the specified range of ports.

**Restrictions** Only administrator-level users can issue this command.

### Example Usage:

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

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

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

```
Success.
```

## **show ports**

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

### Example Usage:

To display the configuration of the ports 1-7:

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

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

# 6

## ***NETWORK MANAGEMENT COMMANDS***

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

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

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

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

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

### **create snmp community**

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

## **create snmp community**

the switch's SNMP agent.

<view\_name> – An alphanumeric string of up to 32 characters that identifies the SNMP view that will be created.

read\_only – Allows the user using the above community string to have read only access to the switch's SNMP agent. The default read only community string is public.

read\_write – Allows the user using the above community string to have read and write access to the switch's SNMP agent. The default read write community string is private.

Restrictions      Only administrator-level users can issue this command. A maximum of four community strings can be specified.

### Example Usage:

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

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



## **delete snmp community**

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

### Example Usage:

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

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

```
Success.
```

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

## **delete trusted\_host**

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

### Example Usage:

To delete a trusted host with an IP address 10.48.74.121:

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

Success.

DGS-3224TGR:4#
```

## **config snmp system\_name**

**config snmp system\_name**

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

## Example Usage:

To configure the switch name for “DGS3224TGR”:

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

Success.

DGS-3224TGR:4#
```

**config snmp system\_location**

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

**config snmp system\_location****<sw\_location>**

Description	This command is used to enter a description of the location of the switch. A maximum of 128 characters can be used.
Parameters	<b>&lt;sw_location&gt;</b> – A description of the location of the switch. A maximum of 128 characters can be used.
Restrictions	Only administrator-level users can issue this command.

## Example Usage:

To configure the switch location for “Timbuktu”:

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

Success.

DGS-3224TGR:4#
```

**config snmp system\_contact :**

Purpose	Used to enter the name of a contact person who is responsible for the switch.
Syntax	<b>config snmp system_contact &lt;sw_contact&gt;</b>

**config snmp system\_contact :**

Description	This command is used to enter the name and/or other information to identify a contact person who is responsible for the switch. A maximum of 128 character can be used.
Parameters	<sw_contact> - A maximum of 128 characters used to identify a contact person who is responsible for the switch.
Restrictions	Only administrator-level users can issue this command.

## Example Usage:

To configure the switch contact to “dlink”:

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

Success.

DGS-3224TGR:4#
```

**enable rmon**

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

### **enable rmon**

enable and disable remote monitoring (RMON) on the switch.

Parameters None.

Restrictions Only administrator-level users can issue this command.

Example Usage:

To enable RMON:

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

```
Command: enable rmon
```

```
Success.
```

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

### **disable rmon**

Purpose Used to disable RMON on the switch.

Syntax **disable rmon**

Description This command is used, in conjunction with the enable rmon command above, to enable and disable remote monitoring (RMON) on the switch.

Parameters None.

## **disable rmon**

Restrictions      Only administrator-level users can issue this command.

Example Usage:

To disable RMON:

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

```
Command: disable rmon
```

```
Success.
```

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

## **show trusted\_host**

Purpose              Used to display a list of trusted hosts entered on the switch using the create trusted\_host command above.

Syntax             **show trusted\_host**

Description        This command is used to display a list of trusted hosts entered on the switch using the create trusted\_host command above.

Parameters         None.

## **show trusted\_host**

Restrictions      None.

Example Usage:

To display the list of trust hosts:

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

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

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

## **enable snmp traps**

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

Example Usage:



To turn on SNMP trap support:

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

```
Command: enable snmp traps
```

```
Success.
```

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

## **disable snmp traps**

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

### Example Usage:

To prevent SNMP traps from being sent from the switch:

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

Success.

DGS-3224TGR:4#
```

## **enable snmp authenticate traps**

Purpose	Used to enable SNMP authentication trap support.
Syntax	<b>enable snmp authenticate traps</b>

### **enable snmp authenticate traps**

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

#### Example Usage:

To turn on SNMP authentication trap support:

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

Success.

DGS-3224TGR:4#
```

### **disable snmp authenticate traps**

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

**disable snmp authenticate traps**

this command.

Example Usage:

To turn off SNMP authentication trap support:

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

```
Success.
```

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

**ping**

Purpose	Used to test the connectivity between network devices.
Syntax	<b>ping &lt;ipaddr&gt; {times &lt;value&gt;} {timeout &lt;sec&gt;}</b>
Description	This command sends Internet Control Message Protocol (ICMP) echo messages to a remote IP address. The remote IP address will then “echo” or return the message. This is used to confirm connectivity between the switch and the remote device.
Parameters	<ipaddr> – The IP address of the remote device.  times <value> – The number of individual

## ping

ICMP echo messages to be sent. A value of 0 will send an infinite ICMP echo messages. The maximum value is 255. The default is 0.

timeout <sec> – defines the time-out period while waiting for a response from the remote device. A value of 1 to 99 seconds can be specified. The default is 1 second.

Restrictions      Only administrator-level users can issue this command.

### Example Usage:

To send ICMP echo message to “10.48.74.121” for 4 times:

```
DGS-3224TGR:4#ping 10.48.74.121 times 4
Command: ping 10.48.74.121
Reply from 10.48.74.121, time<10ms
Reply from 10.48.74.121, time<10ms
Reply from 10.48.74.121, time<10ms
Reply from 10.48.74.121, time<10ms
Ping Statistics for 10.48.74.121
Packets: Sent =4, Received =4, Lost =0

DGS-3224TGR:4#
```

**7**

---

# ***DOWNLOAD/UPLOAD COMMANDS***

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

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

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

## download

Purpose	Used to download and install new firmware or a switch configuration file from a TFTP server.
Syntax	<b>download [ firmware &lt;ipaddr&gt; &lt;path_filename&gt;   configuration &lt;ipaddr&gt; &lt;path_filename&gt; {increment}]</b>
Description	This command is used to download a new firmware or a switch configuration file from a TFTP server.
Parameters	<p>firmware – Download and install new firmware on the switch from a TFTP server.</p> <p>configuration – Download a switch configuration file from a TFTP server.</p> <p>&lt;ipaddr&gt; – The IP address of the TFTP server.</p> <p>&lt;path_filename&gt; – The DOS path and filename of the firmware or switch configuration file on the TFTP server. For example, C:\3224tgr.had.</p> <p>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.</p>
Restrictions	The TFTP server must be on the same IP subnet as the switch. Only administrator-

## download

level users can issue this command.

Example Usage:

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

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

## upload

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



## upload

<ipaddr> – The IP address of the TFTP server. The TFTP server must be on the same IP subnet as the switch.

<path\_filename> – Specifies the location of the switch configuration file on the TFTP server. This file will be replaced by the uploaded file from the switch.

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

Example Usage:

To upload a configuration file:

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

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

## 8

---

## ***NETWORK MONITORING COMMANDS***

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

<b>Command</b>	<b>Parameters</b>
show packet ports	<portlist>
show error ports	<portlist>
show utilization	
clear counters	ports <portlist>
clear log	
show log	index <value>
Enable syslog	
Disable syslog	
Show syslog	
Config syslog	{host(1) [all <index 1-4>]}(1) { severity(2) [informational(21) local1(22) local2(23) local3(24) local4(25) local5(26) local6(27) local7(28)]  udp port(3) <int>   ipaddress(4) <ipaddr>

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

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

### show packet ports

Purpose	Used to display statistics about the packets sent and received by the switch.
Syntax	<b>show packet ports &lt;portlist&gt;</b>
Description	This command is used to display statistics about packets sent and received by ports specified in the port list.
Parameters	<portlist> – specifies a range of ports to be configured. The port list is specified by listing the beginning port number and the highest port number of the range. The beginning and end of the port list range are separated by a dash. For example, 3 would specify port 3. 4 specifies port 4. 3-4 specifies all of the ports between port 3 and port 4 – in numerical order.
Restrictions	None.

Example Usage:

To display the packets analysis for port 7:

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

Port number : 7					
Frame Size	Frame Counts	Frames sec	Frame Type	Total	
Total sec					
64	3275	10	RX Bytes	408973	1657
65-127	755	10	RX Frames	4395	19
128-255	316	1			
256-511	145	0	TX Bytes	7918	178
512-1023	15	0	TX Frames	111	2
1024-1518	0	0			
Unicast RX	152	1			
Multicast RX	557	2			
Broadcast RX	3686	16			
<b>Broadcast RX</b>	<b>4495</b>	<b>42</b>			

### 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 configured. The port list is specified by listing the beginning port number and the

## show error ports

highest port number of the range. The beginning and end of the port list range are separated by a dash. For example, 3 would specify port 3. 4 specifies port 4. 3-4 specifies all of the ports between port 3 and port 4 – in numerical order.

Restrictions      None.

Example Usage:

To display the errors of the port 3:

**DGS-3224TGR:4# show errors port 3**

	RX Frames -----		TX Frames -----
<b>CRC Error</b>	<b>0</b>	<b>Excessive Deferral</b>	<b>0</b>
<b>Undersize</b>	<b>0</b>	<b>CRC Error</b>	<b>0</b>
<b>Oversize</b>	<b>0</b>	<b>Late Collision</b>	<b>0</b>
<b>Fragment</b>	<b>0</b>	<b>Excessive Collision</b>	<b>0</b>
<b>Jabber</b>	<b>0</b>	<b>Single Collission</b>	<b>0</b>
<b>Drop Pkts</b>	<b>0</b>	<b>Collision</b>	<b>0</b>

## show utilization

Purpose              Used to display real-time port utilization statistics.

Syntax             **show utilization**

## show utilization

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

Example Usage:

To display the port utilization statistics:

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

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

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

## clear counters

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

### Example Usage:

To clear the counters:

<b>DGS-3224TGR:4#clear counters ports 7-9</b> <b>Command: clear counters ports 7-9</b>
---

**Success.**

**DGS-3224TGR:4#**

## **clear log**

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

Example Usage:

To clear the log information:

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

**Success.**

**DGS-3224TGR:4#**

## **show log**

Purpose	Used to display the switch history log.
---------	---



**show log**

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

## Example Usage:

To display the switch history log:

```
DGS-3224TGR:4# show log
Index   Time                Log Text
-----
8       2003/09/18 09:03:45 Successful login through Console (Username:
Anonymous)
7       2003/09/18 09:03:30 Logout through Console (Username: Anonymous)
6       2003/09/18 09:03:28 Successful login through Console (Username:
Anonymous)
5       2003/09/18 09:03:26 System started up
4       2003/09/18 16:13:39 Port 1 link down
3       2003/09/18 16:13:38 System started up
2       2003/09/18 16:13:36 Spanning Tree Protocol is disabled
1       2003/09/18 16:13:35 Port 9 link up, 100Mbps FULL duplex
DGS-3224TGR:4#
```

**9**

---

# *SPANNING TREE COMMANDS*

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

<b>Command</b>	<b>Parameters</b>
<b>config stp</b>	<b>maxage &lt;value&gt;</b> <b>hellotime &lt;value&gt;</b> <b>forwarddelay &lt;value&gt;</b> <b>priority &lt;value&gt;</b> <b>fbpdu [enable disable]</b>
<b>config stp ports</b>	<b>&lt;portlist&gt;</b> <b>cost &lt;value&gt;</b> <b>priority &lt;value&gt;</b> <b>priority &lt;value&gt;</b> <b>state [enable disable]</b>
<b>enable stp</b>	
<b>disable stp</b>	
<b>show stp</b>	
<b>show stp ports</b>	<b>&lt;portlist&gt;</b>

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

**config stp**

Purpose	Used to setup STP on the switch.
Syntax	<code>config stp {maxage &lt;value&gt;   hellotime &lt;value&gt;   forwarddelay &lt;value&gt;   priority &lt;value&gt;   fbpdu [enabled   disabled]}</code>
Description	This command is used to setup the Spanning Tree Protocol (STP) for the entire switch.
Parameters	<p><code>maxage &lt;value&gt;</code> – The maximum amount of time (in seconds) that the switch will wait to receive a BPDU packet before reconfiguring STP. The default is 20 seconds.</p> <p><code>hellotime &lt;value&gt;</code> – The time interval between transmission of configuration messages by the root device. The default is 2 seconds.</p> <p><code>forwarddelay &lt;value&gt;</code> – The maximum amount of time (in seconds) that the root device will wait before changing states. The default is 15 seconds.</p> <p><code>priority &lt;value&gt;</code> – A numerical value between 0 and 65,535 that is used in determining the root device, root port, and designated port. The device with the highest priority becomes the root device. The lower the numerical value, the higher the priority. The default is 32,768.</p> <p><code>fbpdu [enabled disabled]</code> – Allows the forwarding of STP BPDU packets from</p>

## config stp

other network devices when STP is disabled on the switch. The default is enabled.

**Restrictions** Only administrator-level users can issue this command.

### Example Usage:

To set maxage to 18 and hellotime to 4:

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

```
Success.
```

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

## config stp ports

Purpose	Used to setup STP on the port level.
Syntax	<b>config stp ports &lt;portlist&gt; {cost &lt;value&gt;   priority &lt;value&gt;   state [enable   disable]}</b>
Description	This command is used to create and configure STP for a group of ports.
Parameters	cost <value> – This defines a metric that indicates the relative cost of forwarding packets to the specified port list. The default cost for a 1000 Mbps port is 4, a 100 Mbps port is 19, and for a 10 Mbps

**config stp ports**

port the default cost is 100.

priority <value> – A numeric value between 0 and 255 that is used in determining the root and designated port in an STP port list. The default is 128, with 0 indicating the highest priority.

<portlist> – Specifies a range of ports to be configured. The port list is specified by listing the beginning port number and the highest port number of the range. The beginning and end of the port list range are separated by a dash. For example, 3 would specify port 3. 4 specifies port 4. 3-4 specifies all of the ports between port 3 and port 4 – in numerical order.

state [enable|disable] – Allows STP to be enabled or disabled for the ports specified in the port list. The default is disabled.

Restrictions      Only administrator-level users can issue this command.

**Example Usage:**

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

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

**Success.**

**DGS-3224TGR:4#**

## **enable stp**

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

Example Usage:

To enable STP on the switch:

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

**Success.**

**DGS-3224TGR:4#**

## **disable stp**

## **disable stp**

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

### Example Usage:

To disable STP on the switch:

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

```
Success.
```

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

## **show stp**

Purpose	Used to display the switch's current STP configuration.
Syntax	<b>show stp</b>
Description	This command displays the switch's current STP configuration.

**show stp**

current STP configuration.

Parameters	None
Restrictions	None.

Example Usage:

Status 1: STP enabled

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

STP Status           : Enabled
Max Age              : 18
Hello Time           : 4
Forward Delay        : 15
Priority              : 32768
Forwarding BPDU      : Enabled

Designated Root Bridge : 00-00-00-12-00-00
Root Priority         : 32768
Cost to Root         : 19
Root Port            : 33
Last Topology Change : 13sec
Topology Changes Count : 0
```

Status 2: STP disabled

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

STP Status           : Disabled
```



<b>Max Age</b>	<b>: 18</b>
<b>Hello Time</b>	<b>: 4</b>
<b>Forward Delay</b>	<b>: 15</b>
<b>Priority</b>	<b>: 32768</b>
<b>Forwarding BPDU</b>	<b>: Enabled</b>

**DGS-3224TGR:4#**

## **show stp ports**

Purpose	Used to display the switch's current per-port group STP configuration.
Syntax	<b>show stp ports &lt;portlist&gt;</b>
Description	This command displays the switch's current per-port group STP configuration.
Parameters	<portlist> – Specifies a range of ports to be configured. The port list is specified by listing the beginning port number and the highest port number of the range. The beginning and end of the port list range are separated by a dash. For example, 3 would specify port 3. 4 specifies port 4. 3-4 specifies all of the ports between port 3 and port 4 – in numerical order.
Restrictions	None

### Example Usage:

To display STP state of port 1-9:

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

<b>Port</b>	<b>Connection</b>	<b>State</b>	<b>Cost</b>	<b>Priority</b>	<b>Status</b>	<b>STP Name</b>
1	Link Down	Enabled	19	128	Forwarding	s0
2	Link Down	Enabled	19	128	Forwarding	s0
3	Link Down	Enabled	19	128	Forwarding	s0
4	Link Down	Enabled	19	128	Forwarding	s0
5	Link Down	Enabled	19	128	Forwarding	s0
6	Link Down	Enabled	19	128	Forwarding	s0
7	Link Down	Enabled	19	128	Forwarding	s0
8	Link Down	Enabled	19	128	Forwarding	s0
9	Link Down	Enabled	19	128	Forwarding	s0

**10*****LAYER 2 FORWARDING  
DATABASE COMMANDS***

The layer 2 forwarding database commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

<b>Command</b>	<b>Parameters</b>
<b>create fdb</b>	<vlan_name> <macaddr> port <port>
<b>create multicast_fdb</b>	<vlan_name> <macaddr>
<b>config multicast_fdb</b>	<vlan_name> <macaddr> [add delete] <portlist>
<b>delete fdb</b>	<vlan_name> <macaddr> [add delete] <portlist>
<b>clear fdb</b>	vlan <vlan_name> port <port> all
<b>show multicast_fdb</b>	vlan <vlan_name> mac_address <macaddr>
<b>show fdb</b>	port <port>

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

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

<b>create fdb</b>	
Purpose	Used to create a static entry to the unicast MAC address forwarding table (database)
Syntax	<b>create fdb &lt;vlan_name&gt; &lt;macaddr&gt; [port &lt;port&gt;]</b>
Description	This command will make an entry into the switch's unicast MAC address forwarding database.
Parameters	<vlan_name> – The name of the VLAN on which the MAC address resides.  <macaddr> – The MAC address that will be added to the forwarding table.  <port> – The port number corresponding to the MAC destination address. The switch will always forward traffic to the specified device through this port.

**create fdb**

**Restrictions**      Only administrator-level users can issue this command.

**Example Usage:**

To create an unicast MAC forwarding:

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

Success.
```

**create multicast\_fdb**

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

**create multicast\_fdb**

added to the forwarding table.

**Restrictions** Only administrator-level users can issue this command.

**Example Usage:**

To create multicast MAC forwarding:

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

Success.

DGS-3224TGR:4#
```

**config multicast\_fdb**

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

## **config multicast\_fdb**

added to the forwarding table.

[add|delete] – Add will add the MAC address to the forwarding table, delete will remove the MAC address from the forwarding table.

<portlist> – Specifies a range of ports to be configured. The port list is specified by listing the beginning port number and the highest port number of the range. The beginning and end of the port list range are separated by a dash. For example, 3 would specify port 3. 4 specifies port 4. 3-4 specifies all of the ports between port 3 and port 4 – in numerical order.

Restrictions      Only administrator-level users can issue this command.

Example Usage:

To add multicast MAC forwarding:

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

## **delete fdb**

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

### Example Usage:

To delete a permanent FDB entry:

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

```
Success.
```

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

## **clear fdb**



**clear fdb**

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

## Example Usage:

To clear all FDB dynamic entries:

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

Success.
```

**DGS-3224TGR:4#****show multicast\_fdb**

Purpose	Used to display the contents of the switch's multicast forwarding database.
Syntax	<b>show           multicast_fdb           [vlan &lt;vlan_name&gt;   mac_address &lt;macaddr&gt;</b>
Description	This command is used to display the current contents of the switch's multicast MAC address forwarding database.
Parameters	<vlan_name> – The name of the VLAN on which the MAC address resides.  <macaddr> – The MAC address that will be added to the forwarding table.
Restrictions	None.

## Example Usage:

To display multicast MAC address table:

**DGS-3224TGR:4#show multicast\_fdb**  
**Command: show multicast\_fdb****VLAN Name     : default**  
**MAC Address   : 01-00-5E-00-00-00**  
**Egress Ports  : 1-5, 21, 22**  
**Mode           : Static****Total Entries : 1**

DGS-3224TGR:4#

**show fdb**

Purpose	Used to display the current unicast MAC address forwarding database.
Syntax	<b>show fdb {port &lt;port&gt;   vlan &lt;vlan_name&gt;   mac_address &lt;macaddr&gt;   static   aging_time}</b>
Description	This command will display the current contents of the switch's forwarding database.
Parameters	<p>&lt;port&gt; – The port number corresponding to the MAC destination address. The switch will always forward traffic to the specified device through this port.</p> <p>&lt;vlan_name&gt; – The name of the VLAN on which the MAC address resides.</p> <p>&lt;macaddr&gt; – The MAC address that will be added to the forwarding table.</p> <p>static – Displays the static MAC address entries.</p> <p>aging_time – Displays the aging time for the MAC address forwarding database.</p>
Restrictions	None.

Example Usage:

To display unicast MAC address table:

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

Unicast MAC Address Ageing Time = 300

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

Total Entries = 2

DGS-3224TGR:4#
```

**11**

---

# ***BROADCAST STORM CONTROL COMMANDS***

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

<b>Command</b>	<b>Parameters</b>
<b>config traffic control</b>	<b>&lt;storm_portlist&gt; all broadcast [enable disable] multicast [enable disable] dIf [enable disable]</b>
<b>show traffic control</b>	<b>port_list &lt;storm_portlist&gt;</b>

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

## config traffic control

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

## **config traffic control**

Restrictions      Only administrator-level users can issue this command.

Example Usage:

To configure traffic control and state:

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

Success.

DGS-3224TGR:4#
```

## **show traffic control**

Purpose	Used to display current traffic control settings.
Syntax	<b>show traffic control &lt;storm_portlist&gt;</b>
Description	This command displays the current storm traffic control configuration on the switch.
Parameters	group_list <storm_portlist> - Used to specify a broadcast storm control group with the syntax: port_number.
Restrictions	None.

Example Usage:

To display traffic control setting:

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

Traffic Control
```

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



**12****ARP COMMANDS**

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

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

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

**config arp\_aging**

**Purpose** Used to configure the age-out timer for ARP table entries on the switch.

**Syntax** **config arp\_aging time <min 0-65535>**

**config arp\_aging**

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

## Example Usage:

To configure ARP aging time:

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

```
Success.
```

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

**show arpentry**

Purpose	Used to display the ARP table.
Syntax	<b>show arpentry {ipif &lt;ipif_name&gt;   ipaddress &lt;network_address&gt;   static}</b>
Description	This command is used to display the current contents of the switch's ARP table.

**show arpentry**

current contents of the switch's ARP table.

**Parameters** <ipif\_name> – The name of the IP interface the end node or station for which the ARP table entry was made, resides on.

<network\_address> – The network address corresponding to the IP interface name above.

static – Displays the static entries to the ARP table.

**Restrictions** None.

Example Usage:

To display the ARP table:

**DGS-3224TGR:4#show arpentry**

**Command: show arpentry**

**ARP Aging Time : 20**

<b>Interface</b>	<b>IP Address</b>	<b>MAC Address</b>	<b>Type</b>
System	10.0.0.0	FF-FF-FF-FF-FF-FF	Local Broadcast
System	10.1.1.169	00-50-BA-70-E4-4E	Dynamic
System	10.1.1.254	00-01-30-FA-5F-00	Dynamic
System	10.9.68.1	00-A0-C9-A4-22-5B	Dynamic
System	10.9.68.4	00-80-C8-2E-C7-45	Dynamic
System	10.10.27.51	00-80-C8-48-DF-AB	Dynamic
System	10.11.22.145	00-80-C8-93-05-6B	Dynamic
System	10.11.94.10	00-10-83-F9-37-6E	Dynamic

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

Total Entries = 20

DGS-3224TGR:4#

## clear arptable

Purpose	Used to remove all dynamic ARP table entries.
Syntax	<b>clear arptable</b>
Description	This command is used to remove dynamic ARP table entries from the switch's ARP table. Static ARP table entries are not effected.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To remove dynamic entries in the ARP table:

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

```
Command: clear arptable
```

```
Success.
```

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

**13****QOS COMMANDS**

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

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

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

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

### config scheduling

Purpose	Used to configure the traffic scheduling mechanism for each COS queue.
Syntax	<b>config scheduling &lt;class_id 0-7&gt; weight &lt;value 1-15&gt;</b>
Description	<p>The switch contains eight hardware priority queues. Incoming packets must be mapped to one of these eight queues. This command is used to specify the rotation by which these eight hardware priority queues are emptied.</p> <p>The switch's default (if the config scheduling command is not used) is to empty the eight hardware priority queues in order – from the highest priority queue (hardware queue 8) to the lowest priority queue (hardware queue 0). Each hardware queue will transmit all of the packets in its buffer before allowing the next lower priority queue to transmit its packets. When the lowest hardware priority</p>

## **config scheduling**

queue has finished transmitting all of its packets, the highest hardware priority queue can again transmit any packets it may have received.

**Parameters**      <class\_id> – This specifies which of the eight hardware priority queues the config scheduling command will apply to. The eight hardware priority queues are identified by number – from 0 to 7 – with the 0 queue being the lowest priority.

**Restrictions**      Only administrator-level users can issue this command.

Example Usage:

To configure scheduling:

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

```
Success.
```

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

## **show scheduling**

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



**show scheduling**

Syntax	<b>show scheduling</b>
Description	This command will display the current traffic scheduling mechanisms in use on the switch.
Parameters	None.
Restrictions	None.

Example Usage:

To show scheduling:

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

```
Command: show scheduling
```

**QOS Output Scheduling**

<b>Class ID</b>	<b>MAX. Weight</b>
<b>Class-0</b>	<b>1</b>
<b>Class-1</b>	<b>2</b>
<b>Class-2</b>	<b>3</b>
<b>Class-3</b>	<b>4</b>
<b>Class-4</b>	<b>5</b>
<b>Class-5</b>	<b>6</b>
<b>Class-6</b>	<b>7</b>
<b>Class-7</b>	<b>8</b>

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

## **config scheduling\_mechanism**

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

### Example Usage:

To configure the traffic scheduling mechanism for each COS queue:

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

```
Success.
```

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

## **show scheduling\_mechanism**

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

### Example Usage:

To show the scheduling mechanism:

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

Scheduling Mechanism : weight_fair

DGS-3224TGR:4#
```

## **config 802.1p user\_priority**

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

**config 802.1p user\_priority**

**Syntax**                    **config 802.1p user\_priority <priority 0-7>**  
**<class\_id 0-7>**

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

The suggested mapping is included in the following table:

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

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

**config 802.1p user\_priority**

You can change this mapping by specifying the 802.1p user priority you want to go to the <class\_id> (the number of the hardware queue).

<priority> – The 802.1p user priority you want to associate with the <class\_id> (the number of the hardware queue) with.

<class\_id> – The number of the switch's hardware priority queue. The switch has eight hardware priority queues available. They are numbered between 0 (the lowest priority) and 7 (the highest priority).

**Restrictions**      Only administrator-level users can issue this command.

**Example Usage:**

To configure 802.1p user priority:

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

```
Success.
```

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

**show 802.1p user\_priority**

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

## **show 802.1p user\_priority**

priority to hardware priority queue mapping in use by the switch.

Syntax **show 802.1p user\_priority**

Description This command will display the current 802.1p user priority to hardware priority queue mapping in use by the switch.

Parameters None.

Restrictions None.

Example Usage:

To show 802.1p user priority:

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

### **QOS Class of Traffic**

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

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

**config 802.1p default\_priority**

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

## **config 802.1p default\_priority**

Restrictions Only administrator-level users can issue this command.

Example Usage:

To configure 802.1p default priority:

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

```
Success.
```

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

## **show 802.1p default\_priority**

Purpose Used to display the current default priority settings on the switch.

Syntax **show 802.1p default\_priority**

Description This command is used to display the current default priority settings on the switch.

Parameters None.

Restrictions None.

Example Usage:

To show 802.1p default priority:



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

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

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

**enable hol\_prevention**

## **enable hol\_prevention**

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

Example Usage:

To enable HOL prevention:

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

```
Success.
```

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

## **disable hol\_prevention**

Purpose	Used to disable HOL prevention.
Syntax	<b>disable hol_prevention</b>
Description	The disable hol_prevention command disables Head of Line prevention.
Parameters	None.

## **disable hol\_prevention**

Restrictions      You must have administrator privileges.

Example Usage:

To disable HOL prevention:

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

Success.

DGS-3224TGR:4#
```

## **show hol\_prevention**

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

Example Usage:

To show HOL prevention:

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

**Command: show hol\_prevention**

**Success.**

**DGS-3224TGR:4#**

**14*****PORT MIRRORING  
COMMANDS***

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

<b>Command</b>	<b>Parameters</b>
<b>config mirror port</b>	<b>&lt;port&gt; [add delete] source ports &lt;portlist&gt; [rx tx both]</b>
<b>enable mirror</b>	
<b>disable mirror</b>	
<b>show mirror</b>	

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

**config mirror port**

Purpose	Used to configure a mirror port – source port pair on the switch.
Syntax	<b>config mirror port &lt;port&gt; add source ports &lt;portlist&gt; [rx   tx   both]</b>

## **config mirror port**

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 or both is mirrored to the Target port.
Parameters	<p>&lt;port&gt; – This specifies the Target port (the port where mirrored packets will be sent).</p> <p>&lt;portlist&gt; – This specifies a range of ports that will be mirrored. That is, a range of ports for which all traffic will be copied and sent to the Target port. The port list is specified by listing the beginning port number on that switch and the highest port number of the range. The beginning and end of the port list range are separated by a dash. For example, 3 would specify port 3. 4 specifies port 4. 3-4 specifies all of the ports between port 3 and port 4 – in numerical order.</p> <p>rx – Allows the mirroring of only packets received (flowing into) the port or ports in the port list.</p> <p>tx – Allows the mirroring of only packets sent (flowing out of) the port or ports in the port list.</p> <p>both – Mirrors all the packets received or sent by the port or ports in the port list.</p>

**config mirror port**

Restrictions      Only administrator-level users can issue this command.

Example Usage:

To add the mirroring ports:

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

**Success.**

**DGS-3224TGR:4#**

**config mirror delete**

Purpose              Used to delete a port mirroring configuration |

Syntax             **config mirror <port> delete source <portlist> [rx | tx | both]**

Description        This command is used to delete a previously entered port mirroring configuration.

Parameters        <port> – This specifies the Target port (the port where mirrored packets will be sent).

<portlist> – This specifies a range of ports that will be mirrored. That is, a range of ports for which all traffic will be copied and

**config mirror delete**

sent to the Target port.

rx – Allows the mirroring of only packets received (flowing into) the port or ports in the port list.

tx – Allows the mirroring of only packets sent (flowing out of) the port or ports in the port list.

both – Mirrors all the packets received or sent by the port or ports in the port list.

Restrictions      Only administrator-level users can issue this command.

## Example Usage:

To delete the mirroring ports:

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

```
Success.
```

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

**enable mirror**

Purpose              Used to enable a previously entered port mirroring configuration.

Syntax             **enable mirror**



**enable mirror**

Description	This command, combined with the disable mirror command below, allows you to enter a port mirroring configuration into the switch, and then turn the port mirroring on and off without having to modify the port mirroring configuration.
Parameters	None.
Restrictions	None.

## Example Usage:

To enable mirroring configurations:

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

```
Command: enable mirror
```

```
Success.
```

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

**disable mirror**

Purpose	Used to disable a previously entered port mirroring configuration.
Syntax	<b>disable mirror</b>
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

## **disable mirror**

and off without having to modify the port mirroring configuration.

Parameters        None.

Restrictions      Only administrator-level users can issue this command.

Example Usage:

To disable mirroring configurations:

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

```
Command: disable mirror
```

```
Success.
```

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

## **show mirror**

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

Syntax           **show mirror**

Description      This command displays the current port mirroring configuration on the switch.

Parameters       None

Restrictions      None.

Example Usage:

To display mirroring configuration:

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

```
Current Settings
```

```
Target Port: 9
```

```
Mirrored Port:
```

```
  RX:
```

```
  TX: 1-5
```

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

**15*****VLAN COMMANDS***

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

<b>Command</b>	<b>Parameters</b>
create vlan	<vlan_name> tag <vlanid> advertisement
delete vlan	<vlan_name>
config vlan	<vlan_name> add [tagged untagged forbidden] <portlist>
config vlan	<vlan_name> delete <portlist>
config vlan	<vlan_name> advertisement [enable disable]
config gvrp	<portlist> all state [enable disable] ingress_checking [enable disable]
enable gvrp	
disable gvrp	

Command	Parameters
show vlan	<vlan_name>
show gvrp	<portlist>

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

### create vlan

Purpose	Used to create a VLAN on the switch.
Syntax	<b>create vlan &lt;vlan_name&gt; {tag &lt;vlanid&gt;   advertisement}</b>
Description	This command allows you to create a VLAN on the switch.
Parameters	<p>&lt;vlan_name&gt; – The name of the VLAN to be created.</p> <p>&lt;vlanid&gt; – The VLAN ID of the VLAN to be created.</p> <p>advertisement – Specifies the VLAN participates normally in GARP/GVRP protocol exchanges. If this parameter is not set, the switch cannot send any GARP/GVRP messages about the VLAN.</p>
Restrictions	Each VLAN name can be up to 32 characters. If the VLAN is not given a tag, it will automatically allocate a VID value. Only administrator-level users can issue this command.

Example Usage:

To create a VLAN v1, tag 2:

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

```
Command: create vlan v1 tag 2
```

```
Success.
```

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

## **delete vlan**

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

Example Usage:

To remove a vlan v1:

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

```
Command: delete vlan v1
```

**Success.**

**DGS-3224TGR:4#**

## **config vlan add ports**

Purpose	Used to add additional ports to a previously configured VLAN.
Syntax	<b>config vlan &lt;vlan_name&gt; add [tagged   untagged   forbidden] &lt;portlist&gt;</b>
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.
Parameters	<p>&lt;vlan_name&gt; – The name of the VLAN you want to add ports to.</p> <p>tagged – Specifies the additional ports as tagged.</p> <p>untagged – Specifies the additional ports as untagged.</p> <p>forbidden – Specifies the additional ports as forbidden.</p> <p>&lt;portlist&gt; – A range of ports to add to the VLAN. The port list is specified by listing the beginning port number and the highest port number of the range. The beginning and end of the port list range are separated by a dash. For example, 3 would specify port 3. 4 specifies port 4. 3-4 specifies all of the ports between port 3 and port 4 – in</p>

**config vlan add ports**

numerical order.

Restrictions Only administrator-level users can issue this command.

## Example Usage:

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

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

```
Success.
```

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

**config vlan delete ports**

Purpose Used to delete one or more ports from a previously configured VLAN |

Syntax **config vlan <vlan\_name> delete <portlist>**

Description This command allows you to delete ports from a previously configured VLAN's port list.

Parameters <vlan\_name> – The name of the VLAN you want to delete ports from.

<portlist> – A range of ports you want to delete from the above specified VLAN. The



**config vlan delete ports**

port list is specified by listing the beginning port number and the highest port number of the range. The beginning and end of the port list range are separated by a dash. For example, 3 would specify port 3. 4 specifies port 4. 3-4 specifies all of the ports between port 3 and port 4 – in numerical order.

**Restrictions** Only administrator-level users can issue this command.

**Example Usage:**

To delete 4 through 8 to the VLAN v1:

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

```
Success.
```

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

**config vlan advertisement**

**Purpose** Used to enable or disable the VLAN advertisement.

**Syntax** **config vlan <vlan\_name> advertisement [enable | disable]**

**Description** This command is used to enable or disable sending GVRP messages on the specified

## **config vlan advertisement**

VLAN.

Parameters	<p>&lt;vlan_name&gt; – The name of the VLAN on which you want to enable or disable sending GVRP messages.</p> <p>enable – Enables sending GVRP messages on the specified VLAN.</p> <p>disable – Disables sending GVRP messages on the specified VLAN.</p>
Restrictions	<p>Only administrator-level users can issue this command.</p>

### Example Usage:

To enable the VLAN default advertisement:

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

Success.

DGS-3224TGR:4#
```

## **config gvrp**

Purpose	Used to configure GVRP on the switch.
---------	---------------------------------------

**config gvrp**

Syntax	<b>config gvrp [&lt;portlist&gt;   all] {state [enable   disable]   ingress_checking [enable   disable]}</b>
Description	This command is used to configure the Group VLAN Registration Protocol on the switch. You can configure ingress checking and the GVRP status for each port.
Parameters	<p>&lt;portlist&gt; – A range of ports for which you want ingress checking. The port list is specified by listing the beginning port number and the highest port number of the range. The beginning and end of the port list range are separated by a dash. For example, 3 would specify port 3. 4 specifies port 4. 3-4 specifies all of the ports between port 3 and port 4 – in numerical order.</p> <p>all – Specifies all of the ports on the switch.</p> <p>state [enable   disable] – Enables or disables GVRP for the ports specified in the port list.</p> <p>ingress_checking [enable   disable] – Enables or disables ingress checking for the specified port list.</p>
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To sets the ingress checking status and the GVRP status:

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

Success.
```

## **enable gvrp**

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

Example Usage:

To enable the generic VLAN Registration Protocol (GVRP):

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

**Success.**

**DGS-3224TGR:4#**

## **disable gvrp**

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

### Example Usage:

To disable the Generic VLAN Registration Protocol (GVRP):

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

**Success.**

**DGS-3224TGR:4#**

**show vlan**

Purpose	Used to display the current VLAN configuration on the switch
Syntax	<b>show vlan {&lt;vlan_name&gt;}</b>
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> – The VLAN name of the VLAN for which you want to display a summary of settings.
Restrictions	None.

Example Usage:

To display VLAN settings:

**DGS-3224TGR:4#show vlan**

**Command: show vlan**

```

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

Total Entries : 1

```

DGS-3224TGR:4#

### **show gvrp**

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

Example Usage:

To display 802.1Q port setting:

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

```
Global GVRP : Disabled
```

Port	PVID	GVRP	Ingress Checking
1	1	Enable	Enable
2	1	Enable	Enable
3	1	Enable	Enable
4	1	Enable	Enable
5	1	Enable	Enable
6	1	Disable	Disable
7	1	Disable	Disable
8	1	Disable	Disable
9	1	Disable	Disable
10	1	Disable	Disable
11	1	Disable	Disable
12	1	Disable	Disable
13	1	Disable	Disable
14	1	Disable	Disable
15	1	Disable	Disable
16	1	Disable	Disable
17	1	Disable	Disable
18	1	Disable	Disable
19	1	Disable	Disable
20	1	Disable	Disable
21	1	Disable	Disable
22	1	Disable	Disable
23	1	Disable	Disable
24	1	Disable	Disable

Total Entries : 24

DGS-3224TGR:4#



# 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.

<b>Command</b>	<b>Parameters</b>
<code>create link_aggregation</code>	<code>{group_id &lt;value1-32&gt; algorithm}</code>
<code>delete link_aggregation</code>	<code>group_id &lt;value&gt;</code>
<code>config link_aggregation</code>	<code>group_id &lt;value&gt; master_port &lt;port&gt; ports &lt;portlist&gt; state [enable disable]</code>
<code>config link_aggregation algorithm</code>	<code>mac_source mac_destination mac_source_dest ip_source ip_destination ip_source_dest</code>
<code>show link_aggregation</code>	<code>group_id &lt;value&gt; algorithm</code>

<b>Command</b>	<b>Parameters</b>
<b>create link_aggregation group_id</b>	<value 1-32>
<b>delete link_aggregation group_id</b>	<value 1-32>
<b>config link_aggregation group_id</b>	<value 1-32> {master_prot <port>   ports <portlist>   state [enabled disabled]}(1)

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

### **create link\_aggregation group\_id**

Purpose	Used to create a link aggregation group on the switch.
Syntax	<b>create link_aggregation group_id &lt;value&gt;</b>
Description	This command will create a link aggregation group.
Parameters	<value> – Specifies the group id. The switch allows up to 32 link aggregation groups to be configured. The group number identifies each of the groups.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To create link aggregation group:

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

```
Success.
```

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

## **delete link\_aggregation group\_id**

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

Example Usage:

To delete link aggregation group:

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

**Success.**

**DGS-3224TGR:4#**

## **config link\_aggregation**

Purpose	Used to configure a previously created link aggregation group.
Syntax	<b>config link_aggregation group_id &lt;value&gt; {master_port &lt;port&gt;   ports &lt;portlist&gt;   state [enable   disable]}</b>
Description	This command allows you to configure a link aggregation group that was created with the create link_aggregation command above.
Parameters	<p>&lt;value&gt; – Specifies the group id. The switch allows up to 32 link aggregation groups to be configured. The group number identifies each of the groups.</p> <p>&lt;port&gt; – Master port ID. Specifies which port (by port number) of the link aggregation group will be the master port. All of the ports in a link aggregation group will share the port configuration with the master port.</p> <p>&lt;portlist&gt; – Specifies a range of ports that will belong to the link aggregation group. The beginning and end of the port list range are separated by a dash. For example, 3 would specify port 3. 4 specifies port 4. 1-4 specifies all of the ports between</p>

## config link\_aggregation

port 1 and 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.

### Example Usage:

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

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

Success.

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

## config link\_aggregation algorithm

Purpose Used to configure the link aggregation algorithm.

Syntax **config link\_aggregation algorithm**  
**[mac\_source | mac\_destination | mac\_source\_d**  
**est |**  
**ip\_source | ip\_destination | ip\_source\_dest]**

## **config link\_aggregation alg rithm**

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

### Example Usage:

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

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

Success.

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

## **show link\_aggregation**

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

Example Usage:

To show link aggregation:

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

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

DGS-3224TGR:4#
```



**17**

---

# ***IP INTERFACE COMMANDS***

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

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

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

## **config ipif System**

Purpose                      Used to configure the System IP interface.

## config ipif System

Syntax	<b>config ipif System</b> [{vlan <vlan_name> ipaddress <network_address> state [enable disable] bootp dhcp}]
Description	This command is used to configure the System IP interface on the switch.
Parameters	<vlan_name> – The name of the VLAN corresponding to the System IP interface.  <network_address> – IP address and netmask of th IP interface to be created. You can specify the address and mask information using the traditional format (for example, 10.1.2.3/255.0.0.0 or in CIDR format, 10.1.2.3/16).  state [enable disable] – Allows you to enable or disable the IP interface.  bootp – Allows the selection of the BOOTP protocol for the assignment of an IP address to the switch's System IP interface.  dhcp – Allows the selection of the DHCP protocol for the assignment of an IP address to the switch's System IP interface.
Restrictions	Only administrator-level users can issue this command.

### Example Usage:

To configure the IP interface System:

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

Success.

DGS-3224TGR:4#
```

## config ipif

Purpose	Used to configure an IP interface on the switch.
Syntax	<b>config ipif &lt;ipif_name&gt; {vlan &lt;vlan_name&gt;   ipaddress &lt;network_address&gt;   state [enabled   disabled]}</b>
Description	This command is used to configure an IP interface on the switch.
Parameters	<p>&lt;ipif_name&gt; – The name of the IP interface to be configured on the switch.</p> <p>&lt;vlan_name&gt; – The name of the VLAN that corresponds to the IP interface above.</p> <p>&lt;network_address&gt; – IP address and netmask of the IP interface to be created. You can specify the address and mask information using the traditional format (for example, 10.1.2.3/255.0.0.0) or in CIDR format, 10.1.2.3/16).</p> <p>state [enabled   disabled] – Allows you to</p>

## **config ipif**

enable or disable the IP interface.

**Restrictions** Only administrator-level users can issue this command.

Example Usage:

To configure the IP interface ip2:

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

```
Success.
```

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

## **show ipif**

**Purpose** Used to display the configuration of an IP interface on the switch.

**Syntax** **show ipif {<ipif\_name>}**

**Description** This command will display the configuration of an IP interface on the switch.

**Parameters** <ipif\_name> – The name of the IP interface you want to disable.

all – Specifies that all IP interfaces configured on the switch will be disabled.

## **show ipif**

Restrictions        None.

Example Usage:

To display IP interface settings:

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

IP Interface Settings

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

Total Entries : 1

DGS-3224TGR:4#
```

**18*****IGMP SNOOPING  
COMMANDS***

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

<b>Command</b>	<b>Parameters</b>
<b>config igmp_snooping</b>	<vlan_name 32> all host_timeout <sec 1-16711450> router_timeout <sec 1-16711450> leave_timer <sec 1-16711450> state [enable disable]
<b>config igmp_snooping querier</b>	<vlan_name 32> all query_interval <sec 1-65535> max_response_time <sec 1-25> robustness_variable <value 1-255> last_member_query_interval <sec 1-65535> state [enable disable]
<b>config router_ports</b>	<vlan_name 32> [add delete] <portlist>
<b>enable igmp snooping</b>	forward_mcrouter_only

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

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

### **config igmp\_snooping**

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

## **config igmp\_snooping**

`host_timeout <sec 1-16711450>` – Specifies the maximum amount of time a host can be a member of a multicast group without the switch receiving a host membership report. The default is 260 seconds.

`router_timeout <sec 1-16711450>` – Specifies the maximum amount of time a route will remain in the switch's can be a member of a multicast group without the switch receiving a host membership report. The default is 260 seconds.

`leave_timer <sec 1-16711450>` – Leave timer. The default is 2 seconds.

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

**Restrictions**      Only administrator-level users can issue this command.

### Example Usage:

To configure the IGMP snooping:

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

```
Success.
```



DGS-3224TGR:4#

**config igmp\_snooping querier**

Purpose	Used to configure the time in seconds between general query transmissions, the maximum time in seconds to wait for reports from members, the permitted packet loss that guarantees IGMP snooping.
Syntax	<b>config igmp_snooping querier</b> [<vlan_name 32>   all] {query_interval <sec 1-65535>   max_response_time <sec 1-25>   robustness_variable <value 1-255>   last_member_query_interval <sec 1-65535>   state [enable   disable]}
Description	This command configures IGMP snooping querier.
Parameters	<p>&lt;vlan_name 32&gt; – The name of the VLAN for which IGMP snooping querier is to be configured.</p> <p>query_interval &lt;sec 1-65535&gt; – Specifies the amount of time in seconds between general query transmissions. The default setting is 125 seconds.</p> <p>max_response_time &lt;sec 1-25&gt; – Specifies the maximum time in seconds to wait for reports from members. The default setting is 10 seconds.</p> <p>robustness_variable &lt;value 1-255&gt; – Provides fine-tuning to allow for expected</p>

**config igmp\_snooping querier**

packet loss on a subnet. The value of the robustness variable is used in calculating the following IGMP message intervals:

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

last\_member\_query\_interval <sec 1-65535>

### **config igmp\_snooping querier**

– The maximum amount of time between group-specific query messages, including those sent in response to leave-group messages. You might lower this interval to reduce the amount of time it takes a router to detect the loss of the last member of a group.

state [enable|disable] – Allows the switch to be specified as an IGMP Querier or Non-querier.

Restrictions      Only administrator-level users can issue this command.

#### Example Usage:

To configure IGMP snooping:

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

```
Command: config igmp_snooping querier default  
query_interval 125 state enable
```

```
Success.
```

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

**config router\_ports**

Purpose	Used to configure ports as router ports.
Syntax	<b>config router_ports &lt;vlan_name 32&gt; [add   delete] &lt;portlist&gt;</b>
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	<p>&lt;vlan_name 32&gt; – The name of the VLAN on which the router port resides.</p> <p>&lt;portlist&gt; – Specifies a range of ports which will be configured as router ports. The port list is specified by listing the beginning port number and the highest port number of the range. The beginning and end of the port list range are separated by a dash. For example, 3 would specify port 3. 4 specifies port 4. 3-4 specifies all of the ports between port 3 and port 4 – in numerical order.</p>
Restrictions	Only administrator-level users can issue this command.

## Example Usage:

To set up static router ports:

**DGS-3224TGR:4#config router\_ports default add1-10**  
**Command: config router\_ports default add 1-10**

**Success.**

**DGS-3224TGR:4#**

## **enable igmp\_snooping**

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

Example Usage:

To enable IGMP snooping on the switch:

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

Success.

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

## **disable igmp\_snooping**

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

Example Usage:

To disable IGMP snooping on the switch:

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

**Success.**

**DGS-3224TGR:4#**

## **show igmp\_snooping**

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

Example Usage:

To show IGMP snooping:

**DGS-3224TGR:4#show igmp\_snooping**  
**Command: show igmp\_snooping**

```
IGMP Snooping Global State : Disabled  
Multicast router Only      : Disabled  
  
VLAN Name                   : default  
Query Interval              : 125  
Max Response Time           : 10
```

```

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

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

Total Entries: 2

DGS-3224TGR:4#

### **show igmp\_snooping group**

**Purpose**                      Used to display the current IGMP snooping group configuration on the switch.

**Syntax**                      **show igmp\_snooping group {vlan <vlan\_name 32>}**

**Description**                This command will display the current IGMP snooping group configuration on the switch.



**show igmp\_snooping group**

Parameters	<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-3224TGR:4#show igmp_snooping group
Command: show igmp_snooping group
```

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

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

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

```
Total Entries : 3
```

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

**show router\_ports**

Purpose	Used to display the currently configured router ports on the switch.
Syntax	<b>show router_ports {vlan &lt;vlan_name 32&gt;} {static   dynamic}</b>
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-3224TGR:4#show router_ports
Command: show router_ports

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

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

**Total Entries:** 2

**DGS-3224TGR:4#**

**19**

---

## ***ROUTING TABLE COMMANDS***

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

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

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

## create iproute

Purpose	Used to create an IP route entry to the switch's IP routing table.
Syntax	<b>create iproute</b> <b>[default   &lt;network_address&gt;] &lt;ipaddr&gt;</b> <b>{&lt;metric&gt;}</b>
Description	This command is used to create an IP route entry to the switch's IP routing table.
Parameters	default – creates a default IP route entry.  <network_address> – IP address and netmask of the IP interface that is the destination of the route. You can specify the address and mask information using the traditional format (for example, 10.1.2.3/255.0.0.0 or in CIDR format, 10.1.2.3/16).  <ipaddr> – The IP address for the next hop router.  <metric> – The default setting is 1.
Restrictions	Only administrator-level users can issue this command.

### Example Usage:

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

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

```
Command: create iproute 10.48.74.121/8 10.1.1.254 1
```

```
Success.
```

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

## delete iproute

**Purpose** Used to delete an IP route entry from the switch's IP routing table.

**Syntax** **delete iproute**  
**[default] <network\_address>**

**Description** This command will delete an existing entry from the switch's IP routing table.

**Parameters** default – Deletes a default IP route entry.

<network\_address> – IP address and netmask of the IP interface that is the destination of the route. You can specify the address and mask information using the traditional format (for example, 10.1.2.3/255.0.0.0) or in CIDR format, 10.1.2.3/16).

**Restrictions** Only administrator-level users can issue this command.

Example Usage:

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

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

**Success.**

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

## show iproute

Purpose	Used to display the switch's current IP routing table.
Syntax	<b>show iproute</b> {<network_address>} {static   rip   ospf}
Description	This command will display the switch's current IP routing table.
Parameters	<network_address> - IP address and netmask of the IP interface that is the destination of the route. You can specify the address and mask information using the traditional format (for example, 10.1.2.3/255.0.0.0 or in CIDR format, 10.1.2.3/16).
Restrictions	none.

Example Usage:

To display the contents of the IP routing table:

DGS-3224TGR:4#show iproute

Command: show iproute

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

Total Entries: 2

DGS-3224TGR:4#



## 20

## 802.1X COMMANDS

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

<b>Command</b>	<b>Parameters</b>
<b>enable 802.1x</b>	
<b>disable 802.1x</b>	
<b>config 802.1x auth_protocol</b>	[local radius_eap]
<b>config 802.1x capability</b>	ports <portlist> all authenticator none
<b>config 802.1x auth_parameter</b>	ports <portlist> all default direction [both in] port_control [force_unauth auto force_auth] quiet_period <sec 0-65535> tx_period <sec 1-65535> supp_timeout <sec 1-65535> server_timeout <sec 1-65535> max_req <value 1-10> reauth_period <sec 1-999999999>

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

**enable 802.1x**

**enable 802.1x**

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

## Example Usage:

To enable 802.1x switch-wide:

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

```
Success.
```

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

**disable 802.1x**

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

## **disable 802.1x**

Access control server application on the switch.

Parameters None.

Restrictions Only administrator-level users can issue this command.

Example Usage:

To disable 802.1x on the switch:

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

**Success.**

**DGS-3224TGR:4#**

## **config 802.1x auth\_protoco**

Purpose Used to configure the 802.1x authentication protocol on the switch.

Syntax **config 802.1x auth\_protocol [local|radius\_eap]**

Description The config 802.1x auth\_protocol command enables you to configure the authentication protocol.

Parameters local|radius\_EAP - Specify the type of authentication protocol desired.

**config 802.1x auth\_protoco**

Restrictions      Only administrator-level users can issue this command.

Example Usage:

To configure 802.1x authentication protocol:

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

Success.

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

**config 802.1x capability**

Purpose              Used to configure the 802.1x capability of a range of ports on the switch.

Syntax             **config 802.1x capability ports**  
**[<portlist> | all] [authenticator | none]**

Description        The config 802.1x command has two capabilities that can be set for each port: Authenticator and None.

Parameters        <portlist> – Specifies a range of ports. The port list is specified by listing the beginning port number and the highest port number of the range. The beginning and end of the port list range are separated by a dash. For example, 3 would specify port 3. 4 specifies port 4. 3-4 specifies all of the ports between port 3 and port 4 – in numerical order.

**config 802.1x capability**

all – Specifies all of the ports on the switch.

authenticator – A user must pass the authentication process to gain access to the network.

none – The port is not controlled by the 802.1x functions.

Restrictions Only administrator-level users can issue this command.

## Example Usage:

To configure 802.1x capability on ports 1-10:

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

**Success.**

DGS-3224TGR:4#

**config 802.1x auth\_parameter**

Purpose Used to configure the 802.1x Authentication parameters on a range of ports. The default parameter will return all ports in the specified range to their default 802.1x settings.

Syntax **config 802.1x auth\_parameter ports**  
 [<portlist> | all] [default | {direction  
 [both | in] | port\_control  
 [force\_unauth | auto | force\_auth] |  
 quiet\_period <sec 0-65535> | max\_req

**config 802.1x auth\_parameter**

	<b>&lt;value 1-10&gt; reauth_period &lt;sec 1-65535&gt; enable_reauth [enabled disabled];]</b>
Description	The config 802.1x auth_parameter command is used to configure the 802.1x Authentication parameters on a range of ports. The default parameter will return all ports in the specified range to their default 802.1x settings.
Parameters	<p>&lt;portlist&gt; – Specifies a range of ports. The port list is specified by listing the beginning port number and the highest port number of the range. The beginning and end of the port list range are separated by a dash. For example, 3 would specify port 3. 4 specifies port 4. 3-4 specifies all of the ports between port 3 and port 4 – in numerical order.</p> <p>all – Specifies all of the ports on the switch.</p> <p>default – Returns all of the ports in the specified range to their 802.1x default settings.</p> <p>direction [both in] – Determines whether a controlled port blocks communication in both the receiving and transmitting directions, or just the receiving direction.</p> <p>port_control – Configures the administrative control over the authentication process for the range of ports.</p> <p>force_auth – Forces the Authenticator for the port to become authorized. Network access is allowed.</p>

**config 802.1x auth\_parameter**

auto – Allows the port's status to reflect the outcome of the authentication process.

force\_unauth – Forces the Authenticator for the port to become unauthorized. Network access will be blocked.

quiet\_period <sec 0-65535> – Configures the time interval between authentication failure and the start of a new authentication attempt.

max\_req <value 1-10> – Configures the number of times to retry sending packets to a supplicant (user).

reauth\_period <sec 1-65535> – Configures the time interval between successive re-authentications.

enable\_reauth [enabled|disabled] – Determines whether or not the switch will re-authenticate. Enabled causes re-authentication of users at the time interval specified in the Re-authentication Period field, above.

Restrictions Only administrator-level users can issue this command.

## Example Usage:

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

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



**both**

**Success.**

**DGS-3224TGR:4#**

## **config 802.1x init**

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

Example Usage:

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

**DGS-3224TGR:4#config 802.1x init ports 1-15****Command: config 802.1x init ports 1-15****Success.****DGS-3224TGR:4#****config 802.1x reauth**

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

## Example Usage:

To configure 802.1x reauthentication for ports 1-15:

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

Success.

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

## config radius add

Purpose	Used to configure the settings the switch will use to communicate with a RADIUS server.
Syntax	<b>config radius add &lt;server_index 1-3&gt; &lt;server_ip&gt; key &lt;passwd 32&gt; [default {auth_port &lt;udp_port_numbe 1-65535&gt;  acct_port &lt;udp_port_number 1-65535&gt;}]</b>
Description	The config radius add command is used to configure the settings the switch will use to communicate with a RADIUS server.
Parameters	<p>&lt;server_index 1-3&gt; – Assigns a number to the current set of RADIUS server settings. Up to three groups of RADIUS server settings can be entered on the switch.</p> <p>&lt;server_ip&gt; – The IP address of the RADIUS server.</p> <p>key – Specifies that a password and encryption key will be used between the switch and the RADIUS server.</p> <p>&lt;passwd 32&gt; – The shared-secret key used by the RADIUS server and the</p>

**config radius add**

switch. Up to 32 characters can be used.

**default** – Returns all of the ports in the range to their default RADIUS settings.

**auth\_port** <udp\_port\_number 1-65535> – The UDP port number for authentication requests. The default is 1812.

**acct\_port** <udp\_port\_number 1-65535> – The UDP port number for accounting requests. The default is 1813.

**Restrictions** Only administrator-level users can issue this command.

## Example Usage:

To configure RADIUS server communication settings:

**DGS-3224TGR:4#config radius add 1 10.48.74.121 key dlink default**  
**Command: config radius add 1 10.48.74.121 key dlink default**

**Success.**

**DGS-3224TGR:4#**

**config radius delete**

**Purpose** Used to delete a previously entered RADIUS server configuration.

**Syntax** **config radius delete <server\_index 1-3>**

**config radius delete**

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

## Example Usage:

To delete previously configured RADIUS server communication settings:

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

Success.

DGS-3224TGR:4#
```

**config radius**

Purpose	Used to configure the switch's RADIUS settings.
Syntax	<b>config radius &lt;server_index 1-3&gt; {ipaddress &lt;server_ip&gt; {ipaddress &lt;server_ip&gt;   key &lt;passwd 32&gt;   auth_port &lt;udp_port_number 1-65535&gt;   acct_port &lt;udp_port_number 1-65535&gt;}}</b>

**config radius**

Description	The config radius command is used to configure the switch's RADIUS settings.
Parameters	<p>&lt;server_index 1-3&gt; – Assigns a number to the current set of RADIUS server settings. Up to three groups of RADIUS server settings can be entered on the switch.</p> <p>&lt;server_ip&gt; – The IP address of the RADIUS server.</p> <p>key – Specifies that a password and encryption key will be used between the switch and the RADIUS server.</p> <p>&lt;passwd 32&gt; – The shared-secret key used by the RADIUS server and the switch. Up to 32 characters can be used.</p> <p>default – Returns all of the ports in the range to their default RADIUS settings.</p> <p>auth_port &lt;udp_port_number 1-65535&gt; – The UDP port number for authentication requests. The default is 1812.</p> <p>acct_port &lt;udp_port_number 1-65535&gt; – The UDP port number for accounting requests. The default is 1813.</p>
Restrictions	Only administrator-level users can issue this command.

## Example Usage:

To configure RADIUS settings:

```
DGS-3224TGR:4#config radius add 1 10.48.74.121 key dlink default  
Command: config radius add 1 10.48.74.121 key dlink default
```

```
Success.
```

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

## show radius

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

Example Usage:

To display RADIUS settings on the switch:

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

```
Command: show radius
```

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

```
Total Entries : 3
```

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

**show 802.1x user**

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

## Example Usage:

To show the 802.1x user:

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

```

Index  UserName
-----  -
1        ctsnow

```

DGS-3224TGR:4#

**create 802.1x user**

Purpose	Used to create a new 802.1x user.
Syntax	<b>create 802.1x user &lt;username 15&gt;</b>
Description	The create 802.1x user command is used to create new 802.1x users.
Parameters	<username 15> – A username can be as



### **create 802.1x user**

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

Example Usage:

To create an 802.1x user:

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

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

DGS-3224TGR:4#
```

### **delete 802.1x user**

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

Example Usage:

To delete 802.1x users:

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

**Command: delete 802.1x user ctsnow**

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

**Success.**

**DGS-3224TGR:4#**

## **show auth\_statistics**

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

Example Usage:

To display authentication statistics:

**DGS-3224TGR:4#show auth\_statistics**

**Command: show auth\_statistics**

Port number : 1

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

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

### show auth\_diagnostics

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

**show auth\_diagnostics**

this command.

Example Usage:

To display authentication diagnostics statistics:

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

Port number   : 1

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

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

**show auth\_session\_statistic ;**

Purpose                      Used to display the authentication session statistics.

**show auth\_session\_statistics**

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

## Example Usage:

To display authentication session statistics:

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

Port number : 1

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

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

## **show radius auth\_client**

Purpose	Used to display the switch's RADIUS authentication client statistics.
Syntax	<b>show radius auth_client</b>
Description	The show radius auth_client command is used to display RADIUS authentication client statistics.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To display RADIUS authentication client statistics:

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

radiusAuthClient ==>
radiusAuthClientInvalidServerAddresses      0
radiusAuthClientIdentifier                  D-Link

radiusAuthServerEntry ==>
radiusAuthServerIndex :1

radiusAuthServerAddress                      0.0.0.0
radiusAuthClientServerPortNumber           0
radiusAuthClientRoundTripTime              0
radiusAuthClientAccessRequests             0
radiusAuthClientAccessRetransmissions      0
radiusAuthClientAccessAccepts              0
radiusAuthClientAccessRejects              0
radiusAuthClientAccessChallenges           0
```

```
radiusAuthClientMalformedAccessResponses 0
radiusAuthClientBadAuthenticators        0
radiusAuthClientPendingRequests          0
radiusAuthClientTimeouts                  0
radiusAuthClientUnknownTypes              0
radiusAuthClientPacketsDropped            0
CTRL+C|ESC|q Quit SPACE|n Next Page|p Previous Page|r Refresh
```

<b>show radius acct_client</b>	
Purpose	Used to configure the switch's RADIUS account client statistics.
Syntax	<b>show radius acct_client</b>
Description	The show radius acct_client command is used to display the switch's RADIUS account client statistics.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

To display the RADIUS account client statistics:

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

radiusAcctClient ==>
radiusAcctClientInvalidServerAddresses 0
radiusAcctClientIdentifier             D-Link

radiusAuthServerEntry ==>
radiusAccServerIndex : 1
```

radiusAccServerAddress	0.0.0.0
radiusAccClientServerPortNumber	0
radiusAccClientRoundTripTime	0
radiusAccClientRequests	0
radiusAccClientRetransmissions	0
radiusAccClientResponses	0
radiusAccClientMalformedResponses	0
radiusAccClientBadAuthenticators	0
radiusAccClientPendingRequests	0
radiusAccClientTimeouts	0
radiusAccClientUnknownTypes	0
radiusAccClientPacketsDropped	0

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



**21*****ACCESS CONTROL LIST  
(ACL) COMMANDS***

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

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

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

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

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

Access profiles allow you to establish criteria to determine whether the switch will forward packets based on the information contained in each packet's header. These criteria can be specified on a VLAN-by-VLAN basis.

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

```
create access_profile ip source_ip_mask 255.255.255.0
profile_id 1 deny
```

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

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

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

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

```
config access_profile profile_id 1 add access_id 1 ip  
source_ip 10.42.73.1
```

Here we use the `profile_id 1` which was specified when the access profile was created. The `add` parameter instructs the switch to add the criteria that follows to the list of rules that are associated with access profile 1. For each rule entered into the access profile, you can assign an `access_id` that both identifies the rule and establishes a priority within the list of rules. A lower `access_id` gives the rule a higher priority. In case of a conflict in the rules entered for an access profile, the rule with the highest priority (lowest `access_id`) will take precedence.

The `ip` parameter instructs the switch that this new rule will be applied to the IP addresses contained within each frame's header. `source_ip` tells the switch that this rule will apply to the source IP addresses in each frame's header. Finally, the IP address 10.42.73.1 will be combined with the `source_ip_mask` 255.255.255.0 to give the IP address 10.42.73.0 for any source IP address between 10.42.73.0 to 10.42.73.255.

## create access\_profile

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

**create access\_profile**

Specific values for the rules are entered using the config access\_profile command, below.

**Parameters**

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

vlan – Specifies that the switch will examine the VLAN part of each packet header.

source\_mac <macmask> – Specifies a MAC address mask for the source MAC address. This mask is entered in the following hexadecimal format,

destination\_mac <macmask> – Specifies a MAC address mask for the destination MAC address.

802.1p – Specifies that the switch will examine the 802.1p priority value in the frame's header.

ethernet\_type – Specifies that the switch will examine the Ethernet type value in each frame's header.

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

vlan – Specifies a VLAN mask.

source\_ip\_mask <netmask> – Specifies an IP address mask for the source IP address.

destination\_ip\_mask <netmask> – Specifies an IP address mask for the destination IP address.

**create access\_profile**

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

tos <value 0-127>– Specifies that the switch will examine the Type of Service value in each frame's header.

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

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

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

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

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

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

src\_port\_mask <hex 0x0-0xffff> – Specifies a TCP port mask for the source port.

dst\_port\_mask <hex 0x0-0xffff> – Specifies a TCP port mask for the destination port.

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

## **create access\_profile**

Protocol (UDP) field.

src\_port\_mask <hex 0x0-0xffff> – Specifies a UDP port mask for the source port.

dst\_port\_mask <hex 0x0-0xffff> – Specifies a UDP port mask for the destination port.

protocol\_id – Specifies that the switch will examine each frame's Protocol ID field.

user\_mask <hex 0x0-0xffffffff> – Specifies that the rule applies to the IP protocol ID and the mask options behind the IP header.

permit – Specifies that packets that match the access profile are permitted to be forwarded by the switch.

deny – Specifies that packets that do not match the access profile are not permitted to be forwarded by the switch and will be filtered.

profile\_id <value 1-255> – Specifies an index number that will identify the access profile being created with this command.

Restrictions Only administrator-level users can issue this command.

Example Usage:



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

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

Success.

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

## **delete access\_profile**

Purpose	Used to delete a previously created access profile.
Syntax	<b>delete access_profile [profile_id &lt;value 1-255&gt;]</b>
Description	The delete access_profile command is used to delete a previously created access profile on the switch.
Parameters	profile_id <value 1-255> – An integer between 1 and 255 that is used to identify the access profile that will be deleted with this command. This value is assigned to the access profile when it is created with the create access_profile command.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

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

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

**Success.**

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

## config access\_profile

**Purpose** Used to configure an access profile on the switch and to define specific values that will be used to by the switch to determine if a given packet should be forwarded or filtered. Masks entered using the create access\_profile command will be combined, using a logical AND operation, with the values the switch finds in the specified frame header fields. Specific values for the rules are entered using the config access\_profile command, below.

**Syntax** **config access\_profile profile\_id <value 1-255> [add access\_id <value 1-255>] [ethernet {vlan <vlan\_name 32> | source\_mac <macaddr> | destination\_mac <macaddr> | 802.1 <value 0-7> | ethernet\_type <hex 0x0-0xffff> | ip {vlan <vlan\_name> | source\_ip <ipaddr> | destination\_ip <ipaddr> | dscp <value 0-63> | [icmp {type <value 0-65535> code <value 0-255>} | igmp {type <value 0-255>} | tcp {src\_port <value 0-65535> | dst\_port <value 0-65535>} | udp {src\_port <value 0-65535> | dst\_port**

**config access\_profile**

```

<value 0-65535> | protocol_id <value 0-
255> {user_define <hex 0x0-
0xffffffff>}} | priority <value 0-7>
{replace_priority} | replace_dscp <value 0-
63> | delete <value 1-255>]

```

Description	<p>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.</p>
Parameters	<p>profile_id &lt;value 1-255&gt; –</p> <p>add access_id &lt;value 1-255&gt; – Adds an additional rule to the above specified access profile. The value specifies the relative priority of the additional rule. A lower access ID, the higher the priority the rule will be given.</p> <p>ethernet – Specifies that the switch will look only into the layer 2 part of each packet.</p> <p>vlan &lt;vlan_name 32&gt; – Specifies that the access profile will apply to only to this VLAN.</p> <p>source_mac &lt;macaddr&gt; – Specifies that the access profile will apply to only packets with this source MAC address.</p> <p>destination_mac &lt;macaddr&gt; – Specifies that the access profile will apply to only packets with this destination MAC address.</p>

## **config access\_profile**

802.1p <value 0-7> – Specifies that the access profile will apply only to packets with this 802.1p priority value.

ethernet\_type <hex 0x0-0xffff> – Specifies that the access profile will apply only to packets with this 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\_id <value 0-255> – Specifies that the access profile will apply to only packets with this destination IP address.

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

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

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

code <value 0-255> – Specifies that the

## **config access\_profile**

access\_profile will apply to this ICMP code.

igmp – Specifies that the switch will examine the Internet Group Management Protocol (IGMP) field within each packet.

type <value 0-255> – Specifies that the access profile will apply to packets that have this IGMP type value.

tcp – Specifies that the switch will examine the Transmission Control Protocol (TCP) field within each packet.

src\_port <value 0-65535> – Specifies that the access profile will apply only to packets that have this TCP source port in their TCP header.

dst\_port <value 0-65535> – Specifies that the access profile will apply only to packets that have this TCP destination port in their TCP header.

udp – Specifies that the switch will examine the Universal Datagram Protocol (UDP) field in each packet.

src\_port <value 0-65535> – Specifies that the access profile will apply only to packets that have this UDP source port in their header.

dst\_port <value 0-65535> – Specifies that the access profile will apply only to packets that have this UDP destination port in their header.

protocol\_id <value 0-255> – Specifies that the switch will examine the Protocol

**config access\_profile**

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

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

`priority <value 0-7>` – Specifies that the access profile will apply to packets that contain this value in their 802.1p priority field of their header.

`replace_priority` – This parameter is specified if you want to change the 802.1p user priority of a packet that meets the specified criteria. Otherwise, a packet will have its incoming 802.1p user priority rewritten to its original value before being transmitted from the switch.

`replace_dscp <value 0-63>` – Allows you to specify a value to be written to the DSCP field of an incoming packet that meets the criteria specified in the first part of the command. This value will over-write the value in the DSCP field of the packet.

`delete <value 1-255>` – Specifies that the access ID of a rule you want to delete.

**Restrictions** Only administrator-level users can issue this command.

Example Usage:

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

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

**Success.**

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

### **show access\_profile**

Purpose	Used to display the currently configured access profiles on the switch.
Syntax	<b>show access_profile</b>
Description	The show access_profile command is used to display the currently configured access profiles
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example Usage:

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

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

Access Profile Table

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



## 22

## SSH COMMANDS

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

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

<b>Command</b>	<b>Parameters</b>
<b>disable ssh</b>	

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

<b>config ssh algorithm</b>	
Purpose	Used to configure the SSH algorithm.
Syntax	<b>config ssh algorithm</b> <b>[3DES   Blowfish   MD5   SHA1   DSA   RSA]</b> <b>[enable   disable]</b>
Description	This command allows you to configure the desired type of SSH algorithm.
Parameters	[3DES   Blowfish   MD5   SHA1   DSA   RSA] – Choose the desired security algorithm.  [enable   disable] – This allows you to enable or disable the SSH algorithm.
Restrictions	None.

Usage Example:

To configure SSH algorithm:

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

Success.

DGS-3224TGR:4#
```

## **show ssh algorithm**

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

Usage Example:

To display the SSH algorithm:

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

### **Encryption Algorithm**

```
MD5      : Enabled  
SHA      : Enabled  
DSA      : Enabled  
RSA      : Enabled  
3DES     : Enabled  
Blowfish : Enabled
```

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

## config ssh authmode

Purpose	Used to configure the SSH authentication mode setting.
Syntax	<b>config ssh authmode [password   publickey   hostbased] [enable   disable]</b>
Description	This command will allow you to configure the SSH authentication mode.
Parameters	[password   publickey   hostbased] – Choose the desired SSH authentication mode.  [enable   disable] – This allows you to enable or disable SSH authentication.
Restrictions	None.

Usage Example:

To display the SSH algorithm:

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

```
Command: show ssh algorithm
```

### Encryption Algorithm

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

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

## show ssh authmode

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

Usage Example:

To display the SSH authmode:

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

```
Authentication Algorithm
Hostbased : Enabled
Password : Enabled
Publickey : Enabled
```

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

## config ssh user

Purpose	Used to configure the SSH user.
Syntax	<b>config ssh user &lt;username&gt; authmode</b> <b>[Publickey   Password   Hostbased]</b>

**config ssh user**

	<b>[Publickey   Password   Hostbased [host_name &lt;domain_name 32&gt;   hostname_IP &lt;domain_name 32&gt; &lt;ipaddr&gt;]]</b>
Description	This command allows you to modify the parameters of the SSH user.
Parameters	<p>&lt;username&gt; – Enter an optional SSH user name.</p> <p>authmode – Select the type of security authentication mode: [Publickey   Password   Hostbased [host_name &lt;domain_name 32&gt;   hostname_IP &lt;domain_name 32&gt; &lt;ipaddr&gt;]] .</p>
Restrictions	None.

## Usage Example:

To configure the SSH user:

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

Success.

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

**show ssh user**

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

Usage Example:

To display the SSH user:

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

Account is empty!

DGS-3224TGR:4#
```

**config ssh server**

Purpose	Used to configure the SSH server.
Syntax	<b>config ssh server {maxsession &lt;int 1-8&gt;   contimeout &lt;min 2-20&gt;   authfail &lt;int 2-20&gt;   rekey [10min   30min   60min   never]}</b>
Description	This command allows you to configure the SSH server.

**config ssh server**

Parameters	<p>maxsession &lt;int 1-8&gt; – Allows the user to set the number of times an outside guest may attempt to log on to the switch.</p> <p>contimeout &lt;min 2-20&gt; – Allows the user to set the connection timeout.</p> <p>authfail &lt;int 2-20&gt; – Allows the user to set the maximum number of authentication fail attempts.</p> <p>rekey [10min  30min   60min  never] – Sets the time period that the switch will change the security shell encryptions.</p>
Restrictions	None.

Usage Example:

To configure the SSH server:

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

**show ssh server**



**show ssh server**

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

Usage Example:

To display the SSH server:

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

The SSH server configuration

```
Max Session      : 8
Connection Timeout : 300
Authfail Attempts : 2
Rekey Timeout    : 60min
```

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

**enable ssh**

Purpose	Used to enable SSH.
Syntax	<b>enable ssh</b>
Description	This command allows you to enable SSH on the switch.

## **enable ssh**

on the switch.

Parameters        None.

Restrictions      None.

Usage Example:

To enable SSH:

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

**Success.**

**DGS-3224TGR:4#**

## **disable ssh**

Purpose             Used to disable SSH.

Syntax            **disable ssh**

Description      This command allows you to disable SSH on the switch.

Parameters       None.

Restrictions      None.

Usage Example:

To disable SSH:

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

```
Command: disable ssh
```

```
Success.
```

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

---

## ***COMMAND HISTORY LIST***

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

<b>Command</b>	<b>Parameters</b>
<b>?</b>	
<b>show command_history</b>	
<b>dir</b>	
<b>config command_history</b>	<value>

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

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

**?**

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

Usage Example:

To display all of the commands in the CLI:

```
DGS-3224TGR:4#?  
Command: ?  
  
..  
?  
clear  
clear arptable  
clear counters  
clear fdb  
clear log  
config 802.1p default_priority  
config 802.1p user_priority  
config 802.1x auth_parameter ports  
config 802.1x auth_protocol  
config 802.1x capability ports  
config 802.1x init ports  
config 802.1x reauth ports  
config access_profile profile_id  
config account  
config arp_aging time  
config bandwidth_control  
config command_history
```

```
config fdb aging_time
config gvrp
config hol prevention
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	<b>show command_history</b>
Description	This command will display the command history.
Parameters	None.
Restrictions	None.

Usage Example:

To display the command history:

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

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

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

## **dir**

Purpose	Used to display all commands.
Syntax	<b>dir</b>
Description	This command will display all commands.
Parameters	None.
Restrictions	None.

Usage Example:

To display all of the commands:

```
DGS-3224TGR:4#dir
Command: dir
..
?
clear
clear arptable
clear counters
clear fdb
clear log
config 802.1p default_priority
config 802.1p user_priority
config 802.1x auth_parameter ports
```

```

config 802.1x auth_protocol
config 802.1x capability ports
config 802.1x init ports
config 802.1x reauth ports
config access_profile profile_id
config account
config arp_aging time
config bandwidth_control
config command_history
config fdb aging_time
config gvrp
config hol prevention
CTRL+C ESC q Quit SPACE n Next Page Enter Next Entry a All
    
```

### config command\_history

Purpose	Used to configure the command history.
Syntax	<b>config command_history &lt;value 1-40&gt;</b>
Description	This command is used to configure the command history.
Parameters	<value 1-40> – This value represents the number of commands to be displayed.
Restrictions	None.

Usage Example:

To configure the command history:

```

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



**Success.**

**DGS-3224TGR:4#**



# TECHNICAL SPECIFICATIONS

<b>General</b>													
Standards:	IEEE 802.3 10BASE-T Ethernet IEEE 802.3u 100BASE-TX Fast Ethernet IEEE 802.3z 1000BASE-SX Gigabit Ethernet IEEE 802.1 P/Q VLAN IEEE 802.3x Full-duplex Flow Control ANSI/IEEE 802.3 Nway auto-negotiation												
Protocols:	CSMA/CD												
Data Transfer Rates:	<table style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 30%;"></th> <th style="width: 35%; text-align: center;">Half-duplex</th> <th style="width: 35%; text-align: center;">Full-duplex</th> </tr> </thead> <tbody> <tr> <td>Ethernet</td> <td style="text-align: center;">10 Mbps</td> <td style="text-align: center;">20Mbps</td> </tr> <tr> <td>Fast Ethernet</td> <td style="text-align: center;">100Mbps</td> <td style="text-align: center;">200Mbps</td> </tr> <tr> <td>Gigabit Ethernet</td> <td style="text-align: center;">n/a</td> <td style="text-align: center;">2000Mbps</td> </tr> </tbody> </table>		Half-duplex	Full-duplex	Ethernet	10 Mbps	20Mbps	Fast Ethernet	100Mbps	200Mbps	Gigabit Ethernet	n/a	2000Mbps
	Half-duplex	Full-duplex											
Ethernet	10 Mbps	20Mbps											
Fast Ethernet	100Mbps	200Mbps											
Gigabit Ethernet	n/a	2000Mbps											
Topology:	Star												

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

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

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

<b>Performance</b>	
Transmission Method:	Store-and-forward
RAM Buffer:	2 MB per device
Packet Filtering/ Forwarding Rate:	Full-wire speed for all connections.  1,488,000 pps per port (for 1000Mbps)
MAC Address Learning:	Automatic update. Supports 16K MAC address
Priority Queues:	8 Priority Queues per port
Forwarding Table Age Time:	Max age:10-1000000 seconds. Default = 300.