D-Link®

# DGS-3212SR

Command Line Interface Reference Manual

First Edition (August 2003)

…….

## Wichtige Sicherheitshinweise

1. Bitte lesen Sie sich diese Hinweise sorgfältig durch.
2. Heben Sie diese Anleitung für den spätern Gebrauch auf.
3. Vor jedem Reinigen ist das Gerät vom Stromnetz zu trennen. Vervenden Sie keine Flüssig- oder Aerosolreiniger. Am besten dient ein angefeuchtetes Tuch zur Reinigung.
4. Um eine Beschädigung des Gerätes zu vermeiden sollten Sie nur Zubehörteile verwenden, die vom Hersteller zugelassen sind.
5. Das Gerät is vor Feuchtigkeit zu schützen.
6. Bei der Aufstellung des Gerätes ist auf sichern Stand zu achten. Ein Kippen oder Fallen könnte Verletzungen hervorrufen. Verwenden Sie nur sichere Standorte und beachten Sie die Aufstellhinweise des Herstellers.
7. Die Belüftungsöffnungen dienen zur Luftzirkulation die das Gerät vor Überhitzung schützt. Sorgen Sie dafür, daß diese Öffnungen nicht abgedeckt werden.
8. Beachten Sie beim Anschluß an das Stromnetz die Anschlußwerte.
9. Die Netzanschlußsteckdose muß aus Gründen der elektrischen Sicherheit einen Schutzleiterkontakt haben.
10. Verlegen Sie die Netzanschlußleitung so, daß niemand darüber fallen kann. Es sollete auch nichts auf der Leitung abgestellt werden.
11. Alle Hinweise und Warnungen die sich am Geräten befinden sind zu beachten.
12. Wird das Gerät über einen längeren Zeitraum nicht benutzt, sollten Sie es vom Stromnetz trennen. Somit wird im Falle einer Überspannung eine Beschädigung vermieden.
13. Durch die Lüftungsöffnungen dürfen niemals Gegenstände oder Flüssigkeiten in das Gerät gelangen. Dies könnte einen Brand bzw. Elektrischen Schlag auslösen.
14. Öffnen Sie niemals das Gerät. Das Gerät darf aus Gründen der elektrischen Sicherheit nur von authorisiertem Servicepersonal geöffnet werden.
15. Wenn folgende Situationen auftreten ist das Gerät vom Stromnetz zu trennen und von einer qualifizierten Servicestelle zu überprüfen:
16. Netzkabel oder Netzstecker sint beschädigt.
17. Flüssigkeit ist in das Gerät eingedrungen.
18. Das Gerät war Feuchtigkeit ausgesetzt.
19. Wenn das Gerät nicht der Bedienungsanleitung ensprechend funktioniert oder Sie mit Hilfe dieser Anleitung keine Verbesserung erzielen.
20. Das Gerät ist gefallen und|oder das Gehäuse ist beschädigt.
21. Wenn das Gerät deutliche Anzeichen eines Defektes aufweist.
22. Bei Reparaturen dürfen nur Orginalersatzteile bzw. den Orginalteilen entsprechende Teile verwendet werden. Der Einsatz von ungeeigneten Ersatzteilen kann eine weitere Beschädigung hervorrufen.
23. Wenden Sie sich mit allen Fragen die Service und Repartur betreffen an Ihren Servicepartner. Somit stellen Sie die Betriebssicherheit des Gerätes sicher.
24. Zum Netzanschluß dieses Gerätes ist eine geprüfte Leitung zu verwenden, Für einen Nennstrom bis 6A und einem Gerätegewicht größer 3kg ist eine Leitung nicht leichter als H05VV-F, 3G, 0.75mm2 einzusetzen.

## WARRANTIES EXCLUSIVE

**IF THE D-LINK PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, THE CUSTOMER'S SOLE REMEDY SHALL BE, AT D-LINK'S OPTION, REPAIR OR REPLACEMENT. THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESSED OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. D-LINK NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION MAINTENANCE OR USE OF D-LINK'S PRODUCTS**

**D-LINK SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THAT THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY THE CUSTOMER'S OR ANY THIRD PERSON'S MISUSE, NEGLECT, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING OR OTHER HAZARD.**

**LIMITATION OF LIABILITY**

**IN NO EVENT WILL D-LINK BE LIABLE FOR ANY DAMAGES, INCLUDING LOSS OF DATA, LOSS OF PROFITS, COST OF COVER OR OTHER INCIDENTAL, CONSEQUENTIAL OR INDIRECT DAMAGES ARISING OUT THE INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE OR INTERRUPTION OF A D- LINK PRODUCT, HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY. THIS LIMITATION WILL APPLY EVEN IF D-LINK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.**

**IF YOU PURCHASED A D-LINK PRODUCT IN THE UNITED STATES, SOME STATES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION MAY NOT APPLY TO YOU.**

## Limited Warranty

### Hardware:

D-Link warrants each of its hardware products to be free from defects in workmanship and materials under normal use and service for a period commencing on the date of purchase from D-Link or its Authorized Reseller and extending for the length of time stipulated by the Authorized Reseller or D-Link Branch Office nearest to the place of purchase.

This Warranty applies on the condition that the product Registration Card is filled out and returned to a D-Link office within ninety (90) days of purchase. A list of D-Link offices is provided at the back of this manual, together with a copy of the Registration Card.

If the product proves defective within the applicable warranty period, D-Link will provide repair or replacement of the product. D-Link shall have the sole discretion whether to repair or replace, and replacement product may be new or reconditioned. Replacement product shall be of equivalent or better specifications, relative to the defective product, but need not be identical. Any product or part repaired by D-Link pursuant to this warranty shall have a warranty period of not less than 90 days, from date of such repair, irrespective of any earlier expiration of original warranty period. When D-Link provides replacement, then the defective product becomes the property of D-Link.

Warranty service may be obtained by contacting a D-Link office within the applicable warranty period, and requesting a Return Material Authorization (RMA) number. If a Registration Card for the product in question has not been returned to D-Link, then a proof of purchase (such as a copy of the dated purchase invoice) must be provided. If Purchaser's circumstances require special handling of warranty correction, then at the time of requesting RMA number, Purchaser may also propose special procedure as may be suitable to the case.

After an RMA number is issued, the defective product must be packaged securely in the original or other suitable shipping package to ensure that it will not be damaged in transit, and the RMA number must be prominently marked on the outside of the package. The package must be mailed or otherwise shipped to D-Link with all costs of mailing|shipping|insurance prepaid. D-Link shall never be responsible for any software, firmware, information, or memory data of Purchaser contained in, stored on, or integrated with any product returned to D-Link pursuant to this warranty.

Any package returned to D-Link without an RMA number will be rejected and shipped back to Purchaser at Purchaser's expense, and D-Link reserves the right in such a case to levy a reasonable handling charge in addition mailing or shipping costs.

### Software:

Warranty service for software products may be obtained by contacting a D-Link office within the applicable warranty period. A list of D-Link offices is provided at the back of this manual, together with a copy of the Registration Card. If a Registration Card for the product in question has not been returned to a D-Link office, then a proof of purchase (such as a copy of the dated purchase invoice) must be provided when requesting warranty service. The term "purchase" in this software warranty refers to the purchase transaction and resulting license to use such software.

D-Link warrants that its software products will perform in substantial conformance with the applicable product documentation provided by D-Link with such software product, for a period of ninety (90) days from the date of purchase from D-Link or its Authorized Reseller. D-Link warrants the magnetic media, on which D-Link provides its software product, against failure during the same warranty period. This warranty applies to purchased software, and to replacement software provided by D-Link pursuant to this warranty, but shall not apply to any update or replacement which may be provided for download via the Internet, or to any update which may otherwise be provided free of charge.

D-Link's sole obligation under this software warranty shall be to replace any defective software product with product which substantially conforms to D-Link's applicable product documentation. Purchaser assumes responsibility for the selection of appropriate application and system|platform software and associated reference materials. D-Link makes no warranty that its software products will work in combination with any hardware, or any application or system|platform software product provided by any third party, excepting only such products as are expressly represented, in D-Link's applicable product documentation as being compatible. D-Link's obligation under this warranty shall be a reasonable effort to provide compatibility, but D-Link shall have no obligation to provide compatibility when there is fault in the third-party hardware or software. D-Link makes no warranty that operation of its software products will be uninterrupted or absolutely error-free, and no warranty that all defects in the software product, within or without the scope of D-Link's applicable product documentation, will be corrected.

### D-Link Offices for Registration and Warranty Service

The product's Registration Card, provided at the back of this manual, must be sent to a D-Link office. To obtain an RMA number for warranty service as to a hardware product, or to obtain warranty service as to a software product, contact the D-Link office nearest you. An address|telephone|fax|e-mail|Web site list of D-Link offices is provided in the back of this manual.

### Trademarks



### Copyright Statement

### FCC Warning

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with this user's guide, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

### CE Mark Warning

This is a Class A product. In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.

### VCCI Warning

注意
この装置は、情報処理装置等電波障害自主規制協議会(VCCI)の基準
に基づく第一種情報技術装置です。この装置を家庭環境で使用すると電波妨
害を引き起こすことがあります。この場合には使用者が適切な対策を講ずる
よう要求されることがあります。

# Table of Contents

# 1

# INTRODUCTION

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

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

## Accessing the Switch via the Serial Port

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

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

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

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


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

There is no initial username or password. Just press the **Enter** key twice to display the CLI input cursor – **DGS-3212SR:4#**. This is the command line where all commands are input.

## Setting the Switch's IP Address

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

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

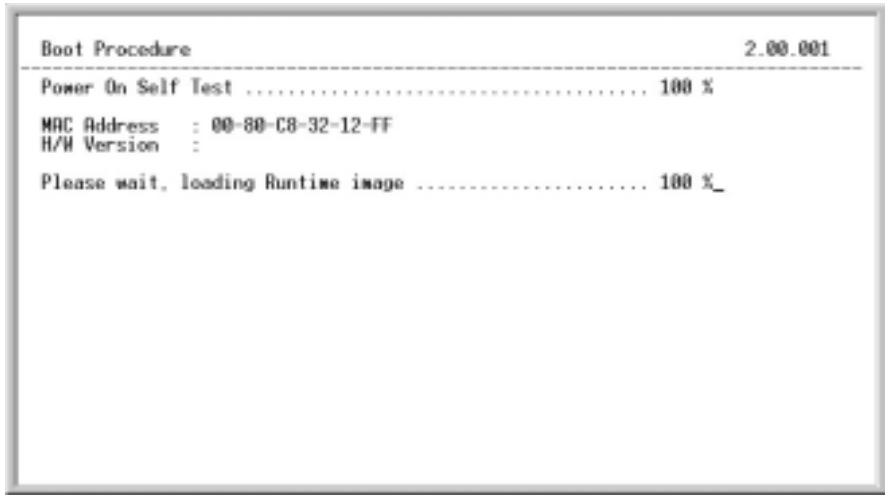


**Figure 1-2. Boot Screen**

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

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

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

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

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

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


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

In the above example, the switch was assigned an IP address of 10.42.73.100 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-3212SR supports a console management interface that allows the user to connect to the switch's management agent via a serial port and a terminal or a computer running a terminal emulation program. The console can also be used over the network using the TCP|IP Telnet protocol. The console program can be used to configure the switch to use an SNMP-based network management software over the network.

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

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

## Connecting to the Switch

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

Your terminal parameters will need to be set to:

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

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

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


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

Commands are entered at the command prompt, **DGS-3212SR:4#**.

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


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

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

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


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

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

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

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

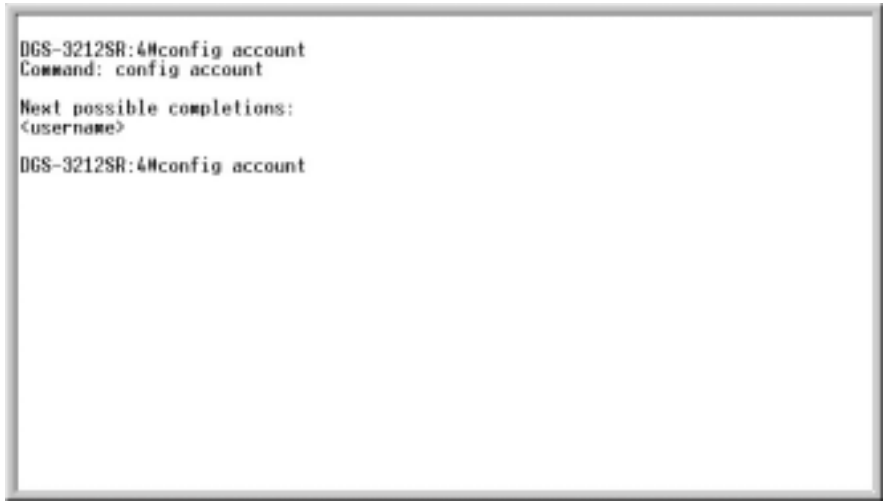


**Figure 2-4. Using the Up Arrow to Re-enter a Command**

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

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

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

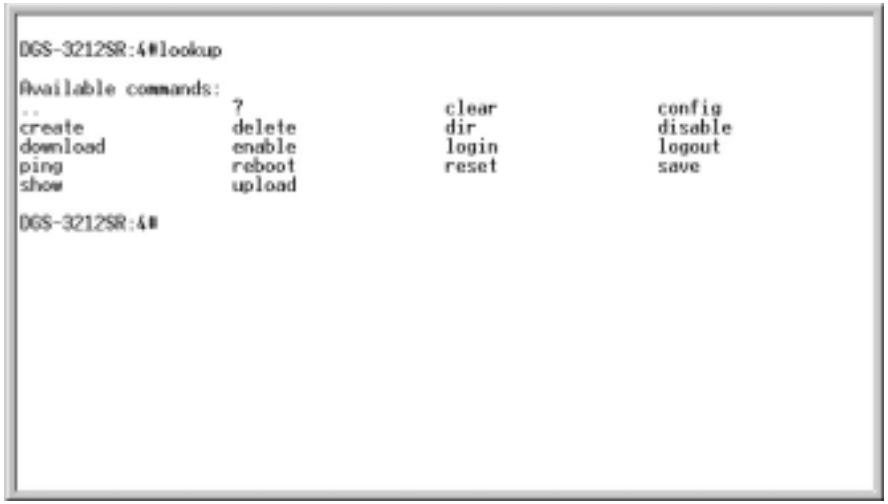


**Figure 2-5. The Next Available Commands Prompt**

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

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

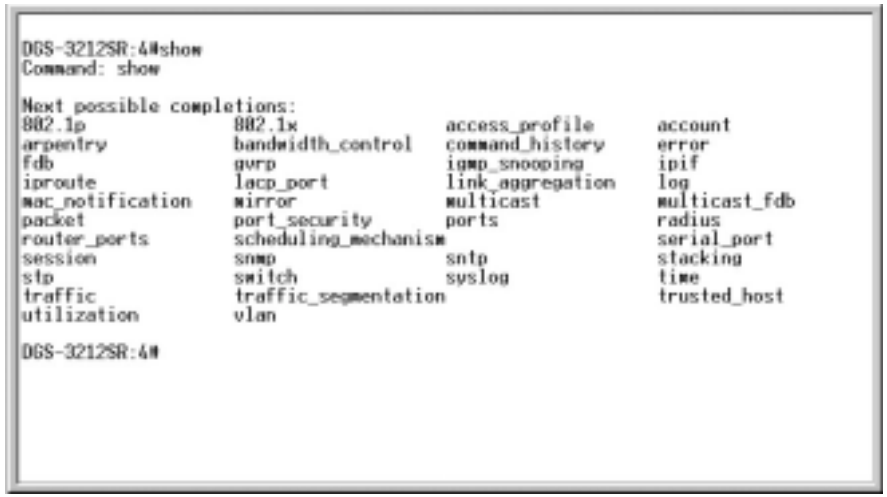


**Figure 2-6. Next possible completions: Show Command**

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

# 3

# COMMAND SYNTAX

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

| <angle brackets> | |
|---|---|
| Purpose | Encloses a variable or value that must be specified. |
| Syntax | **create ipif System ipaddress <network_address>** |
| Description | In the above syntax example, you must type **create ipif System** followed by the network address in the <network_address> space. Do not type the angle brackets. |
| Example Command | create ipif System ipaddress 10.24.22.5/55.0.0.0 |

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

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

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

| Line Editing Key Usage | |
|---|---|
| Delete | Deletes character under the cursor and then shifts the remaining characters in the line to the left. |
| Backspace | Deletes the character to the left of the cursor and shifts the remaining characters in the line to the left**.** |
| Left Arrow | Moves the cursor to the left. |
| Up Arrow | Displays the previous command |
| Down Arrow | Displays the next possible command list, one-by-one. |
| Right Arrow | Moves the cursor to the right. |
| Tab | Shifts the cursor to the next field to the left. |
| Multiple Page Display Control Keys | |
| Space | Displays the next page. |
| CTRL+c | Stops the display of remaining pages when multiple pages are to be displayed. |
| ESC | Stops the display of remaining pages when multiple pages are to be displayed. |
| n | Displays the next page. |
| p | Displays the previous page. |
| q | Stops the display of remaining pages when multiple pages are to be displayed. |
| r | Refreshes the pages currently displaying. |
| a | Displays the remaining pages without pausing between pages. |
| Enter | Displays the next line or table entry. |

4

# BASIC SWITCH COMMANDS

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

| Command | Parameters |
|---|---|
| create account | [admin\|user] <username> |
| config account | <username> |
| show account | |
| show session | |
| show switch | |
| show serial_port | |
| config serial_port | baud_rate [9600\|19200\|38400\|115200] auto_logout [never\|2_minutes\|5_minutes \|10_minutes\|15_minutes] |
| enable clipaging | |
| disable clipaging | |
| enable telnet | <tcp_port_number> |
| disable telnet | |
| enable web | <tcp_port_number> |
| disable web | |
| save | |
| reboot | |
| reset | {config\|system} |
| login | |
| logout | |

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

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

Example Usage:

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

```
DGS-3212SR: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-3212SR:4#
```

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

Example Usage:

To configure the user password of "dlink" account:

```
DGS-3212SR: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-3212SR:4#
```

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

Example Usage:

To display the accounts that have been created:

```
DGS-3212SR:4#show account
Command: show account

 Current Accounts:
   Username         Access Level
 ---------------    ------------
   dlink              Admin
DGS-3212SR:4#
```

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

Example Usage:

To delete the user account “System”:

```
DGS-3212SR:4#delete account System
Command: delete account System

Success.

DGS-3212SR:4#
```

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

Example Usage:

To display the way that the users logged in:

```
DGS-3212SR:4#show session

ID  Login Time              Live Time     From         Level  Name
--  ----------------------  ------------  -----------  -----  ---------
8   0000 days 00:05:54      0:17:16.2     Serial Port  4      Anonymous
```

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

Example Usage:

To display the serial port setting:

```
DGS-3212SR: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-3212SR:4#
```

| show switch | |
|---|---|
| Purpose | Used to display information about the switch. |
| Syntax | **show switch** |
| Description | This command displays information about the switch. |
| Parameters | None. |
| Restrictions | None. |

Example Usage:

To display the switch information:

```
DGS-3212SR:4#show switch
Command: show switch

Device Type         : DGS-3212SR Fast-Ethernet Switch
Module Type         : DES-332GS 1-port GBIC Gigabit Ethernet
and 1 Stacking Port
Unit ID             : 1
MAC Address         : 00-80-C8-12-35-40
IP Address          : 10.1.1.33 (Manual)
VLAN Name           : default
Subnet Mask         : 255.0.0.0
Default Gateway     : 0.0.0.0
Boot PROM Version : Build 1.00.005
Firmware Version    : Build 3.00-B24
Hardware Version    : 1A1
Device S|N          :
System Name         :
System Location     :
System Contact      :
Spanning Tree       : Disabled
GVRP                : Disabled
IGMP Snooping       : Disabled
RIP                 : Disabled
DVMRP               : Disabled
PIM-DM              : Disabled
OSPF                : Disabled
TELNET              : Enable (TCP 23)
WEB                 : Enable (TCP 80)
RMON                : Disabled
DGS-3212SR:4#
```

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

Example Usage:

To display the serial port setting:

```
DGS-3212SR: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-3212SR:4#
```

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

Example Usage:

To configure baud rate:

```
DGS-3212SR:4#config serial_port baud_rate 9600
Command: config serial_port baud_rate 9600

 Success.

DGS-3212SR: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 enable. |
| 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-3212SR:4#enable clipaging
Command: enable clipaging

 Success.

DGS-3212SR:4#
```

| disable clipaging | |
|---|---|
| Purpose | Used to disable the pausing of the console screen scrolling at the end of each page when the show command would display more than one screen of information. |
| Syntax | **disable clipaging** |
| Description | This command is used to disable the pausing of the console screen at the end of each page when the show command would display more than one screen of information. |
| Parameters | None. |
| 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-3212SR:4#disable clipaging
Command: disable clipaging

 Success.

DGS-3212SR:4#
```

| enable telnet | |
|---|---|
| Purpose | Used to enable communication with and management of the switch using the Telnet protocol. |
| Syntax | **enable telnet <tcp_port_number>** |
| Description | This command is used to enable the Telnet protocol on the switch. The user can specify the TCP or UDP port number the switch will use to listen for Telnet requests. |
| Parameters | <tcp_port_number> – The TCP port number. TCP ports are numbered between 1 and 65535. The “well-known” TCP port 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-3212SR:4#enable telnet 23
Command: enable telnet 23

Success.

DGS-3212SR: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-3212SR:4#disable telnet
Command: disable telnet

Success.

DGS-3212SR:4#
```

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

Example Usage:

To enable HTTP and configure port number:

```
DGS-3212SR:4#enable web 80
Command: enable web 80

 Success.

DGS-3212SR: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-3212SR:4#disable web
Command: disable web

Success.

DGS-3212SR:4#
```

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

Example Usage:

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

```
DGS-3212SR:4#save
Command: save

Saving all settings to NV-RAM...   100%
done.
DGS-3212SR:4#
```

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

Example Usage:

To restart the switch:

```
DGS-3212SR:4#reboot
Command: reboot
Are you sure you want to proceed with the system reboot? (y|n)
Please wait, the switch is rebooting...
```

| reset | |
|---|---|
| Purpose | Used to reset the switch to the factory default settings. |
| Syntax | **reset {[config\|system]}** |
| Description | This command is used to restore the switch's configuration to the default settings assigned from the factory. |
| Parameters | config – If config is specified, all of the factory default settings are restored. The switch will not reboot. New user accounts information and IP settings will need to be assigned.<br>system – If system is specified all of the factory default settings are restored on the switch. The switch will reboot. This will clear the dynamic entries in the Forwrding Data Base (FDB). New user accounts information and IP settings will need to be assigned.<br>If no parameter is specified, the switch's current IP address, user accounts, and the switch history log are retained. All other parameters are restored to their factory default settings. The switch will not reboot. |
| Restrictions | Only administrator-level users can issue this command. |

Example Usage:

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

```
DGS-3212SR:4#reset config
Command: reset config

 Success.

DGS-3212SR:4#
```

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

Example Usage:

To initiate the login procedure:

```
DGS-3212SR:4#login
Command: login

UserName:
```

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

Example Usage:

To terminate the current user's console session:

```
DGS-3212SR:4#logout
```

# 5

# SWITCH PORT COMMANDS

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

| Command | Parameters |
|---|---|
| config ports | <portlist\|all><br>speed [auto\|10_half\|10_full\|100_half\|100_full\|<br>1000_half\|1000_full]<br>flow_control [enable\|disable]<br>learning [enable\|disable]<br>state [enable\|disable] |
| show ports | <portlist\|all> |

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

| config ports | |
|---|---|
| Purpose | Used to configure the switch's Ethernet port settings. |
| Syntax | **config ports [<portlist\|all>] {speed[auto\|10_half\|10_full\|100_half\|100_half\|1000_full] learning [enable\|disable] state [enable\|disable]}** |
| Description | This command allows for the configuration of the switch's Ethernet ports. Only the ports listed in the <portlist> will be affected. |
| Parameters | all – Displays all ports on the switch.<br><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.<br>auto – Enables auto-negotiation for the specified range of ports.<br>[10\|100\|1000] – Configures the speed in Mbps for the specified range of ports.<br>[half\|full] – Configures the specified range of ports as either full- or half-duplex.<br>flow_control **[enable\|disable]** - Enables or disables the flow control on the specified range of ports.<br>learning [enable\|disable] – Enables or disables the MAC address learning on the specified range of ports.<br>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 port 3 to be 10 Mbps, full duplex, learning and state enable:

```
DGS-3212SR:4#config ports 1-3 speed 10_full learning on state enable

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

Success.

DGS-3212SR:4#
```

## config port_security

| | |
|---|---|
| Purpose | Used to configure port lock settings. |
| Syntax | config port_security<br><portlist>\|all<br>admin_state [enable\|disaled]<br>max_learning_addr <max_lock_no 0-10><br>lock_address_mode<br>[Permanent\|DeleteOnTimout\|DeleteOnReset] |
| Description | This command allows for the configuration of the port lock security feature. Only the ports listed in the <portlist> are effected. |
| Parameters | all – configure port lock for all ports on the switch.<br>portlist – specifies a range of ports to be configured. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then highest switch number, and the highest port number of the range (also separeted by a colon) are specified. The beginning and end of the port list range are seperated by a dash. For example, 1:3 would specify switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3-2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order.<br>admin_state [enable\|disaled] – enable or disable port lock for the listed ports.<br>max_learning_addr <1-10> - use this to limit the number of MAC addresses dynamically listed in the FDB for the ports.<br>lock_address_mode[Permenent\|DeleteOnTimout\|Delete OnReset] – delete FDB MAC address entries for the ports on timeout of the FDB (see Forwarding Database Commands). Specify DeleteOnReset to delete all FDB entries, including static entries upon system reset or reboot. |
| Restrictions | Only administrator-level users can issue this command. |

Example Usage:

To configure the port lock for ports 1:12 – 1:14 to delete the dynamic address table entries on timeout:

```
DGS-3212SR:4#config port_security ports 12-14
lock_address_mode DeleteOnTimeout

Command: config port_security ports 12-14 lock_address_mode
DeleteOnTimeout


 Success.


DGS-3212SR:4#
```

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

Example Usage:

To display the configuration of the ports:

```
DGS-3212SR:4#show ports
Command: show ports

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

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

## show port_security

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

Example Usage:

To display the port lock configuration:

```
DGS-3212SR:4#show port_security
Command: show port_security
 Port#  Admin State  Max. Learning Addr.  Lock Address Mode
 ----   -----------  --------------------  -----------------
 1      Disabled          1          DeleteOnReset
 2      Disabled          1          DeleteOnReset
 3      Disabled          1          DeleteOnReset
 4      Disabled          1          DeleteOnReset
 5      Disabled          1          DeleteOnReset
 6      Disabled          1          DeleteOnReset
 7      Enabled           10          DeleteOnReset
 8      Disabled          1          DeleteOnReset
 9      Disabled          1          DeleteOnReset
 10     Disabled          1          DeleteOnReset
 11     Disabled          1          DeleteOnReset
 12     Disabled          1          DeleteOnReset
 13     Disabled          1          DeleteOnReset
 14     Disabled          1          DeleteOnReset
 15     Disabled          1          DeleteOnReset
 16     Disabled          1          DeleteOnReset
 17     Disabled          1          DeleteOnReset
 18     Disabled          1          DeleteOnReset
 19     Disabled          1          DeleteOnReset
 20      Disabled          1          DeleteOnReset
CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

6

# SNMP COMMANDS

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

The DGS-3212SR supports the Simple Network Management Protocol (SNMP) versions 1, 2c, and 3. You can specifiy which version of the SNMP you want to use to monitor and control the switch. The three versions of SNMP vary in the level of security provided between the management station and the network device. The following table lists the security features of the three SNMP versions:

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

| Command | Parameters |
|---|---|
| enable rmon | |
| disable rmon | |
| config snmp community | <community_string><br>[readonly\|readwrite] |
| config snmp system_contact | <sw_contact> |
| config snmp system_location | <sw_location> |
| config snmp system_name | <sw_name> |
| enable snmp traps | |
| disable snmp traps | |
| enable snmp authenticate traps | |
| disable snmp authenticate traps | |
| create trusted_host | <ipaddr> |
| show trusted_host | <ipaddr> |
| delete trusted_host | <ipaddr> |
| create snmp user | <username 32> <groupname 32> {encrypted (1) [by_password(1) auth[md5(2) <auth_password |

| Command | Parameters |
|---|---|
| | 8-16 > \| sha(3) <auth_password 8-20 >]<br>priv [none(1) \| des(2) <priv_password 8-16> ]\| by_key(2) auth [md5(2) <auth_key 32-32>\| sha(3) <auth_key 40-40>]<br>priv [none(1) \|des(2) <priv_key 32-32> ]]} |
| delete snmp user | <username 32> |
| show snmp user | |
| show snmp groups | |
| create snmp view | <view_name 32> <oid> view_type [included\|excluded] |
| delete snmp view | <view_name 32> [all \| <oid>] |
| show snmp view | <view_name 32> |
| create snmp community | <community_string 32> view <view_name 32> [read_only\|read_write] |
| delete snmp community | <community_string 32> |
| show snmp community | {<community_string 32>} |
| config snmp engineID | <snmp_engineID> |
| show snmp engineID | |
| create snmp group | <groupname 32> [v1\|v2c\|v3 [noauth_nopriv\|auth_nopriv\|auth_priv]]{read_view <view_name 32> \| write_view <view_name 32> \|notify_view <view_name 32>} |
| delete snmp group | <groupname 32> |


| Command | Parameters |
|---|---|
| delete snmp user | <username 32> |
| show snmp user | |
| show snmp groups | |
| create snmp view | <view_name 32> <oid> view_type [included\|excluded] |
| delete snmp view | <view_name 32> [all \| <oid>] |
| show snmp view | <view_name 32> |
| create snmp community | <community_string 32> view <view_name 32> [read_only\|read_write] |
| delete snmp community | <community_string 32> |
| show snmp community | {<community_string 32>} |
| config snmp engineID | <snmp_engineID> |
| show snmp engineID | |
| create snmp group | <groupname 32> [v1\|v2c\|v3 [noauth_nopriv\|auth_nopriv\|auth_priv]]{read_view <view_name 32> \| write_view <view_name 32> \|notify_view <view_name 32>} |
| delete snmp group | <groupname 32> |

| Command | Parameters |
|---|---|
| create snmp host | <ipaddr> [v1\|v2c\|v3 [noauth_nopriv \| auth_nopriv \| auth_priv]] <auth_string 32> |
| delete snmp host | <ipaddr> |
| show snmp host | {<ipaddr>} |

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

| config snmp community | |
|---|---|
| Purpose | Used to create an SNMP community string. |
| Syntax | config snmp community <community_string> [readonly\|readwrite] |
| Description | This command is used to create an SNMP community string on the switch that will be used to authenticate management stations that want to access the switch using SNMP management software. |
| Parameters | <community_string> – An alpha-numeric string of up to 32 characters that will be used to authenticate management stations that want to access the switch's SNMP agent.<br>readonly – 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.<br>readwrite – 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. |

Example Usage:

To configure an SNMP community "System":

```
DGS-3212SR:4#config snmp community System readwrite
Command: config snmp community System readwrite

Success.

DGS-3212SR:4#
```

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

Example Usage:

To configure the switch name for “DES-3250”:

```
DGS-3212SR:4#config snmp system_name DES3250
Command: config snmp system_name DES3250

Success.

DGS-3212SR:4#
```

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

Example Usage:

To configure the switch location for “Taiwan”:

.

```
DGS-3212SR:4#config snmp system_location Taiwan
Command: config snmp system_location Taiwan

Success.

DGS-3212SR:4#
```

| config snmp system_contact | |
|---|---|
| Purpose | Used to enter the name of a contact person who is responsible for the switch. |
| Syntax | config snmp system_contact <sw_contact> |
| Description | 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 characters 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 “ctsnow”:

.

```
DGS-3212SR:4#config snmp system_contact ctsnow
Command: config snmp system_contact ctsnow

Success.

DGS-3212SR:4#
```

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

Example Usage:

To enable RMON:

```
DGS-3212SR:4#enable rmon
Command: enable rmon

 Success.

DGS-3212SR:4#
```

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

Example Usage:

To disable RMON:

```
DGS-3212SR:4#disable rmon
Command: disable rmon

Success.

DGS-3212SR:4#
```

| create trusted_host | |
|---|---|
| Purpose | Used to create trusted hosts. |
| Syntax | **create trusted_host <ipaddr>** |
| Description | This command is used to create trusted hosts. A trusted host is a recipient of SNMP, Web, and Telnet messages generated by the switch's SNMP agent. |
| Parameters | <ipaddr> – The IP address of the trusted host. |
| Restrictions | Only administrator-level users can issue this command. |

Example Usage:

To create a trusted host:

```
DGS-3212SR:4#create trusted_host
Command: create trusted_host 10.1.1.1

 Success.

DGS-3212SR:4#
```

| show trusted_host | |
|---|---|
| Purpose | Used to display a list of trusted hosts entered on the switch using the create trusted_host command above. |
| Syntax | **show trusted_host** |
| Description | This command is used to display a list of trusted hosts entered on the switch using the create trusted_host command above. |
| Parameters | None. |
| Restrictions | None. |

Example Usage:

To display the list of trusted hosts:

```
DGS-3212SR:4#show trusted_host
Command: show trusted_host

 Management Stations
 IP Address:
-------------------------
10.1.1.1
Total Entries:  1
DGS-3212SR:4#
```

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

Example Usage:

To delete a trusted host with an IP address 10.48.74.121:

```
DGS-3212SR:4#delete trusted_host 10.48.74.121
Command: delete trusted_host 10.48.74.121

Success.

DGS-3212SR:4#
```

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

Example Usage:

To turn on SNMP trap support:

```
DGS-3212SR:4#enable snmp traps
Command: enable snmp traps

Success.

DGS-3212SR:4#
```

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

Example Usage:

To prevent SNMP traps from being sent from the switch:

```
DGS-3212SR:4#disable snmp traps
Command: disable snmp traps

Success.

DGS-3212SR:4#
```

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

Example Usage:

To turn on SNMP authentication trap support:

```
DGS-3212SR:4#enable snmp authenticate traps
Command: enable snmp authenticate traps

Success.

DGS-3212SR:4#
```

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

Example Usage:

To turn off SNMP authentication trap support:

```
DGS-3212SR:4#disable snmp authenticate traps
Command: disable snmp authenticate traps

Success.

DGS-3212SR:4#
```

## create snmp user

| | |
|---|---|
| Purpose | Used to create a new SNMP user and adds the user to an SNMP group that is also created by this command. |
| Syntax | **create snmp user <username 32> <groupname 32> {encrypted (1) [by_password(1) auth[md5(2) <auth_password 8-16 > \| sha(3) <auth_password 8-20 >]priv [none(1) \| des(2) <priv_password 8-16> ]\| by_key(2) auth [md5(2) <auth_key 32-32>\| sha(3) <auth_key 40-40>]priv [none(1) \|des(2) <priv_key 32-32> ]]}** |
| Description | The create snmp user command creates a new SNMP user and adds the user to an SNMP group that is also created by this command. |
| Parameters | <username 32> – An alphanumeric name of up to 32 characters that will identify the new SNMP user.<br>\<groupname 32> – An alphanumeric name of up to 32 characters that will identify the SNMP group the new SNMP user will be associated with.<br>encrypted – Specifies that the password will be in an encrypted format.<br>by_password – Indicate input password for authentication and privacy.<br>by_key – Indicate input key for authentication and privacy.<br>auth – Initiates an authentication level setting session. The options are MD5 and SHA.<br>md5 – The HMAC-MD5-96 authentication level.<br>sha – The HMAC-SHA-96 authentication level.<br><auth_password 8-16> – An alphanumeric sting of between 8 and 20 characters that will be used to authorize the agent to receive packets for the host.<br><priv_password 8-16> – An alphanumeric string of between 8 and 16 characters that will be used to encrypt the contents of messages the host sends to the agent.<br><auth_key> – An authentication key used by MD5 or SHA1, it is hex string type.<br><priv_key> – A privacy key used by DES, it is hex string type. |
| Restrictions | Only administrator-level users can issue this command. |

Example Usage:

To create an SNMP user on the switch:

```
DGS-3212SR:4#create snmp user dlink default encrypted
by_password auth md5 auth_password none

Command: create snmp user dlink default encrypted
by_password auth md5 auth_password none


Success.


DGS-3212SR:4#
```

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

Example Usage:

To delete a previously entered SNMP user on the switch:

```
DGS-3212SR:4#delete snmp user dlink
Command: delete snmp user dlink

Success.

DGS-3212SR:4#
```

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

Example Usage:

To display the SNMP users currently configured on the switch:

```
DGS-3212SR:4#show snmp user
Command: show snmp user

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

Total Entries: 1

DGS-3212SR:4#
```

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

Example Usage:

To display the currently configured SNMP groups on the switch:

```
DGS-3212SR:4#show snmp groups
Command: show snmp groups
Vacm Access Table Settings

Group    Name      : initial
ReadView Name    : restricted
WriteView Name   :
Notify View Name : restricted
Securiy Model    : SNMPv3
Securiy Level    : NoAuthNoPriv

Group    Name      : ReadGroup
ReadView Name    : CommunityView
WriteView Name   :
Notify View Name : CommunityView
Securiy Model    : SNMPv1
Securiy Level    : NoAuthNoPriv
Total Entries: 2
DGS-3212SR:4#
```

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

Example Usage:

To create an SNMP view:

```
DGS-3212SR:4#create snmp view dlinkview 1.3.6 view_type included

Command: create snmp view dlinkview 1.3.6 view_type included


 Success.


DGS-3212SR:4#
```

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

Example Usage:

To delete a previously configured SNMP view from the switch:

```
DGS-3212SR:4#delete snmp view dlinkview
Command: delete snmp view dlinkview

Success.

DGS-3212SR:4#
```

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

Example Usage:

To show SNMP view:

```
DGS-3212SR:4#show snmp view
Command: show snmp view

 Vacm View Table Settings
 View Name         Subtree              View Type
 ----------------- ------------------------ ----------
 ReadView                1              Included
 WriteView               1              Included
 NotifyView            1.3.6            Included
 restricted        1.3.6.1.2.1.1        Included
 restricted        1.3.6.1.2.1.11       Included
 restricted        1.3.6.1.6.3.10.2.1   Included
 restricted        1.3.6.1.6.3.11.2.1   Included
 restricted        1.3.6.1.6.3.15.1.1   Included
 CommunityView           1              Included
 CommunityView       1.3.6.1.6.3        Excluded
 CommunityView       .3.6.1.6.3.1       Included

Total Entries: 11

DGS-3212SR:4#
```

## create snmp community

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

Example Usage:

To create the SNMP community string "dlink:"

```
DGS-3212SR:4#create snmp community dlink view ReadView
read_write

Command: create snmp community dlink view ReadView
read_write


Success.
```

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

Example Usage:

To delete the SNMP community string "dlink:"

```
DGS-3212SR:4#delete snmp community dlink
Command: delete snmp community dlink

Success.

DGS-3212SR:4#
```

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

Example Usage:

To display the currently entered SNMP community strings:

```
DGS-3212SR:4#show snmp community
Command: show snmp community

SNMP Community Table

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

Total Entries: 3
```

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

Example Usage:

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

```
DGS-3212SR:4#config snmp 0035636666
Command: config snmp engineID 0035636666

 Success.

DGS-3212SR:4#
```

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

Example Usage:

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

```
DGS-3212SR:4#show snmp engineID
Command: show snmp engineID

SNMP Engine ID : 0035636666

DGS-3212SR:4#
```

## create snmp group

| | |
|---|---|
| Purpose | Used to create a new SNMP group, or a table that maps SNMP users to SNMP views. |
| Syntax | **create snmp group <groupname 32> [v1\|v2c\|v3 [noauth_nopriv\|auth_nopriv\|auth_priv]] {read_view <view_name 32>\|notify_view <view_name 32>\|notify_view <view_name 32>}** |
| Description | The create snmp group command creates a new SNMP group, or a table that maps SNMP users to SNMP views. |
| Parameters | <groupname 32> – An alphanumeric name of up to 32 characters that will identify the SNMP group the new SNMP user will be associated with.<br>v1 – Specifies that SNMP version 1 will be used. The Simple Network Management Protocol (SNMP), version 1, is a network management protocol that provides a means to monitor and control network devices.<br>v2c – Specifies that SNMP version 2c will be used. The SNMP v2c supports both centralized and distributed network management strategies. It includes improvements in the Structure of Management Information (SMI) and adds some security features.<br>v3 – Specifies that the SNMP version 3 will be used. SNMP v3 adds:<br>Message integrity – ensures that packets have not been tampered with in transit.<br>Authentication – determines that an SNMP message is from a valid source.<br>Encryption – scrambles the contents of messages to prevent it being seen by an unauthorized source.<br>noauth_nopriv – Specifies that there will be no authorization and no encryption of packets sent between the switch and a remote SNMP manager.<br>auth_nopriv – Specifies that authorization will be required, but there will be no encryption of packets sent between the switch and a remote SNMP manager.<br>auth_priv – Specifies that authorization will be required, and that packets sent between the swtich and a remote SNMP manger will be encrypted.<br>read_view – Specifies that the SNMP group being created can request SNMP messages.<br><view_name 32> – An alphanumeric string of up to 32 characters that is used to identify the group of MIB objects that a remote SNMP manager is allowed to access on the switch.<br>notify_view – Specifies that the SNMP group being created can recieve SNMP trap messages generated by the switch's SNMP agent. |
| Restrictions | Only administrator-level users can issue this command. |

Example Usage:

To create an SNMP group named “sg1:”

```
DGS-3212SR:4#create snmp group sg1 v3 noauth_nopriv
read_view v1 write_view v1 no


tify_view v1

Command: create snmp group sg1 v3 noauth_nopriv read_view
v1 write_view v1 notif

y_view v1


 Success.


DGS-3212SR:4#
```

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

Example Usage:

To delete the SNMP group named “sg1”.

```
DGS-3212SR:4#delete snmp group sg1
Command: delete snmp group sg1

 Success.

DGS-3212SR:4#
```

## create snmp host

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

Example Usage:

To create an SNMP host to receive SNMP messages:

```
DGS-3212SR:4#create snmp host 10.48.74.100 v3 auth_priv
public

Command: create snmp host 10.48.74.100 v3 auth_priv public


 Success.


DGS-3212SR:4#
```

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

Example Usage:

To delete an SNMP host entry:

```
DGS-3212SR:4#delete snmp host 10.48.74.100
Command: delete snmp host 10.48.74.100

Success.

DGS-3212SR:4#
```

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

Example Usage:

To display the currently configured SNMP hosts on the switch:

```
DGS-3212SR:4#show snmp host
Command: show snmp host

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

Total Entries: 2
```

7

# DOWNLOAD|UPLOAD COMMANDS

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

| Command | Parameters |
|---|---|
| download | firmware <ipaddr><br><path_filename><br>unit [all\|<unitid>]<br>configuration <ipaddr><br><path_filename><br>{increment} |
| upload | configuration<br>log<br><ipaddr><br><path_filename> |

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

| download | |
|---|---|
| Purpose | Used to download and install new firmware or a switch configuration file from a TFTP server. |
| Syntax | **download [ firmware <ipaddr> <path_filename> {unit [all\|<unitid>]}\|configuration <ipaddr> <path_filename> {increment}]** |
| Description | This command is used to download a new firmware or a switch configuration file from a TFTP server. |
| Parameters | firmware – Download and install new firmware on the switch from a TFTP server.<br>configuration – Download a switch configuration file from a TFTP server.<br><ipaddr> – The IP address of the TFTP server.<br><path_filename> – The DOS path and filename of the firmware or switch configuration file on the TFTP server. For example, C:\3326S.had.<br>unit [all\|<unitid>] – all specifies all units (switches), <unitid> is the unit id of the switch that will receive the download.<br>increment – Allows the download of a partial switch configuration file. This allows a file to be downloaded that will change only the switch parameters explicitly stated in the configuration file. All other switch parameters will remain unchanged. |
| Restrictions | The TFTP server must be on the same IP subnet as the switch. Only administrator-level users can issue this command. |

Example Usage:

```
DGS-3212SR: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-3212SR:4#
```

| upload | |
|---|---|
| Purpose | Used to upload the current switch settings or the switch history log to a TFTP server. |
| Syntax | **upload [configuration\|log] <ipaddr> <path_filename>** |
| Description | This command is used to upload either the switch's current settings or the switch's history log to a TFTP server. |
| Parameters | configuration – Specifies that the switch's current settings will be uploaded to the TFTP server.<br>log – Specifies that the switch history log will be uploaded to the TFTP server.<br><ipaddr> – The IP address of the TFTP server. The TFTP server must be on the same IP subnet as the switch.<br><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:

```
DGS-3212SR: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-3212SR:4#
```

# 8

# NETWORK MONITORING COMMANDS

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

| Command | Parameters |
|---|---|
| show packet ports | <portlist> |
| show error ports | <portlist> |
| show utilitzation | |
| clear counters | ports <portlist> |
| clear log | |
| show log | index <value> |
| enable syslog | |
| disable syslog | |
| show syslog | |
| create syslog host | all<br><index 1-4><br>severity<br>informational<br>warning<br>all<br>facility<br>local0<br>local1<br>local2<br>local3<br>local4<br>local5<br>local6<br>local7<br>udp_port <int><br>ipaddress <ipaddr><br>state [enable\|disable] |
| config syslog host | all<br><index 1-4><br>severity<br>informational<br>warning<br>all<br>facility<br>local0<br>local1<br>local2<br>local3<br>local4<br>local5<br>local6<br>local7<br>udp_port <int><br>ipaddress <ipaddr><br>state [enable\|disable] |
| delete syslog host | <index 1-4><br>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 | s**how packet ports <portlist>** |
| Description | This command is used to display statistics about packets sent and received by ports specified in the port list. |
| Parameters | <portlist> – specifies a range of ports to be configured. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then highest switch number, and the highest port number of the range (also separeted by a colon) are specified. The beginning and end of the port list range are seperated by a dash. For example, **1:3** would specify switch number 1, port 3. **2:4** specifies switch number 2, port 4. **1:3-2:4** specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. |
| Restrictions | None. |

Example Usage:

To display the packets analysis for port 14:

```
DGS-3212SR:4#show packet port 14
Command: show packet ports 14
Port number : 14
 Frame Size    Frame Counts  Frames|sec    Frame Type   Total
Total|sec
 ------------  ------------  ----------    ----------   ---------  ---------
 64            254290        52            RX Bytes     41286744   17290
 65-127        38129         12            RX Frames    359507     86
 128-255       51878         13
 256-511       8058          3             TX Bytes     72755      0
 512-1023      2046          0             TX Frames    335        0
 1024-1518     5441          6

 Unicast RX    2245          0
 Multicast RX  57480         20
 Broadcast RX  299782        66
```

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

Example Usage:

To display the error statistics of the port 3 of module 1:

```
DGS-3212SR:4#show errors port 1:3


RX Frames                       TX Frames
---------------                 ----------------
CRC Error          0            Excessive Deferral      0
Undersize          0            CRC Error               0
Oversize           0            Late Collision          0
Fragment           0            Excessive Collision     0
Jabber             0                    Single Collision
0
Drop Pkts          0            Collision               0
```

## show utilization

| | |
|---|---|
| Purpose | Used to display real-time port utilization statistics. |
| Syntax | **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-3212SR:4#show utilization
Port    TX|sec     RX|sec     Util     Port    TX|sec     RX|sec     Util
----    ---------- ---------- ----     ----    ---------- ---------- ----
1:1          0          0          0    1:22         0          0          0
1:2          0          0          0    1:23         0          0          0
1:3          0          0          0    1:24         0          0          0
1:4          0          0          0    1:25         0          0          0
1:5          0          0          0    1:26        19         49          1
1:6          0          0          0    2:1          0          0          0
1:7          0          0          0    2:2          0          0          0
1:8          0          0          0    2:3          0          0          0
1:9          0          0          0    2:4          0          0          0
1:10         0          0          0    2:5          0          0          0
1:11         0          0          0    2:6          0          0          0
1:12         0          0          0    2:7          0         30          1
1:13         0          0          0    2:8          0          0          0
1:14         0          0          0    2:9         30          0          1
1:15         0          0          0    2:10         0          0          0
1:16         0          0          0    2:11         0          0          0
1:17         0          0          0    2:12         0          0          0
1:18         0          0          0    2:13         0          0          0
1:19         0          0          0    2:14         0          0          0
1:20         0          0          0    2:15         0          0          0
1:21         0          0          0    2:16         0          0          0
```

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

Example Usage:

To clear the counters:

```
DGS-3212SR:4#clear counters ports 2:7-2:9
Command: clear counters ports 2:7-2:9

Success.
```

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

Example Usage:

To clear the log information:

```
DGS-3212SR:4#clear log
Command: clear log

 Success.

DGS-3212SR:4#
```

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

Example Usage:

To display the switch history log**:**

```
DGS-3212SR:4#show log
Index Time      Log Text
----- ---------- ---------------------------------------------------------------
  4   000d00h50m Unit 1, Successful login through Console (Username: Anonymous)
  3   000d00h50m Unit 1, Logout through Console (Username: Anonymous)
  2   000d00h49m Unit 1, Successful login through Console (Username: Anonymous)
  1   000d00h49m Unit 1, Logout through Console (Username: Anonymous)


DGS-3212SR:4#
```

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

Example Usage:

To enable the syslog function on the switch:

```
DGS-3212SR:4#enable syslog
Command: enable syslog

Success.

DGS-3212SR:4#
```

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

Example Usage:

To disable the syslog function on the swtich:

```
DGS-3212SR:4#disable syslog
Command: disable syslog

Success.

DGS-3212SR:4#
```

| show syslog | |
|---|---|
| Purpose | Used to display the syslog protocol status as enable or disable. |
| Syntax | show syslog |
| Description | The **show syslog** command displays the syslog status as enable or disable. |
| Parameters | None. |
| Restrictions | None. |

Example Usage:

To display the current status of the syslog function:

```
DGS-3212SR:4#show syslog
Command: show syslog

 Syslog Global State: Enable

DGS-3212SR:4#
```

## create syslog host

| | |
|---|---|
| Purpose | Used to create a new syslog host. |
| Syntax | create syslog host [all\|<index 1-4>] {severity [informational\|warning\|all]\| facility[local0\|local1\|local2\|local3\| local4\|local5\|local6\|local7]\|udp_port<int>\| ipaddress <ipaddr>\| state[enable\|disable] |
| Description | The **create syslog host** command is used to create a new syslog host. |
| Parameters | all – Specifies that the command will be applied to all hosts.<br>\<index 1-4\> – Specifies that the command will be applied to an index of hosts. There are four available indexes, numbered 1 through 4.<br>severity – Severity level indicator. These are described in the following:<br>Bold font indicates that the corresponding severity level is currently supported on the switch.<br><br>Numerical Code – Severity<br>0 – Emergency: system is unusable<br>1 – Alert: action must be taken immediately<br>2 – Critical: critical conditions<br>3 – Error: error conditions<br>4 – Warning: warning conditions<br>5 – Notice: normal but significant condition<br>6 – Informational: informational messages<br>7 – Debug: debug-level messages |
| Parameters | informational – Specifies that informational messages will be sent to the remote host. This corresponds to number 6 from the list above.<br>warning – Specifies that warning messages will be sent to the remote host. This corresponds to number 4 from the list above.<br>all – Specifies that all of the currently supported syslog messages that are generated by the switch will be sent to the remote host.<br>facility – Some of the operating system daemons and processes have been assigned Facility values. Processes and daemons that have not been explicitly assigned a Facility may use any of the"local use" facilities or they may use the "user-level" Facility. Those Facilities that have been designated are shown in the following: Bold font means the facility values the switch supports now.<br>Numerical Code – Facility<br>0 – kernel messages<br>1 – user-level messages<br>2 – mail system<br>3 – system daemons<br>4 – security\|authorization messages<br>5 – messages generated internally by syslog<br>6 – line printer subsystem<br>7 – network news subsystem<br>8 – UUCP subsystem<br>9 – clock daemon |
| Parameters | 10 – security\|authorization messages<br>11 – FTP daemon<br>12 – NTP subsystem<br>13 – log audit |

| create syslog host | |
|---|---|
| | 14 log alert<br>15 clock daemon<br>16 local use 0 (local0)<br>17 local use 1 (local1)<br>18 local use 2 (local2)<br>19 local use 3 (local3)<br>20 local use 4 (local4)<br>21 local use 5 (local5)<br>22 local use 6 (local6)<br>23 local use 7 (local7)<br>local0 – Specifies that local use 0 messages will be sent to the remote host. This corresponds to number 16 from the list above.<br>local1 – Specifies that local use 1 messages will be sent to the remote host. This corresponds to number 17 from the list above.<br>local2 – Specifies that local use 2 messages will be sent to the remote host. This corresponds to number 18 from the list above.<br>local3 – Specifies that local use 3 messages will be sent to the remote host. This corresponds to number 19 from the list above.<br>local4 – Specifies that local use 4 messages will be sent to the remote host. This corresponds to number 20 from the list above.<br>local5 – Specifies that local use 5 messages will be sent to the remote host. This corresponds to number 21 from the list above.<br>local6 – Specifies that local use 6 messages will be sent to the remote host. This corresponds to number 22 from the list above.<br>local7 – Specifies that local use 7 messages will be sent to the remote host. This corresponds to number 23 from the list above.<br>udp_port <int> – Specifies the UDP port number that the syslog protocol will use to send messages to the remote host. UDP ports available for this purpose are port 514 or any port in the range 6000-65535.<br>ipaddress <ipaddr> – Specifies the IP address of the remote host where syslog messages will be sent.<br>state [enable\|disable] – Allows the sending of syslog messages to the remote host, specified above, to be enabled and disabled. |
| Restrictions | Only administrator-level users can issue this command. |

Example Usage:

To create syslog host:

```
DGS-3212SR:4#create syslog host 1 severity all facility local0
Command: create syslog host 1 severity all facility local0
 Success.
DGS-3212SR:4#
```

## config syslog host

| | |
|---|---|
| Purpose | Used to configure the syslog protocol to send system log data to a remote host. |
| Syntax | config syslog host [all\|<index 1-4>] {severity [informational\|warning\|all]\| facility[local0\|local1\|local2\|local3\| local4\|local5\|local6\|local7]\|udp_port<int>\| ipaddress <ipaddr>\| state[enable\|disable] |
| Description | The **config syslog host** command is used to configure the syslog protocol to send system log information to a remote host. |
| Parameters | all – Specifies that the command will be applied to all hosts.<br><index 1-4> – Specifies that the command will be applied to an index of hosts. There are four available indexes, numbered 1 through 4.<br>severity – Severity level indicator. These are described in the following:<br>Bold font indicates that the corresponding severity level is currently supported on the switch.<br>Numerical Severity<br>Code<br>0 Emergency: system is unusable<br>1 Alert: action must be taken immediately<br>2 Critical: critical conditions<br>3 Error: error conditions<br>4 Warning: warning conditions<br>5 Notice: normal but significant condition<br>6 Informational: informational messages<br>7 Debug: debug-level messages |
| Parameters | informational – Specifies that informational messages will be sent to the remote host. This corresponds to number 6 from the list above.<br>warning – Specifies that warning messages will be sent to the remote host. This corresponds to number 4 from the list above.<br>all – Specifies that all of the currently supported syslog messages that are generated by the switch will be sent to the remote host.<br>facility – Some of the operating system daemons and processes have been assigned Facility values. Processes and daemons that have not been explicitly assigned a Facility may use any of the"local use" facilities or they may use the "user-level" Facility. Those Facilities that have been designated are shown in the following: Bold font means the facility values the switch supports now.<br>Numerical Facility<br>Code<br>0 kernel messages<br>1 user-level messages<br>2 mail system<br>3 system daemons<br>4 security\|authorization messages<br>5 messages generated internally by syslog<br>6 line printer subsystem<br>7 network news subsystem<br>8 UUCP subsystem<br>9 clock daemon |

## config syslog host

| | | |
|---|---|---|
| Parameters | 10 | security\|authorization messages |
| | 11 | FTP daemon |
| | 12 | NTP subsystem |
| | 13 | log audit |
| | 14 | log alert |
| | 15 | clock daemon |
| | 16 | local use 0 (local0) |
| | 17 | local use 1 (local1) |
| | 18 | local use 2 (local2) |
| | 19 | local use 3 (local3) |
| | 20 | local use 4 (local4) |
| | 21 | local use 5 (local5) |
| | 22 | local use 6 (local6) |
| | 23 | local use 7 (local7) |
| | local0 – Specifies that local use 0 messages will be sent to the remote host. This corresponds to number 16 from the list above. | |
| | local1 – Specifies that local use 1 messages will be sent to the remote host. This corresponds to number 17 from the list above. | |
| | local2 – Specifies that local use 2 messages will be sent to the remote host. This corresponds to number 18 from the list above. | |
| | local3 – Specifies that local use 3 messages will be sent to the remote host. This corresponds to number 19 from the list above. | |
| | local4 – Specifies that local use 4 messages will be sent to the remote host. This corresponds to number 20 from the list above. | |
| | local5 – Specifies that local use 5 messages will be sent to the remote host. This corresponds to number 21 from the list above. | |
| | local6 – Specifies that local use 6 messages will be sent to the remote host. This corresponds to number 22 from the list above. | |
| | local7 – Specifies that local use 7 messages will be sent to the remote host. This corresponds to number 23 from the list above. | |
| | udp_port <int> – Specifies the UDP port number that the syslog protocol will use to send messages to the remote host. UDP ports available for this purpose are port 514 or any port in the range 6000-65535. | |
| | ipaddress <ipaddr> – Specifies the IP address of the remote host where syslog messages will be sent. | |
| | state [enable\|disable] – Allows the sending of syslog messages to the remote host, specified above, to be enabled and disabled. | |
| Restrictions | Only administrator-level users can issue this command. | |

Example Usage:

To create syslog host:

```
DGS-3212SR:4#config syslog host all severity all facility local0
Command: config syslog host all severity all facility local0
 Success.
DGS-3212SR:4#
```

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

Example Usage:

To delete a previously configured syslog host:

```
DGS-3212SR:4#delete syslog host 4
Command: delete syslog host 4

Success.

DGS-3212SR:4#
```

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

Example Usage:

To show Syslog host information:

```
DGS-3212SR:4#show syslog host
Command: show syslog host
 Syslog Global State: Disabled
 Host Id  Host IP Address  Severiry   Facility UDP port   Status
 -------  ---------------  ---------- -------- --------  --------
 1        10.1.1.2         All        Local0   514       Disabled
 2        10.40.2.3        All        Local0   514       Disabled
 3        10.21.13.1       All        Local0   514       Disabled

 Total Entries : 3

DGS-3212SR:4#
```

9

# MAC NOTIFICATION

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

| Command | Parameters |
|---|---|
| config mac_notification | interval <int 1-214783647><br>historysize <int 1-500> |
| config mac_notification ports | <portlist><br>all<br>enable<br>disable |
| enable mac_notification | |
| disable mac_notification | |
| show mac_notification | |
| show mac_notification ports | <portlist> |

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

| config mac_notification | |
|---|---|
| Purpose | Used to configure MAC address notification. |
| Syntax | **config mac_notification**<br>**ports <portlist>\|all**<br>**interval <sec>**<br>**historysize <1 - 500>** |
| Description | MAC address notificiation is used to monitor MAC addresses learned and entered into the FDB. |
| Parameters | **ports <portlist> -** specifies a range of ports to be configured. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then highest switch number, and the highest port number of the range (also separeted by a colon) are specified. The beginning and end of the port list range are seperated by a dash. For example, **1:3** would specify switch number 1, port 3. **2:4** specifies switch number 2, port 4. **1:3-2:4** specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order.<br>all – to configure all ports for MAC notification.<br>interval <sec 1-2147483647> - time in seconds between notifications.<br>historysize <1 - 500> - maximum number of entries listed in the history log used for notification. |
| Restrictions | Only administrator-level users can issue this command. |

Example Usage:

To configure a 60 second interval for MAC address notification on unit 1 ports 6-9:

```
DGS-3212SR:4#config mac_notification ports 1:6-1:9 60
Command: config mac_notification ports 1:6-1:9 interval 60

Success.

DGS-3212SR:4#
```

| config mac_notification ports | |
|---|---|
| Purpose | Used to configure MAC address notification on a port basis. |
| Syntax | **config mac_notification ports**<br>**ports <portlist>\|all**<br>**enable**<br>**disable** |
| Description | MAC address notificiation is used to monitor MAC addresses learned and entered into the FDB. |
| Parameters | **ports <portlist> - S**pecifies a range of ports to be configured. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then highest switch number, and the highest port number of the range (also separeted by a colon) are specified. The beginning and end of the port list range are seperated by a dash. For example, **1:3** would specify switch number 1, port 3. **2:4** specifies switch number 2, port 4. **1:3-2:4** specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order.<br>all – To configure all ports for MAC notification.<br>enable – Used to enable a port's MAC notification<br>disable – Used to disable a port's MAC notification. |
| Restrictions | Only administrator-level users can issue this command. |

Example Usage:

To configure MAC address notification on unit 1 ports 6-9:

```
DGS-3212SR:4#config mac_notification ports 1:6-1:9
Command: config mac_notification ports 1:6-1:9
 Success.

DGS-3212SR:4#
```

| enable mac_notification | |
|---|---|
| Purpose | Used to globally enable MAC address notification without changing the mac_notification configuration. |
| Syntax | **enable mac_notification** |
| Description | Enables MAC notication on the switch. |
| Parameters | None. |
| Restrictions | Only administrator-level users can issue this command. |

Example Usage:

To globally enable MAC notification:

```
DGS-3212SR:4#enable mac_notification
Command: enable mac_notification

Success.

DGS-3212SR:4#
```

| disable mac_notification | |
|---|---|
| Purpose | Used to disable MAC address notification globally without changing mac_notification configuration.. |
| Syntax | **disable mac_notification** |
| Description | Disables MAC notication on the switch. |
| Parameters | None. |
| Restrictions | Only administrator-level users can issue this command. |

Example Usage:

To globally disnable MAC notification:

```
DGS-3212SR:4#disable mac_notification
Command: disable mac_notification

 Success.

DGS-3212SR:4#
```

| show mac_notification | |
|---|---|
| Purpose | Used to display MAC address notification. |
| Syntax | **show mac_notification {ports}** |
| Description | Displays MAC notification settings either per port or globally as desired. |
| Parameters | None – this will display global MAC notification settings currently configured including Interval, History Size and State.<br>ports – this displays per ports MAC notification settings. |
| Restrictions | Only administrator-level users can issue this command. |

Example usage:

To display global MAC notification settings:

```
DGS-3212SR:4#show mac_notification
Command: show mac_notification

 Global Mac Notification Settings

     State       : Disabled
     Interval    : 1
     History Size : 1

DGS-3212SR:4#
```

| show mac_notification ports | |
|---|---|
| Purpose | Used to display MAC address notification. |
| Syntax | **show mac_notification ports** |
| Description | Displays MAC notification settings either per port or globally as desired. |
| Parameters | ports – this displays per ports MAC notification settings. |
| Restrictions | Only administrator-level users can issue this command. |

Example Usage:

To display per port MAC notification settings:

```
DGS-3212SR:4#show mac_notification ports
Command: show mac_notification ports

Port #  MAC Address Table Notification State
------  ------------------------------------
1               Enabled
2               Disabled
3               Disabled
4               Disabled
5               Disabled
6               Disabled
7               Disabled
8               Disabled
9               Disabled
10              Disabled
11              Disabled
12              Disabled
13              Disabled
14              Disabled
15              Disabled
16              Disabled
17              Disabled
18              Disabled
19              Disabled
20              Disabled
CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

10

# SPANNING TREE COMMANDS

The switch supports 802.1d STP and 802.1w Rapid STP. The spanning tree commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

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

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

| config stp | |
|---|---|
| Purpose | Used to setup STP and RSTP on the switch. |
| Syntax | **config stp {maxage <value 6-40> \|hellotime <value 1-10> \|forwarddelay <value 4-30>\|priority <value 0-61440> \|fbpdu [enable\|disable]\| txholdcount <value 1-10>\| version[rstp\|stp]}** |
| Description | This command is used to setup the Spanning Tree Protocol (STP) for the entire switch. |
| Parameters | maxage <value 6-40> – The maximum amount of time (in seconds) that the switch will wait to receive a BPDU packet before reconfiguring STP. The default is 20 seconds.<br>hellotime <value 1-10> – The time interval between transmission of configuration messages by the root device. The default is 2 seconds.<br>forwarddelay <value 4-30> – The maximum amount of time (in seconds) that the root device will wait before changing states. The default is 15 seconds.<br>priority <value 0-61440> – A numerical value between 0 and 61440 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.<br>fbpdu [**enable**\|**disable**] – Allows the forwarding of STP BPDU packets from other network devices when STP is disabled on the switch. The default is enabled.<br>txholdcount <value 1-10> – the maximum number of Hello packets transmitted per interval. Default value = 3.<br>version [rstp\|stp] – select the Spanning Tree Protocol version used for the switch. For IEEE 802.1d STP select stp. Select rstp for IEEE 802.1w Rapid STP. |
| Restrictions | Only administrator-level users can issue this command. |

Example Usage:

To configure STP with maxage 18 and hellotime 4:

```
DGS-3212SR:4#config stp maxage 18 hellotime 4
Command: config stp maxage 18 hellotime 4

Success.

DGS-3212SR:4#
```

## config stp ports

| | |
|---|---|
| Purpose | Used to setup STP on the port level. |
| Syntax | **config stp ports <portlist> {cost [auto\|<value 1-200000000>]\|priority <value 0-240>\| migrate [yes\|no]\| edge [true\|false]\| p2p [true\|false\|auto]\| state [enable\|disable]** |
| Description | This command is used to create and configure STP for a group of ports. |
| Parameters | Cost <value 1-200000000> – This defines a metric that indicates the relative cost of forwarding packets to the specified port list. Port cost can be set from 1 to 200000000. The lower the number, the greater the probability the port will be chosen to forward packets.<br>Default port cost: 100Mbps port = 200000<br>Gigabit port = 20000<br>priority <value 0-240> – Port Priority can be from 0 to 240. The lower the number, the greater the probability the port will be chosen as the Root Port. Default = 128.<br><portlist> – Specifies a range of ports to be configured. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 3 would specify port 3. 4 specifies port 4. 3-4 specifies all of the ports between port 3 and port 4 – in numerical order.<br>migrate [yes\|no] – yes will enable the port to migrate from 802.1d STP status to 802.1w RSTP status. RSTP can coexist with standard STP, however the benefits of RSTP are not realized on a port where an 802.1d network connects to an 802.1w enabled network. Migration should be enabled (yes) on ports connected to network stations or segments that will be upgraded to 802.1w RSTP on all or some portion of the segment.<br>edge [true\|false] – true designates the port as an edge port. Edge ports cannot create loops, however an edge port can lose edge port status if a topology change creates a potential for a loop. An edge port normally should not receive BPDU packets. If a BPDU packet is received, it automatically loses edge port status. False indicates the port does not have edge port status.<br>p2p [true\|false\|auto] – true indicates a point-to-point (p2p) shared link. These are similar to edge ports, however they are restricted in that a p2p port must operate in full duplex. Like edge ports, p2p ports transition to a forwarding state rapidly thus benefiting from RSTP.<br>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 configure STP with path cost 19, priority 15, and state enabled for ports 1-5.

```
DGS-3212SR:4#config stp_ports 1-5 cost 19 priority 15 state
enable

Command: config stp_ports 1-5 cost 19 priority 15 state enable


 Success.


DGS-3212SR:4#
```

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

Example Usage:

To enable STP, globally, on the switch:

```
DGS-3212SR:4#enable stp
Command: enable stp

 Success.

DGS-3212SR:4#
```

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

Example Usage:

To disable STP on the switch:

```
DGS-3212SR:4#disable stp
Command: disable stp

Success.

DGS-3212SR:4#
```

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

Example Usage:

To display the status of STP on the switch:

Status 1: STP Enabled

```
DGS-3212SR:4#show stp
Command: show stp

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


Designated Root Bridge: 00-80-00-00-01-02
Root Priority           : 32767
Cost to Root            : 200015
Root Port               : 2
Last Topology Change    : 77sec
Topology Changes Count: 198
Protocol Specification  : 3
Max Age                 : 20
```

```
Hello Time                  : 2
Forward Delay               : 15
Hold Time                   : 3
```

Status 2: STP Disabled

```
DGS-3212SR:4#show stp
Command: show stp

STP Status              : Disabled
Max Age                 : 20
Hello Time              : 2
Forward Delay           : 15
Priority                : 32768
STP Version             : RSTP
TX Hold Count           : 3
Forwarding BPDU         : Enabled

DGS-3212SR:4#
```

## show stp ports

| | |
|---|---|
| Purpose | Used to display the switch's current per-port group STP configuration. |
| Syntax | **show stp ports <portlist>** |
| Description | This command displays the switch's current per-port group STP configuration. |
| Parameters | <portlist> – Specifies a range of ports to be configured. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 3 would specify port 3. 4 specifies switch number 2, 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 STP state of ports 1-9:

```
DGS-3212SR:4#show stp ports 1-9
Command: show stp ports 1-9

Port   Designated Bridge        State  Cost      Pri  Edge  P2P  Status      Role
------ ------------------------ -------- ---------- ----- ------ ----- --------- ------------
1      8000|000104031001        Yes  *200000   128  No    Yes  Forwarding  Designated
2      N|A                      Yes  *200000   128  No    Yes  Disabled    Disabled
3      N|A                      Yes  *200000   128  No    Yes  Disabled    Disabled
4      N|A                      Yes  *200000   128  No    Yes  Disabled    Disabled
5      N|A                      Yes  *200000   128  No    Yes  Disabled    Disabled
6      N|A                      Yes  *200000   128  No    Yes  Disabled    Disabled
7      8000|000102030400        Yes   *200000  128  No    Yes  Forwarding  Root
8      N|A                      Yes  *200000   128  No    Yes  Disabled    Disabled
9      N|A                      Yes  *200000   128  No    Yes  Disabled    Disabled
DGS-3212SR:4#
```

# 11

# FORWARDING DATABASE COMMANDS

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

| Command | Parameters |
|---|---|
| create fdb | <vlan_name><br><macaddr><br>port <port> |
| create multicast_fdb | <vlan_name><br><macaddr> |
| config multicast_fdb | <vlan_name><br><macaddr> [add\|delete]<br><portlist> |
| config fdb aging_time | <sec 10-1000000> |
| config multicast port_filtering_mode | [<portlist>\|all]<br>[forward_all_groups\|forward_unregistered_groups<br>\|<br>filter_unregistered groups] |
| delete fdb | <vlan_name 32><br><macaddr> |
| clear fdb | vlan <vlan_name 32><br>port <port>\|all |
| show multicast_fdb | vlan <vlan_name 32><br>mac_address <macaddr> |
| show fdb | port <port><br>vlan <vlan_name 32> |
| | mac_address <macaddr><br>static<br>aging_time |

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

| create fdb | |
|---|---|
| Purpose | Used to create a static entry to the unicast MAC address forwarding table (database) |
| Syntax | **create fdb <vlan_name32> <macaddr> [port <port>]** |
| Description | This command will make an entry into the switch's unicast MAC address forwarding database. |
| Parameters | <vlan_name 32> – The name of the VLAN on which the MAC address resides.<br><macaddr> – The MAC address that will be added to the forwarding table.<br><port> – The port number corresponding to the MAC destination address. The switch will always forward traffic to the specified device through this port. |
| Restrictions | Only administrator-level users can issue this command. |

Example Usage:

To create an unicast MAC forwarding:

```
local>create fdb default 00-00-00-00-01-02 port 5
Command: create fdb default 00-00-00-00-01-02 port 5

Success.
```

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

Example Usage:

To create multicast MAC forwarding:

```
local>create multicast_fdb default 01-00-5E-00-00-00
Command: create multicast_fdb default 01-00-5E-00-00-00

Success.

local>
```

| config multicast_fdb | |
|---|---|
| Purpose | Used to configure the switch's multicast MAC address forwarding database. |
| Syntax | **config multicast_fdb <vlan_name 32> <macaddr> [add\|delete] [egress\|forbidden] <portlist>** |
| Description | This command configures the multicast MAC address forwarding table. |
| Parameters | <vlan_name 32> – The name of the VLAN on which the MAC address resides.<br><br><macaddr> – The MAC address that will be added to the forwarding table.<br><br>[add\|delete] – Add will add the MAC address to the forwarding table, delete will remove the MAC address from the forwarding table.<br><br>[egress\|forbidden] – Egress specifies the port as being a source of multicast packets originating from the MAC address specified above, forbidden specifies the port as not being a member of the VLAN and that the port is forbidden from becoming a member of the VLAN dynamically.<br><br><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:

```
local>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.

local>
```

| delete fdb | |
|---|---|
| Purpose | Used to delete an entry to the switch's forwarding database. |
| Syntax | **delete fdb <vlan_name 32> <macaddr>** |
| Description | This command is used to delete a previous entry to the switch's MAC address forwarding database. |
| Parameters | <vlan_name 32> – The name of the VLAN on which the MAC address resides.<br><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:

```
local>delete fdb default 00-00-00-00-01-02
Command: delete fdb default 00-00-00-00-01-02

Success.

local>
```

| clear fdb | |
|---|---|
| Purpose | Used to clear the switch's forwarding database of all dynamically learned MAC addresses. |
| Syntax | **clear fdb [vlan <vlan_name 32>\|port <port>\|all]** |
| Description | This command is used to clear dynamically learned entries to the switch's forwarding database. |
| Parameters | <vlan_name 32> – The name of the VLAN on which the MAC address resides.<br><br><port> – The port number corresponding to the MAC destination address. The switch will always forward traffic to the specified device through this port.<br><br>all – Clears all dynamic entries to the switch's forwarding database. |
| Restrictions | Only administrator-level users can issue this command. |

Example Usage:

To clear all FDB dynamic entries:

```
local>clear fdb all
Command: clear fdb all

 Success.

local>
```

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

Example Usage:

To display multicast MAC address table:

```
local>show multicast_fdb
Command: show multicast_fdb

 VLAN Name       : default
 MAC Address     : 01-00-5E-00-00-00
 Egress Ports    : 1-5, 26
 Mode            : Static

 Total Entries   : 1

local>
```

| config fdb aging_time | |
|---|---|
| Purpose | Used to set the aging time of the forwarding database. |
| Syntax | **config fdb aging_time <sec>** |
| Description | The aging time affects the learning process of the switch. Dynamic forwarding table entries, which are made up of the source MAC addresses and their associated port numbers, are deleted from the table if they are not accessed within the aging time. The aging time can be from 10 to 1,000,000 seconds with a default value of 300 seconds. A very long aging time can result in dynamic forwarding table entries that are out-of-date or no longer exist. This may cause incorrect packet forwarding decisions by the switch. If the aging time is too short however, many entries may be aged out too soon. This will result in a high percentage of received packets whose source addresses cannot be found in the forwarding table, in which case the switch will broadcast the packet to all ports, negating many of the benefits of having a switch. |
| Parameters | <sec> – The aging time for the MAC address forwarding database value. |
| Restrictions | Only administrator-level users can issue this command. |

Example Usage:

To set the fdb aging time:

```
Local>config fdb aging_time 25
Command: config fdb aging_time 25

 Success.

local>
```

## config multicast port_filtering_mode

| | |
|---|---|
| Purpose | Used to configure the multicast packet filtering mode for ports. |
| Syntax | **config multicast port_filtering_mode [<portlist>\|all] [forward_all_groups\|**<br>**forward_unregistered_groups\|**<br>**filter_unregistered_groups]** |
| Description | The config multicast port_filtering_mode command configures the multicast packet filtering mode for 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.<br>all – Specifies all of the ports on the switch.<br>forward_all_groups – Specifies that all multicast packets will be forwarded to all multicast groups.<br>forward_unregistered_groups – Specifies that multicast packets will be forwarded to unregistered multicast groups.<br>filter_unregistered_groups – Specifies that multicast packets with unregistered multicast groups as a destination will be dropped. |
| Restrictions | You must have administrator privledges. |

Example Usage:

To configure the mulitcast packet filtering mode for ports:

```
Local>config multicast port_filtering_mode 15:1-15:4
forward_all_groups

Command: config multicast port_filtering_mode 15:1-15:4
forward_all_groups


 Success.


local>
```

| show fdb | |
|---|---|
| Purpose | Used to display the current unicast MAC address forwarding database. |
| Syntax | **show fdb {port <port>\|vlan <vlan_name 32>\|mac_address <macaddr>\|static\|aging_time}** |
| Description | This command will display the current contents of the switch's forwarding database. |
| Parameters | <port> – The port number corresponding to the MAC destination address. The switch will always forward traffic to the specified device through this port.<br>\<vlan_name 32> – The name of the VLAN on which the MAC address resides.<br><macaddr> – The MAC address that will be added to the forwarding table.<br>static – Displays the static MAC address entries.<br>aging_time – Displays the aging time for the MAC address forwarding database. |
| Restrictions | None. |

Example Usage:

To display unicast MAC address table:

```
local>show fdb
Command: show fdb

Unicast MAC Address Ageing Time  = 300

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

Total Entries = 3

local>
```

12

# BROADCAST STORM CONTROL COMMANDS

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

| Command | Parameters |
|---|---|
| config traffic control | <storm_grouplist><br>all<br>broadcast [enable\|disable]<br>multicast [enable\|disable]<br>dlf [enable\|disable]<br>threshold <value> |
| show traffic control | group_list <storm_grouplist> |

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

## config traffic control

| | |
|---|---|
| Purpose | Used to configure broadcast\|multicast traffic control. |
| Syntax | **config traffic control [<storm_grouplist>\|all] broadcast [enable\|disable]\|multicast [enable\|disable]\|dlf [enable\|disable]\|threshold <value>** |
| Description | This command is used to configure broadcast storm control. |
| Parameters | <storm_grouplist> – Used to specify a broadcast storm control group with the syntax: module_id:group_id.<br>all – Specifies all broadcast storm control groups on the switch.<br>broadcast [enable\|disable] – Enables or disables broadcast storm control.<br>multicast [enable\|disable] – Enables or disables multicast storm control.<br>dlf [enable\|disable] – Enables or disables dlf traffic control.<br>threshold <value> – The upper threshold at which the specified traffic control is switched on. The <value> is the number of broadcast\|multicast\|dlf packets, in packets per second, received by the switch that will trigger the storm traffic control measures. |
| Restrictions | Only administrator-level users can issue this command. |

Example Usage:

To configure traffic control:

```
DGS-3212SR:4#config traffic control 1-3,1-2 broadcast enable
Command: config traffic control 1-1,2-2 broadcast enable

Success.

DGS-3212SR:4#
```

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

Example Usage:

To display traffic control setting:

```
DGS-3212SR:4#show traffic control
Command: show traffic control


Traffic Control

                                  Broadcast Multicast Destination
Module Group [ports] Threshold Storm     Storm     Lookup Fail
------ ------------- --------- --------- --------- -----------
1      1 [ 1 - 8 ]   128       Disabled  Disabled  Disabled
1      2 [ 9 - 16]   128       Disabled  Disabled  Disabled
1      3 [17 - 24]   128       Disabled  Disabled  Disabled
1      4 [  25   ]   128       Disabled  Disabled  Disabled
1      5 [  26   ]   128       Disabled  Disabled  Disabled

Total Entries: 5


DGS-3212SR:4#
```

13

# QOS COMMANDS

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

| Command | Parameters |
|---|---|
| config bandwidth_control | <portlist><br>rx_rate<br>no_limit<br><value 1-1000><br>tx_rate<br>no_limit<br><value 1-1000> |
| show bandwidth_control | <portlist> |
| config scheduling_mechanism | strict<br>round_robin |
| show scheduling | |
| config 802.1p user_priority | <priority 0-7><br><class_id 0-3> |
| show 802.1p user_priority | |
| config 802.1p default_priority | <portlist><br>all<br><priority 0-7> |
| show 802.1p default_priority | <portlist> |

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

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

| config bandwidth_control | |
|---|---|
| Parameters | <value 1-1000> – Specifies the limit, in Mbps, that the above ports will be allowed to receive packets.<br><br>tx_rate – Specifies that one of the parameters below (**no_limit** or **<value 1-1000>**) will be applied to the rate at which the above specified ports will be allowed to transmit packets.<br><br>no_limit – Specifies that there will be no limit on the rate of packets received by the above specified ports.<br><br><value 1-1000> – Specifies the limit, in Mbps, that the above ports will be allowed to receive packets. Gigabit ports must be configured to using a limit value that is a multiplt of 8 i.e. for Gigabit ports <value 8-1000 in increments of 8>. |
| Restrictions | Only administrator-level users can issue this command. |

Example Usage:

To configure bandwitdth control:

```
DGS-3212SR:4#config bandwidth_control 1-10 tx_rate 10
Command: config bandwidth_control 1-10 tx_rate 10

Success.

DGS-3212SR:4#
```

| show bandwidth_control | |
|---|---|
| Purpose | Used to display the bandwidth control configuration on the switch. |
| Syntax | **show bandwidth_control {<portlist>}** |
| Description | The **show bandwidth_control** command displays the current bandwidth control configuration on the switch, on a port-by-port basis. |
| Parameters | <portlist> – Specifies a range of ports to be configured. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, **1:3** would specify switch number 1, port 3. **2:4** specifies switch number 2, port 4. **1:3-2:4** specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. |
| Restrictions | None. |

Example Usage:

To display bandwidth control settings:

```
DGS-3212SR:4#show bandwidth_control  1-10
Command: show bandwidth_control 1-10

Bandwidth Control Table

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

DGS-3212SR:4#
```

| config scheduling_mechanism | |
|---|---|
| Purpose | Used to configure the traffic sheduling mechanism for each COS queue. |
| Syntax | **config scheduling_mechanism [strict\|round_robin]** |
| Description | The switch contains 8 hardware priority queues. Incoming packets must be mapped to one of these eight queues. This command is used to specify the rotation by which these eight hardware priority queues are emptied. The switch's default is to empty the 8 hareware priority queues in order – from the highest priority queue (hardware queue 7) to the lowest priority queue (hardware queue 0). Each hardware queue will transmit all of the packets in its buffer before allowing the next lower priority queue to transmit its packets. When the lowest hardware priority queue has finished transmitting all of its packets, the highest hardware priority queue can again transmit any packets it may have received. |
| Parameters | strict – The highest priority queue is processed first, until its buffer is empty.<br>round_robin – a round-robin schedule is used to process packets. |
| Restrictions | You must have administator privileges. |

Example Usage:

To configure traffic scheduling mechanism to be strict:

```
DGS-3212SR:4# config scheduling_mechanism strict
Command: config scheduling_mechanism strict

 Success.

DGS-3212SR:4#
```

| show scheduling | |
|---|---|
| Purpose | Used to display the currently configured traffic scheduling on the switch. |
| Syntax | **show scheduling** |
| Description | The **show scheduling** command displays the current configuration for the maximum number of packets (**max_packets**) and the maximum latency (**max_latency**) values assigned to the four priority queues on the switch. The switch's default max_latency = 0. At this value it will empty the four hardware queues in order, from the highest priority (queue 0) to the lowest priority (queue 3). |
| Parameters | None. |
| Restrictions | None. |

Example Usage:

To display the current scheduling configuration:

```
DGS-3212SR:4# show scheduling
Command: show scheduling


QOS Output Scheduling

      MAX. Packets  MAX. Latency
      ------------  ------------
Class-0    50            1
Class-1    100           1
Class-2    150           1
Class-3    200           1

DGS-3212SR:4#
```

## config 802.1p user_priority

| | |
|---|---|
| Purpose | Used to map the 802.1p user priority of an incoming packet to one of the four hadware queues available on the switch. |
| Syntax | config 802.1p user_priority <priority 0-7> <class_id 0-3> |
| Description | The **config 802.1p user_priority** command is used to configure the way the switch will map an incoming packet, based on its 802.1p user priority tag, to one of the four hardware priority queues available on the switch. The switch's default is to map the incoming 802.1p priority values to the four hardware queues according to the following chart:<br>802.1p Value — Switch Priority Queue — Remark<br>--- — --- — ---<br>1 — 0<br>0 — 0<br>1 — 1<br>2 — 2<br>2 — 3<br>3 — 3 |
| Parameters | <priority 0-7> – Specifies which of the 8 802.1p priority values (0 through 7) you want to map to one of the switch's hardware priority queues (<class_id>, 0 through 3).<br><class_id 0-3> – Specifies which of the switch's hardware priority queues the 802.1p priority value (specified above) will be mapped to. |
| Restrictions | Only administrator-level users can issue this command. |

Example Usage:

To configure 802.1 user priority on the switch:

```
DGS-3212SR:4# config 802.1p user_priority 1 3
Command: config 802.1p user_priority 1 3

 Sucess.

DGS-3212SR:4#
```

| show 802.1p user_priority | |
|---|---|
| Purpose | Used to display the current mapping between an incoming packet's 802.1p priority value and one of the switch's four hardware priority queues. |
| Syntax | show 802.1p user_priority |
| Description | The **show 802.1p user_priority** command displays the current mapping of an incoming packet's 802.1p priority value to one of the switch's four hardware priority queues. |
| Parameters | None. |
| Restrictions | None. |

Example Usage:

To show 802.1p user priority:

```
DGS-3212SR:4# show 802.1p user_priority
Command: show 802.1p user_priority

COS Class of Traffic

Priority-0  ->  <Class-1>
Priority-1  ->  <Class-0>
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-3212SR:4#
```

## config 802.1p default_priority

| | |
|---|---|
| Purpose | Used to specify how to map an incoming packet that has no 802.1p priority tag to one of the switch's four hardware priority queues. |
| Syntax | **config 802.1p default_priority [<portlist>\|all] <priority 0-7>** |
| Description | The **config 802.1p default_priority** command allows you to specify the 802.1p priority value an untagged, incoming packet will be assigned before being forwarded to its destination. |
| Parameters | <portlist> – Specifies a range of ports to be configured. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, **1:3** would specify switch number 1, port 3. **2:4** specifies switch number 2, port 4. **1:3-2:4** specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order.<br><br>all – Specifies that the **config 802.1p default_priority** command will be applied to all ports on the switch.<br><br><priority 0-7> – Specifies the 802.1p priority value that an untagged, incoming packet will be given before being forwarded to its destination. |
| Restrictions | Only administrator-level users can issue this command. |

Example Usage:

To configure 802.1p default priority on the switch:

```
DGS-3212SR:4#config 802.1p default_priority all 5
Command: config 802.1p default_priority all 5

Success.

DGS-3212SR:4#
```

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

Example Usage:

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

```
DGS-3212SR: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
  25       0
  26       0

DGS-3212SR:4#
```

14

# 802.1X COMMANDS

The DGS-3212SR implements the server-side of the IEEE 802.1x Port-based Network Access Control. This mechanism is intended to allow only authorized users, or other network devices, access to network resources by establishing criteria for each port on the switch that a user or network device must meet before allowing that port to forward or receive frames.

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

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

| enable 802.1x | |
|---|---|
| Purpose | Used to enable the 802.1x server on the switch. |
| Syntax | **enable 802.1x** |
| Description | 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-3212SR:4#enable 802.1x
Command: enable 802.1x

Success.

DGS-3212SR:4#
```

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

Example Usage:

To disable 802.1x on the switch:

```
DGS-3212SR:4#disable 802.1x
Command: disable 802.1x

Success.

DGS-3212SR:4#
```

| show 802.1x | |
|---|---|
| Purpose | Used to display the current configuration of the 802.1x server on the switch. |
| Syntax | **show 802.1x {ports <portlist>}** |
| Description | The **show 802.1x** command is used to display the current configuration of the 802.1x Port-based Network Access Control server application on the switch. |
| Parameters | ports <portlist> – Specifies a range of ports. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, **1:3** would specify switch number 1, port 3. **2:4** specifies switch number 2, port 4. **1:3-2:4** specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order.<br><br>The following details what is displayed:<br><br>802.1x Enable\|Disable – Shows the current status of 802.1x functions on the switch.<br><br>Authentication Protocol: Raduis_Eap – Shows the authentication protcol suite in use between the switch and a Radius server.<br><br>Port number – Shows the physical port number on the switch. |

| show 802.1x | |
|---|---|
| Parameters | Capability: Authenticator\|None – Shows the capability of 802.1x functions on the port number displayed above. There are four 802.1x capabilities that can be set on the switch:<br><br>Authenciator, Suplicant, Authenticator and Suplicant, and None.<br><br>Prot Status: Authorized\|Unauthorized – Shows the result of the authentication process. Authorized means that the user was authenticated, and can access the network. Unauthorized means that the user wan not authenticated, and can not access the network.<br><br>PAE State: Initalize\|Disconnected\|Connecting\| Authenticating\|Authenticated\|Held \|ForceAuth\|ForceUnauth – Shows the current state of the Authenticator PAE.<br><br>Backend State: Request\|Response\|Fail\| Idle\|Initalize – Shows the current state of the Backend Authenticatior.<br><br>AdminCtlDir: Both\|In – Shows whether a controlled Port that is unauthorized will exert control over communication in both recieving and transmitting directions, or just the recieving direction. |

| show 802.1x | |
|---|---|
| Parameters | OpenCtlDir: Both\|In – Shows whether a controlled Port that is unauthorized will exert control over communication in both recieving and transmitting directions, or just the recieving direction.<br>Port Control: ForceAuth\|ForceUnauth\|Auto – Shows the adminstrative control over the port's authorization status. ForceAuth forces the Authenticator of the port to become Authorized. ForceUnauth forces the port to become Unauthorized.<br>QuietPeriod – Shows the time interval between authentication failure and the start of a new |
| Parameters | authentication attempt.<br>TxPeriod – Shows the time to wait for a response from a supplicant (user) to send EAP Request\|Identiy packets.<br>SuppTimeout – Shows the time to wait for a response from a supplicant (user) for all EAP packets, except for the Request\|Identity packets.<br>ServerTimeout – Shows the length of time to wait for a response from a Radius server.<br>MaxReq – Shows the maximum number of times to retry sending packets to the supplicant.<br>ReAuthPeriod – shows the time interval between successive re-authentications.<br>ReAuthenticate: Enable\|Disable – Shows whether or not to re-authenticate. |
| Restrictions | Only administrator-level users can issue this command. |

Example Usage:

To display 802.1x port settings for port 1:1:

```
DGS-3212SR:4#show 802.1x ports 1:
Command: show 802.1x ports 1:1

802.1X              : Disabled
Authentication Protocol: Radius_Eap

 Port number      : 1:1
 Capability       : None
 Port Status      : Authorized
 PAE  State       : ForceAuth
 Backend State    : Sucess
 AdminCrlDir      : Both
 OpenCrlDir       : Both
 Port Control     : Auto
 QuietPeriod      : 60    sec
 TxPeriod         : 30    sec
 SuppTimeout      : 30    sec
 ServerTimeout    : 30    sec
 MaxReq           : 2     times
 ReAuthPeriod     : 3600  sec
 ReAuthenticate   : Disabled

DGS-3212SR: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 four capabilities that can be set for each port. Authenticaor, Supplicant, Authenticator and Supplicant, and None. |
| Parameters | <portlist> – Specifies a range of ports. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, **1:3** would specify switch number 1, port 3. **2:4** specifies switch number 2, port 4. **1:3-2:4** specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order.<br>all – Specifies all of the ports on the switch.<br>authenticator – A user must pass the authentication process to gain access to the network.<br>none – The port is not controlled by the 802.1x functions. |
| Restrictions | Only administrator-level users can issue this command. |

Example Usage:

To configure 802.1x capability on ports 1-10 on switch 1:

```
DGS-3212SR:4#config 802.1x capability ports 1:1 – 1:10 authenticator

Command: config 802.1x capability ports 1-10 authenticator


 Success.


DGS-3212SR: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 <value 1-10>\|reauth_period <sec 1-65535>\|enable_reauth [enable\|disable]}]** |
| Description | The **config 802.1x auth_parameter** command is used to configure the 802.1x Authentication parameters on a range of ports. The default parameter will return all ports in the specified range to their default 802.1x settings. |
| Parameters | <portlist> – Specifies a range of ports. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, **1:3** would specify switch number 1, port 3. **2:4** specifies switch number 2, port 4. **1:3-2:4** specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order.<br>all – Specifies all of the ports on the switch.<br>default – Returns all of the ports in the specified range to their 802.1x default settings.<br>direction [both\|in] – Determins whether a controlled port blocks communication in both the recieving and transmitting directions, or just the receiving direction.<br>port_control – Configures the administrative control over the authentication process for the range of ports.<br>force_auth – Forces the Authenticator for the port to become authorized. Network access is allowed.<br>auto – Allows the port's status to reflect the outcome of the authentication process.<br>force_unauth – Forces the Authenticator for the port to become unauthorized. Network access will be blocked.<br>quiet_period <sec 0-65535> – Configures the time interval between authentication failure and the start of a new authenticaiton attempt.<br>max_req <value 1-10> – Configures the number of times to retry sending packets to a supplicant (user).<br>reauth_period <sec 1-65535> – Configures the time interval between successive re-authentications.<br>enable_reauth [enable\|disable] – Determines whether or not the switch will re-authenticate. Enable causes re-authentication of users at the time interval specified in the Re-authentication Period field, above. |
| Restrictions | Only administrator-level users can issue this command. |

Example Usage:

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

```
DGS-3212SR:4#config 802.1x auth_parameter ports 1:1 – 1:20 direction both

Command: config 802.1x auth_parameter ports 1:1-1:20 direction both


 Success.


DGS-3212SR:4#
```

| config 802.1x auth_mode | |
|---|---|
| Purpose | Used to configure 802.1x authentication mode. |
| Syntax | **config 802.1x auth_mode [port_based\|mac_based]** |
| Description | The configu 802.1x auth_mode command configures the authentication mode. |
| Parameters | port_based – Configure the authentication as port based mode.<br>mac_based – Configure the authentication as MAC based mode. |
| Restrictions | You must have administrator privileges. |

Example Usage:

To configure 802.1x authorization mode as MAC based:

```
DGS-3212SR:4#config 802.1x auth_mode mac_based
Command: config 802.1x auth_mode mac_based

 Success.

DGS-3212SR:4#
```

| config 802.1x init ports | |
|---|---|
| Purpose | Used to initialize the 802.1x functions on a range of ports. |
| Syntax | **config 802.1x init ports [<portlist>\|all]** |
| Description | The **config 802.1x init** command is used to immediately initialize the 802.1x functions on a range of ports. |
| Parameters | <portlist> – Specifies a range of ports. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, **1:3** would specify switch number 1, port 3. **2:4** specifies switch number 2, port 4. **1:3-2:4** specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order.<br>all – Specifies all of the ports on the switch. |
| Restrictions | Only administrator-level users can issue this command. |

Example Usage:

To initialize 802.1xfunctions on ports 1:1 – 1:15:

```
DGS-3212SR:4#config 802.1x init ports 1:1-1:15
Command: config 802.1x init ports 1:1-1:15

 Success.

DGS-3212SR:4#
```

## config 802.1x reauth ports

| | |
|---|---|
| Purpose | Used to configure the 802.1x re-authentication feature of the switch. |
| Syntax | **config 802.1x reauth ports [<portlist>\|all]** |
| Description | The **config 802.1x reauth ports** 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 lowest switch number and the beginning port number on that switch, separated by a colon. Then highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, **1:3** would specify switch number 1, port 3. **2:4** specifies switch number 2, port 4. **1:3-2:4** specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order.<br>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 posrts 1:1-1:15:

```
DGS-3212SR:4#config 802.1x init ports 1:1-1:15
Command: config 802.1x init ports 1:1-1:15

 Success.
DGS-3212SR:4#
```

| config radius add | |
|---|---|
| Purpose | Used to configure the settings the switch will use to communicate with a Radius server. |
| Syntax | **config radius add <server_index 1-3> <server_ip> key <passwd 32> [default\|{auth_port <udp_port_number>\| acct_port <udp_port_number>}]** |
| Description | The **config radius add** command is used to configure the settings the switch will use to communicate with a Radius server. |
| Parameters | <server_index 1-3> – Assins a number to the current set of Radius server settings. Up to 3 groups of Radius server settings can be entered on the switch.<br><server_ip> – The IP address of the Radius server.<br>key – Specifies that a password and encryption key will be used between the switch and the Radius server.<br><passwd 32> – The shared-secret key used by the Radius server and the switch. Up to 32 characters can be used.<br>default – Returns all of the ports in the range to their default Radius settings.<br>auth_port <udp_port_number> – The UDP port number for authentication requests. The default is 1812.<br>acct_port <udp_port_number> – The UDP port number for accounting requests. The default is 1813. |
| Restrictions | Only administrator-level users can issue this command. |

Example Usage:

To configure Radius server communication settings:

```
DGS-3212SR: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-3212SR:4#
```

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

Example Usage:

To delete previously configured Radius server communication settings:

```
DGS-3212SR:4#config radius delete 1
Command: config radius delete 1

Success.

DGS-3212SR:4#
```

| config radius | |
|---|---|
| Purpose | Used to configure the switch's Radius settings. |
| Syntax | **config radius <server_index 1-3> {ipaddress <server_ip> {ipaddress <server_ip>\|key <passwd 32>\|auth_port <udp_port_number>\|acct_port <udp_port_number>}** |
| Description | The **config radius** command is Used to configure the switch's Radius settings. |
| Parameters | <server_index 1-3> – Assins a number to the current set of Radius server settings. Up to 3 groups of Radius server settings can be entered on the switch.<br><br><server_ip> – The IP address of the Radius server.<br><br>key – Specifies that a password and encryption key will be used between the switch and the Radius server.<br><br><passwd 32> – The shared-secret key used by the Radius server and the switch. Up to 32 characters can be used.<br><br>default – Returns all of the ports in the range to their default Radius settings.<br><br>auth_port <udp_port_number> – The UDP port number for authentication requests. The default is 1812.<br><br>acct_port <udp_port_number> – The UDP port number for accounting requests. The default is 1813. |
| Restrictions | Only administrator-level users can issue this command. |

Example Usage:

To configure Radius settings:

```
DGS-3212SR: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-3212SR:4#
```

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

Example Usage:

To display Radius settings on the switch:

```
DGS-3212SR: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      des3326
3      30.1.1.1         1812               1813               Active      dlink

Total Entries : 3

DGS-3212SR:4#
```

15

# ACCESS CONTROL LIST (ACL) COMMANDS

The DGS-3212SR implements Access Control Lists that enable the switch to deny network access to specific devices or device groups based on IP settings or MAC address.

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

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

Due to a chipset limitation, the switch currently supports a maximum of 10 access profiles, each containing a maximum of 50 rules – with the additional limitation of 50 rules total for all 10 access profiles.

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

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

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

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

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

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

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

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

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

| create access_profile | |
|---|---|
| Purpose | Used to create an access profile on the switch and to define which parts of each incoming frame's header the switch will examine. Masks can be entered that will be combined with the values the switch finds in the specified frame header fields. Specific values for the rules are entered using the config access_profile command, below. |
| Syntax | **create access_profile [ethernet {vlan\|source_mac <macmask>\|destination_mac <macmask> \|802.1p\|ethernet_type}\|ip {vlan\|source_ip_mask <netmask>\|destination_ip_mask <netmask>\|dscp\|[icmp {type\|code}\|igmp {type}\|tcp {src_port_mask <hex 0x0-0xffff>\|dst_port_mask <hex 0x0-0xffff>}\|udp {src_port_mask <hex 0x0-0xfff>\|dst_port_mask <hex 0x0-0xffff>}\|protocol_id {user_mask <hex 0x0-0xffffffff>}]}]{[permit\|deny]\|profile_id <value 1-255>}** |
| Description | The create access_profile command is used to create an access profile on the switch and to define which parts of each incoming frame's header 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. |

| create access_profile | |
|---|---|
| Parameters | ethernet – Specifies that the switch will examine the layer 2 part of each packet header.<br>vlan – Specifies that the switch will examine the VLAN part of each packet header.<br>source_mac <macmask> – Specifies a MAC address mask for the source MAC address. This mask is entered in the following hexadecimal format,<br>destination_mac <macmask> – Specifies a MAC address mask for the destination MAC address.<br>802.1p – Specifies that the switch will examine the 802.1p priority value in the frame's header.<br>ethernet_type – Specifies that the switch will examine the Ethernet type value in each frame's header.<br>ip – Specifies that the switch will examine the IP address in each frame's header.<br>vlan – Specifies a VLAN mask.<br>source_ip_mask <netmask> – Specifies an IP address mask for the source IP address.<br>destination_ip_mask <netmask> – Specifies an IP address mask for the destination IP address.<br>dscp – Specifies that the switch will examine the DiffServ Code Point (DSCP) field in each frame's header.<br>icmp – Specifies that the switch will examine the Internet Control Message Protocol (ICMP) field in each frame's header. |

## create access_profile

| | |
|---|---|
| Parameters | type – Specifies that the switch will examine each frame's ICMP Type field.<br>code – Specifies that the switch will examine each frame's ICMP Code field.<br>igmp – Specifies that the switch will examine each frame's Internet Group<br>type – Specifies that the switch will examine each frame's IGMP Type field.<br>tcp – Specifies that the switch will examine each frames Transport Control Protocol (TCP) field.<br>src_port_mask <hex 0x0-0xffff> – Specifies a TCP port mask for the source port.<br>dst_port_mask <hex 0x0-0xffff> – Specifies a TCP port mask for the destination port.<br>udp – Specifies that the switch will examine each frame's Universal Datagram Protocol (UDP) field.<br>src_port_mask <hex 0x0-0xffff> – Specifies a UDP port mask for the source port.<br>dst_port_mask <hex 0x0-0xffff> – Specifies a UDP port mask for the destination port.<br>protocol_id – Specifies that the switch will examine each frame's Protocol ID field.<br>user_mask <hex 0x0-0xffffffff> – Specifies that the rule applies to the IP protocol ID and the mask options behind the IP header.<br>permit – Specifies that packets that match the access profile are permitted to be forwarded by the switch.<br>deny – Specifies that packets that do not match the access profile are not permitted to be forwarded by the switch and will be filtered.<br>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-3212SR: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-3212SR:4#
```

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

Example Usage:

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

```
DGS-3212SR:4# delete access_profile profile_id 1
Command: delete access_profile profile_id 1

Success.

DGS-3212SR: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 <value 0-65535>}\|protocol_id <value 0-255> {user_define <hex 0x0-0xffffffff>}]}]{priority <value 0-7> {replace_priority}\|replace_dscp <value 0-63>}\|delete <value 1-255>]** |
| Description | The **config access_profile** command is used to configure an access profile on the switch and to enter specific values that will be combined, using a logical AND operation, with masks entered with the **create access_profile** command, above. |

| config access_profile | |
|---|---|
| Parameters | profile_id <value 1-255> – <br><br> add access_id <value 1-255> – Adds an additional rule to the above specified access profile. The value specifies the relative priority of the additional rule. A lower access ID, the higher the priority the rule will be given. <br><br> ethernet – Specifies that the switch will look only into the layer 2 part of each packet. <br><br> vlan <vlan_name 32> – Specifies that the access profile will apply to only to this VLAN. <br><br> source_mac <macaddr> – Specifies that the access profile will apply to only packets with this source MAC address. <br><br> destination_mac <macaddr> – Specifies that the access profile will apply to only packets with this destination MAC address. <br><br> 802.1p <value 0-7> – Specifies that the access profile will apply only to packets with this 802.1p priority value. <br><br> ethernet_type <hex 0x0-0xffff> – Specifies that the access profile will apply only to packets with this hexidecimal 802.1Q Ethernet type value in the packet header. |

## config access_profile

Parameters

ip – Specifies that the switch will look into the IP fields in each packet.

vlan <vlan_name 32> – – Specifies that the access profile will apply to only to this VLAN.

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

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

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

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

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

code <value 0-255> – Specifies that the access profile will apply to this ICMP code.

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

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

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

## config access_profile

Parameters

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

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

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

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

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

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

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

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

| config access_profile | |
|---|---|
| Parameters | replace_priority – This parameter is specified if you want to change the 802.1p user priority of a packet that meets the specified criteria. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being transmitted from the switch.<br><br>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.<br><br>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-3212SR: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-3212SR:4#
```

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

Example Usage:

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

```
DGS-3212SR:4#
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
```

16

# TRAFFIC SEGMENTATION

Traffic segmentation allows you to further sub-divide VLANs into smaller groups of ports that will help to reduce traffic on the VLAN. The VLAN rules take precedence, and then the traffic segmentation rules are applied.

| Command | Parameters |
|---|---|
| config traffic_segmentation | <portlist><br>forward_list<br>null<br><portlist> |
| show traffic_segmentation | <portlist> |

| config traffic_segmentation | |
|---|---|
| Purpose | Used to configure traffic segmentation on the switch. |
| Syntax | **config traffic_segmentation <portlist> forward_list [null\|<portlist>]** |
| Description | The **config traffic_segmentation** command is used to configure traffic segmentation on the switch. |
| Parameters | <portlist> – Specifies a range of ports that will be configured for traffic setmentation. 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.<br>forward_list – Specifies a range of ports that will receive forwarded frames from the ports specified in the portlist, above.<br>null – no ports are specified<br><portlist> – Specifies a range of ports for the forwarding list. This list must be on the same switch previously specified for traffic segmentation (i.e. following the <portlist> specified above for config traffic_segmentation). |
| Restrictions | Only administrator-level users can issue this command. |

Example Usage:

To configure ports 1 through 10 to be able to forward frames to port 11 through 15:

```
DGS-3212SR:4# config traffic_segmentation 1-10 forward_list 11-15

Command: config traffic_segmentation 1-10 forward_list 11-15


Success.


DGS-3212SR:4#
```

## show traffic_segmentation

| | |
|---|---|
| Purpose | Used to display the current traffic segmentation configuration on the switch. |
| Syntax | **config traffic_segmentation <portlist> forward_list [null\|<portlist>]** |
| Description | The **show traffic_segmentation** command is used to display the current traffic segmentation configuration on the switch. |
| Parameters | <portlist> – Specifies a range of ports for which the current traffic setmentation configuration on the switch will 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 between port 3 and port 4 – in numerical order. |
| Restrictions | The port lists for segmentation and the forward list must be on the same switch. |

Example Usage:

To display the current traffic segmentation configuraiton on the switch.

```
DGS-3212SR:4#show traffic_segmentation
Command: show traffic_segmentation
Traffic Segmentation Table
Port  Forward Portlist
----  ------------------------------------------------
1     9-15
2     9-15
3     9-15
4     9-15
5     9-15
6     9-15
7     9-15
8     9-15
9     9-15
10    9-15
11    1-26
12    1-26
13    1-26
14    1-26
15    1-26
16    1-26
17    1-26
18    1-26
19    1-26
20    1-26
21    1-26
22    1-26
23    1-26
24    1-26
25    1-26
26    1-26

DGS-3212SR:4#
```

# 17

# STACKING

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

| Command | Parameters |
|---|---|
| config stacking mode | enable\|disable<br>auto_detect\|force_star\|force_ring<br>master\|auto\|slave<br>portlist <portlist> |
| show stacking | mode<br>version |

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

## config stacking mode

| | |
|---|---|
| Purpose | Used to configure the stacking mode. |
| Syntax | **config stacking mode [enable\|disable] [auto_detect\|force_star\|force_ring][master\|auto\|slave] [portlist <portlist>]** |
| Description | Configure the switch's stacking mode including the switch's role (master\|slave) and the topology used |
| Parameters | enable – To enable the switch to function in a stacked group.<br>disable – To disable the stacking function. This will force the switch to function as a standalone unit.<br>auto_detect – Use this command when using the switch with a stacked group of DES-3226S\|SR switches. This instructs the switch to detect the configured topology of the other switches in the stack.<br>The default topology is star for the DGS-3212SR. This is important if for example the preferred setup for a stacked group of DGS-3212SR switches is ring topology. Using auto_detect would not allow the ring topology to function since star topology will be indicated by the other switches.<br>force_star – This forces a star topology for the ports listed in the portlist <portlist>. This command requires an additional portlist command. It is not necessary for use with DES-3226S\|SR switches since star topology is required for such a stacked group.<br>force_ring – This forces a ring topology for the ports listed in the portlist <portlist>. This command requires an additional portlist command. It cannot be used with DES-3226S\|SR switches since star topology is required for such a stacked group.<br>master – The switch in the switch stack that becomes the management switch.<br>slave – Forces a given switch in the switch stack to never become the master switch.<br>auto - Automatically determine the master switch and the stacking order based upon the numerical value of the individual switch's MAC address. The lowest MAC address becomes the master switch.<br>portlist <portlist> – This command is dependent upon use of either the force_star or force_ring topology commands. It is not required if the topology is automatically determined (auto_detect). |
| Restrictions | Only administrator-level users can issue this command. |

Usage Example

To configure the stacking mode to force a star topology for ports 5-8:

```
DGS-3212SR:4#config stacking mode enable force_star auto portlist 1:5-1:8
Command: config stacking mode enable force_star auto portlist 1:5-1:8

Success.

DGS-3212SR:4#
```

| show stacking | |
|---|---|
| Purpose | Used to display the current stacking mode. |
| Syntax | **show stacking {mode\|version}** |
| Description | This command will display the current stacking mode. |
| Parameters | mode – Displays the current stacking mode.<br>version – Displays the version number of the stacking firmware. |
| Restrictions | None. |

Usage Example

To display the current stacking mode:

```
DES-3212SR:4#show stacking
Command: show stacking


DGS-3212SR:4#show stacking
Command: show stacking

 ID   MAC Address       Port Range   Mode       Version      RPS Status    Model Name
 ---  ----------------  ----------   ----------  --------    ------------  ----------
 *1   00-01-02-03-04-00  1 - 12      MASTER      1.00-B14    Not Present   DGS-3212SR
 *2   01-02-03-04-05-00  1 - 12      Slave       1.00-B14    Not Present   DGS-3212SR


 Total number = 2


DES-3212SR:4#
```

18

# PORT MIRRORING COMMANDS

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

| Command | Parameters |
|---|---|
| config mirror port | <port> [add\|delete]<br>source ports <portlist> [rx\|tx\|both] |
| enable mirror | |
| disable mirror | |
| show mirror | |

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

## config mirror port

| | |
|---|---|
| Purpose | Used to configure a mirror port – source port pair on the switch. |
| Syntax | config mirror port <port> add source ports <portlist> [rx\|tx\|both] |
| Description | This command allows a range of ports to have all of their traffic also sent to a designated port – where a network sniffer or other device can monitor the network traffic. In addition, you can specify that only traffic received by or sent by or both is mirrored to the Target port. |
| Parameters | <port> – This specifies the Target port (the port where mirrored packets will be sent). The Target port cannot be the same as the port being mirrored.<br><br><portlist> – specifies a range of ports to be configured. Ports are specified by entering the lowest port number in a group, and then the highest port number in a group, separated by a dash. So, a port group including the switch ports 1, 2, and 3 would be entered as **1-3**. Ports that are not contained within a group are specified by entering their port number, separated by a comma. So, the port group 1-3 and port 26 would be entered as **1-3, 26**. Additional ports can be individually entered by their port number, separated by commas.<br><br>rx – Allows the mirroring of only packets received (flowing into) the port or ports in the port list.<br><br>tx – Allows the mirroring of only packets sent (flowing out of) the port or ports in the port list.<br><br>both – Mirrors all the packets received or sent by the port or ports in the port list. |
| Restrictions | Only administrator-level users can issue this command. |

Example Usage:

To add the mirroring ports:

```
DGS-3212SR:4#config mirror port 1 add source ports 4 both
Command: config mirror port 1 add source ports 4 both

Success.

DGS-3212SR: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).<br><portlist> – This specifies a range of ports that will be mirrored. That is, a range of ports for which all traffic will be copied and sent to the Target port.<br>rx – Allows the mirroring of only packets received (flowing into) the port or ports in the port list.<br>tx – Allows the mirroring of only packets sent (flowing out of) the port or ports in the port list.<br>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-3212SR:4#config mirror port 1 delete source ports 4 both
Command: config mirror port 1 delete source ports 4 both

 Success.

DGS-3212SR:4#
```

| enable mirror | |
|---|---|
| Purpose | Used to enable a previously entered port mirroring configuration. |
| Syntax | **enable mirror** |
| Description | This command, combined with the disable mirror command below, allows you to enter a port mirroring configuration into the switch, and then turn the port mirroring on and off without having to modify the port mirroring configuration. |
| Parameters | None. |
| Restrictions | None. |

Example Usage:

To enable mirroring configurations:

```
DGS-3212SR:4#enable mirror
Command: enable mirror
 Success.
DGS-3212SR:4#
```

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

Example Usage:

To disable mirroring configurations:

```
DGS-3212SR:4#disable mirror
Command: disable mirror
 Success.
DGS-3212SR: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-3212SR:4#show mirror
Command: show mirror
 Current Settings
 Target Port: 9
 Mirrored Port:
        RX:
        TX: 1-5
DGS-3212SR:4#
```

19

# VLAN COMMANDS

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

| Command | Parameters |
|---|---|
| create vlan | <vlan_name><br>tag <vlanid><br>advertisement |
| delete vlan | <vlan_name> |
| config vlan | <vlan_name><br>add [tagged\|untagged\|forbidden]<br>delete<br><portlist><br>advertisement [enable\|disable] |
| config vlan | <vlan_name><br>delete <portlist> |
| config vlan | <vlan_name> |
| config gvrp | <portlist><br>all<br>state [enable\|disable]<br>ingress_checking [enable\|disable]<br>acceptable_frame [{tagged_only\|admit_all]]\|pvid <vlanid>} |
| enable gvrp | |
| disable gvrp | |
| show vlan | <vlan_name> |
| show gvrp | <portlist> |

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

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

Example Usage:

To create a VLAN v1, tag 2:

```
DGS-3212SR:4#create vlan v1 tag 2
Command: create vlan v1 tag 2

 Success.

DGS-3212SR:4#
```

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

Example Usage:

To remove a vlan v1:

```
DGS-3212SR:4#delete vlan v1
Command: delete vlan v1

 Success.

DGS-3212SR:4#
```

| config vlan | |
|---|---|
| Purpose | Used to add additional ports to or remove ports from a previously created VLAN. |
| Syntax | **config vlan <vlan_name> add [tagged\|untagged\|forbidden]\|delete <portlist>\|advertisement [enable\|disable]}** |
| Description | This command allows you to add or remove ports in the port list of a previously created VLAN. You can specifiy the additional ports as tagging, untagging, or forbidden. The default is to assign the ports as untagging. |
| Parameters | <vlan_name> – The name of the previously created VLAN you want to modify (adding or removing ports).<br>add – Specifies that the ports in the portlist are to be added to the VLAN named above.<br>tagged – Specifies the added ports as tagged ports.<br>untagged – Specifies the added ports as untagged ports.<br>forbidden – Specifies the added ports as forbidden port.<br>delete – Removes the ports specified in the portlist from the VLAN.<br><portlist> – A range of ports to add or delete on the VLAN. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, **1:3** would specify switch number 1, port 3. **2:4** specifies switch number 2, port 4. **1:3-2:4** specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order.<br>advertisement [**enable**\|**disable**] – Enables or disables GVRP on the specified VLAN. |
| Restrictions | Only administrator-level users can issue this command. |

Example Usage:

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

```
DGS-3212SR:4#config vlan v1 add tagged 2:4-2:8
Command: config vlan v1 add tagged 2:4-2:8

 Success.

DGS-3212SR:4#
```

## config gvrp

| | |
|---|---|
| Purpose | Used to configure GVRP on the switch. |
| Syntax | **config gvrp [<portlist>\|all] {state [enable\|disable]\|ingress_checking [enable\|disable]}\|acceptable_frame {[tagged_only\|admit_all]\|pvid <vlanid>}** |
| Description | This command is used to configure the Group VLAN Registration Protocol on the switch. You can configure ingress checking, the sending and receiving of GVRP information, and the Port VLAN ID (PVID). |
| Parameters | <portlist> – A range of ports for which you want ingress checking. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, **1:3** would specify switch number 1, port 3. **2:4** specifies switch number 2, port 4. **1:3-2:4** specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order.<br>all – Specifies all of the ports on the switch.<br>state [enable\|disable] – Enabled or disables GVRP for the ports specified in the port list.<br>ingress_checking [enable\|disable] – Enables or disables ingress checking for the specified port list.<br>acceptable_frame – determines the type of frame that will be accepted by the port.<br>tagged_only – only packets with a VLAN tag will be accepted.<br>admit_all – all packets will be accepted.<br>pvid – Specifies the VLAN that will be associated with the port. |
| Restrictions | Only administrator-level users can issue this command. |

Example Usage:

To set the ingress checking status, the sending and receiving GVRP information and Port VLAN ID(PVID):

```
DGS-3212SR:4#config gvrp 1:1-1:5 state enable ingress_checking
enable pvid 21

Command: config gvrp 1:1-1:5 state enable ingress_checking
enable pvid 21


 Success.


DGS-3212SR:4#
```

| enable gvrp | |
|---|---|
| Purpose | Used to enable GVRP on the switch. |
| Syntax | **enable gvrp** |
| Description | This command is used to enable GVRP on the switch – without changing the GVRP configuration on the switch. |
| Parameters | None. |
| Restrictions | Only administrator-level users can issue this command. |

Example Usage:

To enable the generic VLAN Registration Protocol (GVRP):

```
DGS-3212SR:4#enable gvrp
Command: enable gvrp

Success.

DGS-3212SR:4#
```

| disable gvrp | |
|---|---|
| Purpose | Used to disable GVRP on the switch. |
| Syntax | **disable gvrp** |
| Description | This command used to disable GVRP on the switch – without changing the GVRP configuration on the switch. |
| Parameters | None. |
| Restrictions | Only administrator-level users can issue this command. |

Example Usage:

To disable the Generic VLAN Registration Protocol (GVRP):

```
DGS-3212SR:4#disable gvrp
Command: disable gvrp

 Success.

DGS-3212SR:4#
```

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

```
DGS-3212SR:4#show vlan
Command: show vlan

VID              : 1              VLAN Name      : default
VLAN TYPE        : static         Advertisement  : Enabled
Member ports     : 1:1-1:26,2:1-2:26
 Static ports    : 1:1-1:26,2:1-2:26
Untagged ports   : 1:1-1:25,2:1-2:25
Forbidden ports  :
VID              : 2              VLAN Name      : v1
VLAN TYPE        : static         Advertisement  : Disabled
Member ports     : 1:26,2:26
 Static ports    : 1:26,2:26
Untagged ports   :
Forbidden ports  :

 Total Entries : 2

DGS-3212SR:4#
```

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

Example Usage:

To display GVRP port status:

```
DGS-3212SR:4#show gvrp
Command: show gvrp

 Global GVRP : Disabled

 Port   PVID    GVRP        Ingress Checking
 ----   ------- --------    --------------------
 1:1    21      Enabled     Enabled
 1:2    21      Enabled     Enabled
 1:3    21      Enabled     Enabled
 1:4    21      Enabled     Enabled
 1:5    21      Enabled     Enabled
 1:6    1       Disabled    Disabled
 1:7    1       Disabled    Disabled
 1:8    1       Disabled    Disabled
 1:9    1       Disabled    Disabled
 1:10   1       Disabled    Disabled
 1:11   1       Disabled    Disabled
 1:12   1       Disabled    Disabled
 1:13   1       Disabled    Disabled
 1:14   1       Disabled    Disabled
 1:15   1       Disabled    Disabled
```

```
1:16   1      Disabled       Disabled
1:17   1      Disabled       Disabled
1:18   1      Disabled       Disabled
1:19   1      Disabled       Disabled
1:20   1      Disabled       Disabled
1:21   1      Disabled       Disabled
1:22   1      Disabled       Disabled
1:23   1      Disabled       Disabled
1:24   1      Disabled       Disabled
1:25   1      Disabled       Disabled
1:26   0      Enabled        Disabled
2:1    1      Disabled       Disabled
2:2    1      Disabled       Disabled
2:3    1      Disabled       Disabled
2:4    1      Disabled       Disabled
2:5    1      Disabled       Disabled
2:6    1      Disabled       Disabled
2:7    1      Disabled       Disabled
2:8    1      Disabled       Disabled
2:9    1      Disabled       Disabled
2:10   1      Disabled       Disabled
2:11   1      Disabled       Disabled
2:12   1      Disabled       Disabled
2:13   1      Disabled       Disabled
```

```
2:14   1      Disabled       Disabled
2:15   1      Disabled       Disabled
2:16   1      Disabled       Disabled
2:17   1      Disabled       Disabled
2:18   1      Disabled       Disabled
2:19   1      Disabled       Disabled
2:20   1      Disabled       Disabled
2:21   1      Disabled       Disabled
2:22   1      Disabled       Disabled
2:23   1      Disabled       Disabled
2:24   1      Disabled       Disabled
2:25   1      Disabled       Disabled
2:26   0      Enabled        Disabled

Total Entries : 52

DGS-3212SR:4#
```

20

# LINK AGGREGATION COMMANDS

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

| Command | Parameters |
|---|---|
| create link_aggregation | group_id <value><br>type [lacp\|static] |
| delete link_aggregation | group_id <value> |
| config link_aggregation | group_id <value><br>master_port <port><br>ports <portlist><br>state [enable\|disable] |
| config link_aggregation algorithm | mac_source<br>mac_destination<br>mac_source_dest<br>ip_source<br>ip_destination<br>ip_source_dest |
| show link_aggregation | group_id <value><br>algorithm |

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

| create link_aggregation group_id | |
|---|---|
| Purpose | Used to create a link aggregation group on the switch. |
| Syntax | **create link_aggregation group_id <value>** |
| Description | This command will create a link aggregation group. |
| Parameters | <value> – Specifies the group id. The switch allows up to 6 link aggregation groups to be configured. The group number identifies each of the groups.<br>type – Specifies the group type as lacp or static. The default is static.<br>lacp – Specifies the group type as LACP.<br>static – Specifies the group type as static/ |
| Restrictions | Only administrator-level users can issue this command. |

Example Usage:

To create link aggregation group:

```
DGS-3212SR:4#create link_aggregation group_id 1
Command: create link_aggregation group_id 1

 Success.

DGS-3212SR:4#
```

| delete link_aggregation group_id | |
|---|---|
| Purpose | Used to delete a previously configured link aggregation group. |
| Syntax | **delete link_aggregation group_id <value>** |
| Description | This command is used to delete a previously configured link aggregation group. |
| Parameters | <value> – Specifies the group id. The switch allows up to 6 link aggregation groups to be configured. The group number identifies each of the groups. |
| Restrictions | Only administrator-level users can issue this command. |

Example Usage:

To delete link aggregation group:

```
DGS-3212SR:4#delete link_aggregation group_id 6
Command: delete link_aggregation group_id 6

 Success.

DGS-3212SR:4#
```

| config link_aggregation | |
|---|---|
| Purpose | Used to configure a previously created link aggregation group. |
| Syntax | **config link_aggregation group_id <value> {master_port <port>\|ports <portlist>\| {state [enable\|disable]}** |
| Description | This command allows you to configure a link aggregation group that was created with the **create link_aggregation** command above. |
| Parameters | <value> – Specifies the group id. The switch allows up to 6 link aggregation groups to be configured. The group number identifies each of the groups.<br><port> – Master port ID. Specifies which port (by port number) of the link aggregation group will be the master port. All of the ports in a link aggregation group will share the port configuration with the master port.<br><portlist> – specifies a range of ports to be configured. Ports are specified by entering the lowest port number in a group, and then the highest port number in a group, separated by a dash. So, a port group including the switch ports 1, 2, and 3 would be entered as **1-3**. Ports that are not contained within a group are specified by entering their port number, separated by a comma. So, the port group 1-3 and port 26 would be entered as **1-3, 26**. Additional ports can be individually entered by their port number, separated by commas.<br>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 of module 2:

```
DGS-3212SR: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-3212SR:4#
```

## config link_aggregation algorithm

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

Example Usage:

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

```
DGS-3212SR:4#config link_aggregation algorithm
mac_source_dest

Command: config link_aggregation algorithm mac_source_dest

 Success.


DGS-3212SR:4#
```

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

Example Usage:

To display the current link aggregation configuration:

```
DGS-3212SR:4#show link_aggregation
Command: show link_aggregation

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

21

# IP INTERFACE COMMANDS

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

| Command | Parameters |
|---|---|
| config ipif System | ipaddress <network_address> |
| show ipif | |

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

| config ipif System | |
|---|---|
| Purpose | Used to configure the System IP interface. |
| Syntax | **config ipif System [{vlan <vlan_name>\|ipaddress <network_address>\|state [enable\|disable]\|bootp\|dhcp}]** |
| Description | This command is used to configure the System IP interface on the switch. |
| Parameters | <vlan_name> – The name of the VLAN corresponding to the System IP interface.<br>\<network_address> – 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).<br>state [enable\|disable] – Allows you to enable or disable the IP interface.<br>bootp – Allows the selection of the BOOTP protocol for the assignment of an IP address to the switch's System IP interface.<br>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-3212SR:4#config ipif System ipaddress 10.48.74.122|8
Command: config ipif System ipaddress 10.48.74.122|8

 Success.

DGS-3212SR:4#
```

| show ipif | |
|---|---|
| Purpose | Used to display the configuration of an IP interface on the switch. |
| Syntax | **show ipif** |
| Description | This command will display the configuration of an IP interface on the switch. |
| Parameters | None. |
| Restrictions | None. |

Example Usage:

To display IP interface settings:

```
DGS-3212SR:4#show ipif
Command: show ipif

 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      : 1-26

DGS-3212SR:4#
```

22

# ROUTING TABLE COMMANDS

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

| Command | Parameters |
|---|---|
| create iproute | default<br><ipaddr><br><metric> |
| delete iproute | default |
| show iproute | |

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

| create iproute | |
|---|---|
| Purpose | Used to create an IP route entry to the switch's IP routing table. |
| Syntax | **create iproute [default] <ipaddr>** |
| 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.<br><ipaddr> – The IP address for the next hop router. |
| Restrictions | Only administrator-level users can issue this command. |

Example Usage:

To add a static address 10.48.74.121 to the routing table:

```
DGS-3212SR:4#create iproute 10.48.74.121
Command: create iproute 10.48.74.121

 Success.

DGS-3212SR:4#
```

| delete iproute | |
|---|---|
| Purpose | Used to delete an IP route entry from the switch's IP routing table. |
| Syntax | **delete iproute [default]** |
| Description | This command will delete an existing entry from the switch's IP routing table. |
| Parameters | default – deletes a default IP route entry. |
| Restrictions | Only administrator-level users can issue this command. |

Example Usage:

To delete a static address from the routing table:

```
DGS-3212SR:4#delete iproute default
Command: delete iproute default
 Success.
DGS-3212SR:4#
```

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

Example Usage:

To display the contents of the IP routing table:

```
DGS-3212SR:4#show iproute
Command: show iproute

IP Address       Netmask        Gateway        Interface Name  Hops  Protocol
---------------  ---------------  ---------------  ---------------  ----  -----------
 0.0.0.0          0.0.0.0        0.1.1.254      System          1    Default
 10.0.0.0       255.0.0.0    10.48.74.122     System          1     Local

Total Entries: 2

DGS-3212SR:4#
```

23

# IGMP SNOOPING COMMANDS

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

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

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

| config igmp_snooping | |
|---|---|
| Purpose | Used to configure IGMP snooping on the switch. |
| Syntax | config igmp_snooping [<vlan_name 32>\|all] {host_timeout <sec 1-16711450>\|router_timeout < sec 1-16711450>\|leave_timer < sec 1-16711450>\|state [enable\|disable]} |
| Description | This command allows you to configure IGMP snooping on the switch\| |
| Parameters | <vlan_name 32> – The name of the VLAN for which IGMP snooping is to be configured.<br>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.<br>route_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.<br>leave_timer < **sec 1-16711450>** – Leave timer. The default is 2 seconds.<br>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-3212SR:4#config igmp_snooping default host_timeout 250 state enable**

**Command: config igmp_snooping default host_timeout 250 state enable**

**Success.**

DGS-3212SR:4#

| config igmp_snooping querier | |
|---|---|
| Purpose | Used to configure the time in seconds between general query transmissions, the maximum time in seconds to wait for reports from members, the permitted packet loss that guarantees IGMP snooping. |
| Syntax | config igmp_snooping querier [<vlan_name 32>\|all] {query_interval <sec 1-65535>\|max_response_time <sec 1-25>\|robustness_variable <value 1-255>\|last_member_query_interval <sec 1-25>\|state [enable\|disable] |
| Description | This command configures IGMP snooping querier. |
| Parameters | <vlan_name 32> – The name of the VLAN for which IGMP snooping querier is to be configured.<br>query_interval <sec 1-65535> – Specifies the amount of time in seconds between general query transmissions. the default setting is 125 seconds.<br>max_response_time <sec 1-25> – Specifies the maximum time in seconds to wait for reports from members. The default setting is 10 seconds.<br>robustness_variable <value 1-255> – Provides fine-tuning to allow for expected packet loss on a subnet. The value of the robustness variable is used in calculating the following IGMP message intervals:<br>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).<br>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).<br>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.<br>By default, the robustness variable is set to 2. You might want to increase this value if you expect a subnet to loose packets.<br>last_member_query_interval <sec 1-25> – The maximum amount of time between group-specific query messages, including those sent in response to leave-group messages. You might lower this interval to reduce the amount of time it takes a router to detect the loss of the last member of a group.<br>state [enable\|disable] – Allows the switch to be specified as an IGMP Querier or Non-querier. |
| Restrictions | Only administrator-level users can issue this command. |

Example Usage:

To configure the igmp snooping:

```
DGS-3212SR:4#config igmp_snooping querier default
query_interval 125 state enable


Command: config igmp_snooping querier default query_interval
125 state enable


 Success.


DGS-3212SR:4#
```

| config router_ports | |
|---|---|
| Purpose | Used to configure ports as router ports. |
| Syntax | **config router_ports <vlan_name 32> [add\|delete] <portlist>** |
| Description | This command allows you to designate a range of ports as being connected to multicast-enable routers. This will ensure that all packets with such a router as its destination will reach the multicast-enable router – regardless of protocol, etc. |
| Parameters | <vlan_name 32> – The name of the VLAN on which the router port resides.<br><br><portlist> – specifies a range of ports to be configured. Ports are specified by entering the lowest port number in a group, and then the highest port number in a group, separated by a dash. So, a port group including the switch ports 1, 2, and 3 would be entered as **1-3**. Ports that are not contained within a group are specified by entering their port number, separated by a comma. So, the port group 1-3 and port 26 would be entered as **1-3, 26**. Additional ports can be individually entered by their port number, separated by commas. |
| Restrictions | Only administrator-level users can issue this command. |

Example Usage:

To set up static router ports:

```
DGS-3212SR:4#config router_ports default add 2:1-2:10
Command: config router_ports default add 2:1-2:10

Success.

DGS-3212SR:4#
```

| enable igmp_snooping | |
|---|---|
| Purpose | Used to enable IGMP snooping on the switch. |
| Syntax | **enable igmp_snooping {forward_mcrouter_only}** |
| Description | This command allows you to enable IGMP snooping on the switch. If **forward_mcrouter_only** is specified, the switch will forward all multicast traffic to the multicast router, only. Otherwise, the switch forwards all multicast 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-3212SR:4#enable igmp_snooping
Command: enable igmp_snooping

Success.

DGS-3212SR:4#
```

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

Example Usage:

To disable IGMP snooping on the switch:

```
DGS-3212SR:4#disable igmp_snooping
Command: disable igmp_snooping

 Success.

DGS-3212SR:4#
```

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

Example Usage:

To show igmp snooping:

```
DGS-3212SR: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-3212SR:4#
```

| show igmp_snooping group | |
|---|---|
| Purpose | Used to display the current IGMP snooping group configuration on the switch. |
| Syntax | **show igmp_snooping group {vlan <vlan_name 32>}** |
| Description | This command will display the current IGMP snooping group configuration on the switch. |
| Parameters | <vlan_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-3212SR: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          :26

 VLAN Name            : default
 Multicast group      : 224.0.0.9
 MAC address          : 01-00-5E-00-00-09
 Reports              : 1
 Port Member          : 26
 VLAN Name            : default
 Multicast group      : 234.5.6.7
 MAC address          : 01-00-5E-05-06-07
 Reports              : 1
 Port Member          : 26

 VLAN Name            : default
 Multicast group      : 236.54.63.75
 MAC address          : 01-00-5E-36-3F-4B
 Reports              : 1
 Port Member          : 26

 VLAN Name            : default
 Multicast group      : 239.255.255.250
 MAC address          : 01-00-5E-7F-FF-FA
 Reports              : 2
 Port Member          : 26

 Total Entries : 5
DGS-3212SR:4#
```

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

Example Usage:

To display the router ports.

```
DGS-3212SR:4#show router_ports
Command: show router_ports

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

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

 Total Entries: 2

DGS-3212SR:4#
```

24

# COMMAND HISTORY LIST

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

| Command | Parameters |
|---|---|
| ? | {command} |
| show command_history | |
| dir | |
| config command_history | <value> |

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

| ? | |
|---|---|
| Purpose | Used to display all commands in the Command Line Interface (CLI). |
| Syntax | **? {command}** |
| Description | This command will display all of the commands available through the Command Line Interface (CLI). |
| Parameters | <command> - a specific command or command group about which you are inquiring. |
| Restrictions | None. |

Usage Example:

To display all of the commands in the CLI:

```
DGS-3212SR: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 capability ports
config 802.1x init ports
config 802.1x reauth ports
config access_profile profile_id
config account
config arp_aging time
config arpentry
config bandwidth_control
config bootp_relay
config bootp_relay add ipif
config bootp_relay delete ipif
 CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

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

Usage Example:

To display the command history:

```
DGS-3212SR:4#show command_history
Command: show command_history

?
? show
show vlan
config router_ports vlan2 add 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-3212SR:4#
```

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

Usage Example:

To display all of the commands:

```
DGS-3212SR: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 capability ports
config 802.1x init ports
config 802.1x reauth ports
config access_profile profile_id
config account
config arp_aging time
config arpentry
config bandwidth_control
config bootp_relay
config bootp_relay add ipif
config bootp_relay delete ipif
 CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

| config command_history | |
|---|---|
| Purpose | Used to configure the command history. |
| Syntax | config command_history <value 1-40> |
| Description | This command is used to configure the command history. |
| Parameters | <value 1-40> – the number of commands to display from the switch's command history. |
| Restrictions | None. |

Usage Example:

To configure the command history:

```
DGS-3212SR:4#config command_history 20
Command: config command_history 20

 Success.

DGS-3212SR:4#
```

A

# TECHNICAL SPECIFICATIONS

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

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

| Performance | |
|---|---|
| Transmission Method | Store-and-forward |
| RAM Buffer | 8 MB per device |
| Filtering Address Table: | 8K MAC address per device |
| Packet Filtering\| Forwarding Rate: | Full-wire speed for all connections. 148,800 pps per port (for 100Mbps)<br>1,488,000 pps per port (for 1000Mbps) |
| MAC Address Learning | Automatic update. |
| Forwarding Table Age Time: | Max age:300–1000000 seconds.<br>Default = 300. |

| Physical and Environmental | |
|---|---|
| AC inputs | 100 - 240 VAC, 50\|60 Hz (internal universal power supply) |
| Power Consumption | 29 watts maximum |
| DC fans: | 2 built-in 40 x 40 x10 mm fan |
| Operating Temperature: | 0 to 50 degrees Celsius |
| Storage Temperature | -25 to 55 degrees Celsius |
| Humidity | Operating: 5% to 95% RH non-condensing; Storage: 0% to 95% RH non-condensing |
| Dimensions | 441 mm x 207 mm x 44 mm (1U), 19 inch rack-mount width |
| Weight | 2.5 kg |
| EMI: | FCC Class A, CE Class A, VCCI Class A, BSMI Class A, C-Tick Class A<br>FCC Part 15\|IECES-003 (Canada), VCCI Class A ITE, EN55022\|EN50082-1 or EN%%o24, C-Tick (AS\|NZS3548, BSMI (CNS 13438) |
| Safety: | UL, CSA, CE Mark, TUV\|GS<br>CSA International |