Information in this document is subject to change without notice.

© 2009 D-Link Computer Corporation. All rights reserved.

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

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

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

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.

Warnung!

Dies ist ein Produkt der Klasse A. Im Wohnbereich kann dieses Produkt Funkstörungen verursachen. In diesem Fall kann vom Benutzer verlangt werden, angemessene Massnahmen zu ergreifen.

Precaución!

Este es un producto de Clase A. En un entorno doméstico, puede causar interferencias de radio, en cuyo caso, puede requerirse al usuario para que adopte las medidas adecuadas.

Attention!

Ceci est un produit de classe A. Dans un environnement domestique, ce produit pourrait causer des interférences radio, auquel cas l’utilisateur devrait prendre les mesures adéquates.

Attenzione!

Il presente prodotto appartiene alla classe A. Se utilizzato in ambiente domestico il prodotto può causare interferenze radio, nel cui caso è possibile che l’utente debba assumere provvedimenti adeguati.

VCCI Warning

この装置は、クラス A 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

August, 2009
create snmp view.................................................................................................................................................................. 35
delete snmp view.................................................................................................................................................................. 35
show snmp view.................................................................................................................................................................. 36
create snmp community .......................................................................................................................................................... 37
delete snmp community .......................................................................................................................................................... 37
show snmp community .......................................................................................................................................................... 38
config snmp engineID............................................................................................................................................................ 38
show snmp engineID............................................................................................................................................................ 39
create snmp group ................................................................................................................................................................. 39
delete snmp group ................................................................................................................................................................. 41
show snmp groups ................................................................................................................................................................. 41
create snmp host ...................................................................................................................................................................... 42
delete snmp host ...................................................................................................................................................................... 43
show snmp host ...................................................................................................................................................................... 43
create trusted_host ................................................................................................................................................................. 44
delete trusted_host ................................................................................................................................................................. 44
enable snmp traps ................................................................................................................................................................. 45
disable snmp traps ................................................................................................................................................................. 45
enable snmp authenticate trap .................................................................................................................................................. 46
disable snmp authenticate trap .................................................................................................................................................. 46
show snmp traps ................................................................................................................................................................. 47
config snmp system_contact .................................................................................................................................................. 47
config snmp system_location .................................................................................................................................................. 48
config snmp system_name .................................................................................................................................................. 48
DOWNLOAD/UPLOAD COMMANDS ........................................................................................................................................... 49
download.................................................................................................................................................................................. 49
upload...................................................................................................................................................................................... 50
config dhcp_auto enable .......................................................................................................................................................... 51
show dhcp_auto...................................................................................................................................................................... 51
config firmware....................................................................................................................................................................... 52
show firmware information.......................................................................................................................................................... 52
NETWORK MONITORING COMMANDS .................................................................................................................................... 53
show packet ports................................................................................................................................................................. 53
show error ports................................................................................................................................................................. 54
show utilization................................................................................................................................................................. 55
clear counters................................................................................................................................................................. 55
clear log.................................................................................................................................................................................. 56
show log.................................................................................................................................................................................. 56
enable syslog................................................................................................................................................................. 57
disable syslog................................................................................................................................................................. 57
show syslog................................................................................................................................................................. 58
create syslog host ................................................................................................................................................................. 58
config syslog host................................................................................................................................................................. 60
delete syslog host ................................................................................................................................................................. 62
show syslog host................................................................................................................................................................. 63
SPANNING TREE COMMANDS .............................................................................................................................................. 64
config stp....................................................................................................................................................................... 64
config stp ports............................................................................................................................................................... 65
config stp version............................................................................................................................................................ 67
disable stp........................................................................................................................................................................ 67
enable stp ......................................................................................................................................................................... 67
show stp........................................................................................................................................................................... 68
show stp instance_id ....................................................................................................................................................... 69
show stp mst_config_id .............................................................. 70
config stp mst_config_id ................................................................. 70
cfg stp priority............................................................................................................................................................... 71
config stp mst_config_id ................................................................. 72
cfg stp mst_ports............................................................................................................................................................ 72

FORWARDING DATABASE COMMANDS ................................................................................................................... 75
create fdb........................................................................................................................................................................ 75
create multicast_fdb ........................................................................................................................................................ 76
config multicast_fdb ...................................................................................................................................................... 76
cfg fdb aging_time.......................................................................................................................................................... 77
delete fdb...................................................................................................................................................................... 77
clear fdb........................................................................................................................................................................ 78
show multicast_fdb ....................................................................................................................................................... 78
show fdb......................................................................................................................................................................... 79
cfg multicast filtering_mode .......................................................................................................................................... 80
show multicast filtering_mode .................................................................................................................................. 80
cfg dlf filtering_mode ................................................................................................................................................... 81
show dlf filtering_mode ............................................................................................................................................... 81

BROADCAST STORM CONTROL COMMANDS ........................................................................................................ 83
config traffic control .................................................................................................................................................... 83
show traffic control .................................................................................................................................................. 84

QOS COMMANDS ....................................................................................................................................................... 85
config scheduling .......................................................................................................................................................... 85
show scheduling .......................................................................................................................................................... 86
config bandwidth_control ........................................................................................................................................ 87
show bandwidth_control ....................................................................................................................................... 87
config 802.1p user_priority ...................................................................................................................................... 88
show 802.1p user_priority ......................................................................................................................................... 89
config 802.1p default_priority ................................................................. 90
show 802.1p default_priority .................................................................................................................................. 90
config scheduling _mechanism ................................................................................................................................ 91
show scheduling _mechanism .................................................................................................................................. 92
config rate _limit.......................................................................................................................................................... 92
show rate _limit.......................................................................................................................................................... 93

PORT MIRROURING COMMANDS .......................................................................................................................... 94
config mirror .................................................................................................................................................................. 94
delete mirror ................................................................................................................................................................. 95
show mirror ................................................................................................................................................................. 95

VLAN COMMANDS ................................................................................................................................................... 96
ARP COMMANDS................................................................................................................................................146

TIME AND SNTP COMMANDS...........................................................................................................................138

MAC AUTHENTICATION COMMANDS..............................................................................................................132

PORT SECURITY COMMANDS....................................................................................................................................135

TIME AND SNTP COMMANDS ...........................................................................................................................138

ROUTING TABLE COMMANDS ..........................................................................................................................144

ARP COMMANDS ..................................................................................................................................................146
BANNER COMMANDS .............................................................................................................................................151
  config login banner ................................................................................................................................................... 151

COMMAND HISTORY LIST COMMANDS ..........................................................................................................152
  ? ........................................................................................................................................................................... 152
  show command_history ........................................................................................................................................... 153
  dir ........................................................................................................................................................................ 153
  config command_history .................................................................................................................................... 154

SSH COMMANDS ................................................................................................................................................155
  enable ssh.............................................................................................................................................................. 155
  disable ssh.......................................................................................................................................................... 156
  config ssh authmode ............................................................................................................................................ 156
  show ssh authmode ............................................................................................................................................... 156
  config ssh server ................................................................................................................................................ 157
  show ssh server .................................................................................................................................................. 157
  show ssh algorithm ............................................................................................................................................. 158
  config ssh crypto ................................................................................................................................................ 158
  show ssh crypto .................................................................................................................................................. 159
  delete ssh crypto ................................................................................................................................................ 160

SSL COMMANDS ...............................................................................................................................................161
  enable ssl.............................................................................................................................................................. 161
  disable ssl.......................................................................................................................................................... 162
  show ssl ............................................................................................................................................................. 162
  show ssl cachetimeout ......................................................................................................................................... 163
  crypto certificate (generate) ................................................................................................................................ 163
  crypto certificate (request) .................................................................................................................................. 164
  crypto certificate (import) .................................................................................................................................. 165
  config ssl certificate .......................................................................................................................................... 165
  show crypto certificate mycertificate ................................................................................................................ 166

ACCESS AUTHENTICATION CONTROL COMMANDS ..................................................................................167
  create authen_login method_list_name .................................................................................................................. 168
  config authen_login ............................................................................................................................................... 168
  delete authen_login method_list_name .................................................................................................................. 169
  show authen_login ................................................................................................................................................. 170
  create authen_enable method_list_name .................................................................................................................. 170
  config authen_enable ............................................................................................................................................. 171
  delete authen_enable method_list_name .................................................................................................................. 172
  show authen_enable .............................................................................................................................................. 173
  config authen application ................................................................................................................................. 173
  show authen application .................................................................................................................................... 174
  create authen server_host .................................................................................................................................... 175
  config authen server_host .................................................................................................................................... 175
  delete authen server_host ..................................................................................................................................... 176
  show authen server_host ..................................................................................................................................... 177
  local_enable admin .............................................................................................................................................. 178
  config admin local_enable ................................................................................................................................... 178

LACP COMMANDS ..............................................................................................................................................180
  config lacp port_priority ....................................................................................................................................... 180
show safeguard_engine

LLDP COMMANDS

enable lldp (global)
disable lldp (global)
enable lldp forward_message
disable lldp forward_message
cfg lldp message tx_interval
cfg lldp message tx_hold_multiplier
cfg lldp reinit_delay
cfg lldp tx_delay
cfg lldp

cfg lldp ports
cfg lldp local_ports
cfg lldp remote_ports

cfg lldp ports

STACKING COMMANDS

cfg box_id

cfg box_id

cfg box_id

POE COMMANDS

config poe

cfg poe ports

cfg poe

ACCESS CONTROL LIST COMMANDS

create access_profile (for Ethernet)
cfg access_profile (for Ethernet)
cfg access_profile (for IP)
cfg access_profile

delete access_profile

cfg access_profile

cfg time_range

cfg time_range

TRAFFIC SEGMENTATION COMMANDS

config traffic_segmentation

cfg traffic_segmentation

TRACEROUTE COMMANDS

traceroute

SAFEGUARD COMMANDS

config safeguard_engine

cfg safeguard_engine

DEVICE SPECIFICATIONS

Technical Specifications

Cable Lengths
INTRODUCTION

The DGS-3100 series is a D-Link DGS-3100 switch family. The DGS-3100 series of products family consists of 24 / 48 -port 10/100/1000Base-T PoE / NonPoE L2 Stackable Management Switches with 4 Combo SFPs and DGS-3100-24TG, a switch with 16 SFPs and 8 copper GE ports.

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 Manual. For detailed information on installing hardware please refer also to the Manual.

Accessing the Switch via the Serial Port

The Switch’s serial port’s default settings are as follows:

- 9600 bps
- 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.

![Initial CLI screen](image)

**Figure 1–1. Initial CLI screen**

The initial username is admin (lower case). Press the Enter key twice to display the CLI input cursor. 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, but can be found on the initial boot console screen – shown below.
The Switch’s MAC address can also be found in the Web management program on the Device Information window on the Configuration menu.

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

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

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

2. Alternatively, enter config ipif System ipaddress xxx.xxx.xxx.xxx/z. Where the letter x represents the IP address to be assigned to the IP interface named System and the letter 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.
In the above example, the Switch was assigned an IP address of 1.1.1.10 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, SNMP MIB browser and the CLI or via the Web-based management agent using the above IP address to connect to the Switch.

**NOTE:** The DGS-3100 series of switches have the capability to be configured to have no IP address. This function may be used to disable Layer 3 functions of the Switch. When the IP address is disabled, the Switch can only be managed through the console port. Other management applications such as Telnet, Web-based and SNMP cannot be used to manage the Switch when the switch has no IP address.
The Switch 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 a SNMP-based network management software over the network.

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

**NOTE:** Switch configuration settings are saved to non-volatile RAM using the save command. The current configuration will then be retained in the Switch’s NV-RAM, and reloaded when the Switch is rebooted. If the Switch is rebooted without using the save command, the last configuration saved to NV-RAM is 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 (for example, the HyperTerminal program included with the Windows operating system) using an RS-232C serial cable. Your terminal parameters will need to be set to:

- VT-100 compatible
- 9600 bps
- 8 data bits
- No parity
- One stop bit
- No flow control

The same functions may also be accessed over a Telnet interface. Once an IP address for the Switch has been set, A Telnet program can be used (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 to logged in, the console looks like this:
Commands are entered at the command prompt, DGS3100#.

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

```
clear  clear
config config
create create
crypto Cryptographic commands
debug-mode Exit from the EXEC to debug mode
delete delete
dir display all commands.
disable disable
download download
enable enable
local_enable local_enable
locate locate the device.
login log in a user to the switch’s console.
logout log out a user from the switch’s console.
ping test the connectivity between network devices.
reboot restart the switch.
reset reset the switch to the factory default settings.
save save changes in the switch’s configuration to non-volatile ram.
show show
upload upload the current switch settings or the switch history log to a tftp server.
```

Figure 2–2. The ? Command

When entering a command without its required parameters, the CLI displays the prompt: command: config account message and the options listed below.
In this case, the command config account was entered with the parameter <username>. The CLI will then prompt to enter the <username> with the message, command: config account. 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, users can see all of the next possible sub-commands, in sequential order, by pressing the ? key.

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

In the above example, the command config account was entered without the required parameter <username>, the CLI returned the command: config account prompt. The up arrow cursor control key was pressed to re-enter the previous command (config account) at the command prompt. Now the appropriate username 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. The <> can also indicate a word with a number for character allowed.

If a command is entered that is unrecognized by the CLI, the top-level commands are displayed under the Available commands: prompt.
The top-level commands consist of commands such as show or config. Most of these commands require one or more parameters to narrow the top-level command. This is equivalent to show what? or config what? Where the what? is the next parameter.

For example, entering the show command with no additional parameters, the CLI will then display all of the possible next parameters.

In the above example, all of the possible next parameters for the show command are displayed. At the next command prompt in the example, 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.
The following symbols are used to describe how command entries are made and values and arguments are specified in this manual. The online help contained in the CLI and available through the console interface uses the same syntax.

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

### <angle brackets>

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Encloses a variable or value that must be specified.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>`create account [admin</td>
</tr>
<tr>
<td>Description</td>
<td>In the above syntax example, supply a username in the <code>&lt;username&gt;</code> space. Do not type the angle brackets.</td>
</tr>
<tr>
<td>Example Command</td>
<td><code>create account admin newadmin1</code></td>
</tr>
</tbody>
</table>

### [square brackets]

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Encloses a required value or set of required arguments. One value or argument can be specified.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>`create account [admin</td>
</tr>
<tr>
<td>Description</td>
<td>In the above syntax example, specify <code>admin</code>, <code>oper</code>, or a <code>user</code> level account to be created. Do not type the square brackets.</td>
</tr>
<tr>
<td>Example Command</td>
<td><code>create account user newuser1</code></td>
</tr>
</tbody>
</table>

### | vertical bar

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Separates two or more mutually exclusive items in a list, one of which must be entered.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>`create account [admin</td>
</tr>
<tr>
<td>Description</td>
<td>In the above syntax example, specify <code>admin</code>, <code>oper</code>, or <code>user</code>. Do not type the vertical bar.</td>
</tr>
<tr>
<td>Example Command</td>
<td><code>create account user newuser1</code></td>
</tr>
</tbody>
</table>

All commands are case-sensitive. Be sure to disable Caps Lock or any other unwanted function that changes text case.
### {braces}

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Encloses an optional value or set of optional arguments.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>reset</td>
</tr>
<tr>
<td>Description</td>
<td>execute &quot;reset&quot; will return the switch to its factory default setting.</td>
</tr>
</tbody>
</table>
| Example command | reset  
Please be aware that all configuration will be reset to default value.  
Are you sure you want to proceed with system reset now? (Y/N) | N |

### Line Editing Key Usage

<table>
<thead>
<tr>
<th>Key</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete</td>
<td>Deletes the character under the cursor and then shifts the remaining characters in the line to the left.</td>
</tr>
<tr>
<td>Backspace</td>
<td>Deletes the character to the left of the cursor and then shifts the remaining characters in the line to the left.</td>
</tr>
<tr>
<td>Insert or Ctrl+R</td>
<td>Toggle on and off. When toggled on, inserts text and shifts previous text to the right.</td>
</tr>
<tr>
<td>Left Arrow</td>
<td>Moves the cursor to the left.</td>
</tr>
<tr>
<td>Right Arrow</td>
<td>Moves the cursor to the right.</td>
</tr>
<tr>
<td>Up Arrow</td>
<td>Repeats the previously entered command. Each time the up arrow is pressed, the command previous to that displayed appears. This way it is possible to review the command history for the current session. Use the down arrow to progress sequentially forward through the command history list.</td>
</tr>
<tr>
<td>Down Arrow</td>
<td>The down arrow displays the next command in the command history entered in the current session. This displays each command sequentially as it was entered. Use the up arrow to review previous commands.</td>
</tr>
<tr>
<td>Tab</td>
<td>Shifts the cursor to the next field to the left.</td>
</tr>
<tr>
<td>Key</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Space</td>
<td>Displays the next page.</td>
</tr>
<tr>
<td>CTRL+c</td>
<td>Stops the display of remaining pages when multiple pages are to be displayed.</td>
</tr>
<tr>
<td>ESC</td>
<td>Stops the display of remaining pages when multiple pages are to be displayed.</td>
</tr>
<tr>
<td>n</td>
<td>Displays the next page.</td>
</tr>
<tr>
<td>p</td>
<td>Displays the previous page.</td>
</tr>
<tr>
<td>q</td>
<td>Stops the display of remaining pages when multiple pages are to be displayed.</td>
</tr>
<tr>
<td>r</td>
<td>Refreshes the pages currently displayed.</td>
</tr>
<tr>
<td>a</td>
<td>Displays the remaining pages without pausing between pages.</td>
</tr>
<tr>
<td>Enter</td>
<td>Displays the next line or table entry.</td>
</tr>
</tbody>
</table>
## BASIC SWITCH COMMANDS

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>create account</td>
<td>[admin</td>
</tr>
<tr>
<td>config account</td>
<td>&lt;username 15&gt;</td>
</tr>
<tr>
<td>show account</td>
<td></td>
</tr>
<tr>
<td>show session</td>
<td></td>
</tr>
<tr>
<td>show system_defaults</td>
<td></td>
</tr>
<tr>
<td>show switch</td>
<td></td>
</tr>
<tr>
<td>show serial_port</td>
<td></td>
</tr>
<tr>
<td>config serial_port</td>
<td>{baud_rate [2400</td>
</tr>
<tr>
<td>enable clipaging</td>
<td></td>
</tr>
<tr>
<td>disable clipaging</td>
<td></td>
</tr>
<tr>
<td>delete account</td>
<td>&lt;username 15&gt;</td>
</tr>
<tr>
<td>enable web</td>
<td>&lt;tcp_port_number 1-65535&gt;</td>
</tr>
<tr>
<td>disable web</td>
<td></td>
</tr>
<tr>
<td>save</td>
<td></td>
</tr>
<tr>
<td>reboot</td>
<td>&lt;box_id 1-6&gt;</td>
</tr>
<tr>
<td>reset</td>
<td></td>
</tr>
<tr>
<td>login</td>
<td></td>
</tr>
<tr>
<td>logout</td>
<td></td>
</tr>
<tr>
<td>ping</td>
<td>&lt;ipaddr&gt; {times &lt;value 1-255&gt;} {timeout &lt;sec 1-99&gt;}</td>
</tr>
<tr>
<td>show configuration</td>
<td>[running</td>
</tr>
<tr>
<td>enable jumbo_frame</td>
<td></td>
</tr>
<tr>
<td>disable jumbo_frame</td>
<td></td>
</tr>
<tr>
<td>show jumbo_frame</td>
<td></td>
</tr>
<tr>
<td>locate</td>
<td></td>
</tr>
<tr>
<td>enable telnet</td>
<td></td>
</tr>
<tr>
<td>disable telnet</td>
<td></td>
</tr>
<tr>
<td>Command</td>
<td>Parameter</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>enable dhcp_relay</td>
<td></td>
</tr>
<tr>
<td>disable dhcp_relay</td>
<td></td>
</tr>
<tr>
<td>config dhcp_relay add ipi</td>
<td>&lt;ipaddr&gt;</td>
</tr>
<tr>
<td>config dhcp_relay delete ipif</td>
<td>&lt;ipaddr&gt;</td>
</tr>
<tr>
<td>show dhcp_relay</td>
<td>{ipif}</td>
</tr>
</tbody>
</table>

Each command is listed in detail, as follows:

### create account

**Purpose**: To create user accounts.

**Syntax**: `create account [admin | oper | user] <username 15>

**Description**: The `create account` command creates an administrator, operator, or user account that consists of a username and an optional password. Up to 31 accounts can be created. The system prompts for the account's password, which may be between 0 and 15 characters.

**Parameters**:
- `admin` – creates an administrator account.
- `oper` – creates an operator account.
- `user` – creates a user account.
- `<username 1-15>` – The account username may be between 1 and 15 characters.

**Restrictions**: Only Administrator or Operator-level users can issue this command.

**Example usage**: To create an administrator-level user account with the username ‘dlink’:

```
DGS3100# create account admin dlink
Enter a case-sensitive password:****
Enter the password again for confirmation:****
Success.
DGS3100#
```

### config account

**Purpose**: To change the password for an existing user account.

**Syntax**: `config account <username 15>

**Description**: The `config account` command changes the password for a user account that has been created using the `create account` command. The system prompts for the account's new password, which may be between 0 and 15 characters.
Parameters  
<username 1-15> – the account username.

Restrictions  
Only Administrator-level users can issue this command.

Example usage:
To configure the user password of ‘dlink’ account:

```
DGS3100# config account dlink
Enter a case-sensitive new password:****
Enter the new password again for confirmation:****
Success.
DGS3100#
```

show account

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To display information about all user accounts on the Switch.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>show account</code></td>
</tr>
<tr>
<td>Description</td>
<td>The <code>show account</code> command displays all account usernames and their access levels created on the Switch. Up to 31 user accounts can exist on the Switch at one time.</td>
</tr>
<tr>
<td>Parameters</td>
<td>None.</td>
</tr>
<tr>
<td>Restrictions</td>
<td>None.</td>
</tr>
</tbody>
</table>

Example usage:
To display user account information:

```
DGS3100# show account

<table>
<thead>
<tr>
<th>Username</th>
<th>Access Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dlink</td>
<td>User</td>
</tr>
<tr>
<td>admin</td>
<td>Admin</td>
</tr>
</tbody>
</table>

Total Entries: 2

DGS3100#
```

show session

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To display information about currently logged-in users.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>show session</code></td>
</tr>
<tr>
<td>Description</td>
<td>The <code>show session</code> command displays a list of all the users that are logged-in at the time the command is issued. The information includes the session ID (0 for the first logged-in user, 1 for the next logged-in user, etc.), the Protocol used to connect to the Switch, the user’s IP address, the user's access Level (1=user, 15=admin), and</td>
</tr>
</tbody>
</table>
the account name on the Switch.

Parameters
None.

Restrictions
None.

Example usage:
To display the way users logged in:

```
DGS3100# show session

ID       Protocol    From          Level    Name
-------   ----------   ---------------------   --------   -----------------
0         HTTP        10.6.10.43          15    admin
1         HTTP        10.6.10.43          15    admin
2         Telnet      10.6.60.13          15    admin

DGS3100#
```

```
show system defaults

Purpose
To display information about all system defaults on the Switch.
Syntax
show system defaults
Description
The `show system defaults` command displays system defaults.
Parameters
None.
Restrictions
Only Administrator-level users can issue this command.

Example usage:
To display system default information:

```
DGS-3100# show system defaults
System Mode: Switch
Maximum units in stack: 6
# Management defaults
Telnet: Enabled
SSH: Enabled
HTTP: Enabled, port 80
HTTPS: Disabled
SNMP: Enabled.
   User: first
SNMP version: V3
SNMP Local Engine ID: 00001
SNMP Notifications: Enabled
SNMP Authentication Notifications: Enabled
AAA Telnet authentication login: Local user data base
AAA HTTP authentication login: Local data base
AAA HTTPS authentication login: Local data base
Logging: Enabled
   Logging to console: Informational messages
   Logging to internal buffer: Informational messages
   Logging to file: Error messages

DGS-3100#
```
Logging to remote server: Informational messages
Maximum no. of syslog messages: 430
SNTP Port No.: 123
DGS-3100#

### show switch

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To display information about the Switch.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>show switch</code></td>
</tr>
<tr>
<td>Description</td>
<td>The <code>show switch</code> command displays information about the Switch settings, including Device Type, MAC Address, IP configuration, Hardware/Software version, System information, and Switch Network configuration.</td>
</tr>
<tr>
<td>Parameters</td>
<td>None.</td>
</tr>
<tr>
<td>Restrictions</td>
<td>None.</td>
</tr>
</tbody>
</table>

#### Example usage:

To display the Switch information:

```
DGS3100# show switch
```

| Device Type | DGS-3100 Gigabit-Ethernet Switch |
| MAC Address | DA-10-21-00-00-01 |
| IP Address | 10.6.41.104 |
| VLAN Name | default |
| Subnet Mask | 255.255.255.224 |
| Default Gateway | 10.6.41.97 |
| Boot PROM Version | 1.0.0.03 |
| Firmware Version | 1.00.29 |
| Hardware Version | 00.00.01 |
| System Name | DGS-3100 |
| System Location | 7th_flr_east_cabinet |
| System Contact | Julius_Erving_212-555-6666 |
| Spanning Tree | Enabled |
| GVRP | Disabled |
| IGMP Snooping | Disabled |
| TELNET | Enabled |
| WEB | Enabled (TCP 80) |

DGS3100#

### show serial_port

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To display the current serial port settings.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>show serial_port</code></td>
</tr>
<tr>
<td>Description</td>
<td>The <code>show serial_port</code> command displays the current serial port configuration.</td>
</tr>
</tbody>
</table>

---

DGS-3100 Series Gigabit Stackable Managed Switch CLI Manual
settings.
Parameters None.
Restrictions None.

Example usage:
To display the serial port settings:

```
DGS3100# show serial_port
Baud Rate : 9600
Data Bits : 8
Parity Bits : None
Stop Bits : 1
Auto-Logout : 10 mins
DGS3100#
```

```
config serial_port
Purpose To configure the serial port.
Syntax  config serial_port {baud_rate [2400 | 4800 | 9600 | 19200 | 38400] auto_logout [never | 2_minutes | 5_minutes | 10_minutes | 15_minutes]}
Description The show serial_port command configures the serial port's baud rate and auto logout settings.
Parameters baud rate [2400 | 4800 | 9600 | 19200 | 38400] - The serial bit rate used to communicate with the management host.
auto_logout - The amount of time the Switch's serial port can be idle before automatically logging out. The possible values are:
never - There is no time limit on the length of time the console can be open with no user input.
2_minutes - The console logs out the current user if there is no user input for 2 minutes.
5_minutes - The console logs out the current user if there is no user input for 5 minutes.
10_minutes - The console logs out the current user if there is no user input for 10 minutes.
15_minutes - The console logs out the current user if there is no user input for 15 minutes.
Restrictions Only Administrator or operator-level users can issue this command.

Example usage:
To configure the baud rate:

```
DGS3100# config serial_port baud_rate 9600
Success.
DGS3100#
```
### enable clipaging

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To pause the scrolling of the console screen after each page when a show command displays more than one page.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>enable clipaging</td>
</tr>
<tr>
<td>Description</td>
<td>The <code>enable clipaging</code> command pauses the scrolling of the console screen at the end of each page when issuing a command which would display more than one screen of information. The default setting is enabled.</td>
</tr>
<tr>
<td>Parameters</td>
<td>None.</td>
</tr>
<tr>
<td>Restrictions</td>
<td>Only Administrator or operator-level users can issue this command.</td>
</tr>
</tbody>
</table>

**Example usage:**

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

```plaintext
DGS3100# enable clipaging
Success.
DGS3100#
```

### disable clipaging

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To disable the pausing of the console screen scrolling at the end of each page when the command displays more than one screen of information.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>disable clipaging</td>
</tr>
<tr>
<td>Description</td>
<td>The <code>disable clipaging</code> command disables the pausing of the console screen at the end of each page when issuing a command which would display more than one screen of information. This causes the console screen to rapidly scroll through several pages.</td>
</tr>
<tr>
<td>Parameters</td>
<td>None.</td>
</tr>
<tr>
<td>Restrictions</td>
<td>Only Administrator or operator-level users can issue this command.</td>
</tr>
</tbody>
</table>

**Example usage:**

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

```plaintext
DGS3100# disable clipaging
Success.
DGS3100#
```

### delete account

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To delete an existing user account.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>delete account &lt;username 15&gt;</td>
</tr>
<tr>
<td>Description</td>
<td>The <code>delete account</code> command deletes a user account that has been</td>
</tr>
</tbody>
</table>

---

17
**create account**

*Parameters*

<username 1-15> – the account username.

*Restrictions*

Only Administrator-level users can issue this command.

**Example usage:**

To delete the user account ‘System’:

```
DGS3100# delete account System

Are you sure to delete the last administrator account?(y/n)

Success.

DGS3100#
```

**enable web**

*Purpose*

To enable the HTTP-based management software on the Switch.

*Syntax*

```
enable web <tcp_port_number 1-65535>
```

*Description*

The `enable web` command enables the Web-based management software on the Switch. The user can specify the TCP port number the Switch uses to listen for Telnet requests.

*Parameters*

<tcp_port_number 1-65535> – The TCP port number. TCP ports are numbered between 1 and 65535. The ‘well-known’ port for the Web-based management software is 80.

*Restrictions*

Only Administrator or operator-level users can issue this command.

**Example usage:**

To enable HTTP and configure the TCP port number to listen for Telnet requests:

```
DGS3100# enable web 80

Success.

DGS3100#
```

**disable web**

*Purpose*

To disable the HTTP-based management software on the Switch.

*Syntax*

```
disable web
```

*Description*

The `disable web` command disables the Web-based management software on the Switch.

*Parameters*

None.

*Restrictions*

Only Administrator or operator-level users can issue this command.

**Example usage:**

To disable HTTP-based management software on the Switch:

```
DGS3100# disable web
```
save

Purpose To save changes in the Switch's configuration to non-volatile RAM.
Syntax `save`
Description The `save` command saves the current switch configuration to non-volatile RAM. The saved switch configuration is loaded to 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:

```
DGS3100# save

verbatim file [startup-config] ?[Yes/press any key for no]...01-Jan-2000 19:03
:59 %COPY-I-FILECPY: Files Copy - source URL running-config destination URL flash:
01-Jan-2000 19:04:06 %COPY-N-TRAP: The copy operation was completed successfully

Copy succeeded
Success.
DGS3100#
```

reboot

Purpose To reboot the Switch. If the Switch is a member of a stack, it may be rebooted individually, without affecting the other members of the stack.
Syntax `reboot <box_id 1-6>`
Description The `reboot` command restarts the Switch.
Parameters `<box_id 1-6>` - The unit's current stack membership number.
Restrictions Only Administrator or operate-level users can issue this command.

Example usage:
To restart the Switch unit 1:

```
DGS3100# reboot 1
```

Success.
DGS3100#
DGS3100# reboot 1
Are you sure you want to proceed with system reboot now? (Y/N)[N] Y
This action may take a few minutes
DGS3100#

<table>
<thead>
<tr>
<th>reset</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td><strong>Syntax</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td><strong>Parameters</strong></td>
</tr>
<tr>
<td><strong>Restrictions</strong></td>
</tr>
</tbody>
</table>

**Example usage:**

To restore all of the Switch’s parameters to their default values:

```
DGS3100# reset
Please be aware that all configuration will be reset to default value.
Are you sure you want to proceed with system reset now? (Y/N)[N] Y
Deleting auto update backup file...OK
Deleting auto update instruction file...OK
Deleting startup configuration file... Done.
Please make sure that your terminal is set to the default baud rate - 9600 bps.
This action may take a few minutes
Success.
DGS3100#
```

<table>
<thead>
<tr>
<th>login</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td><strong>Syntax</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td><strong>Parameters</strong></td>
</tr>
<tr>
<td><strong>Restrictions</strong></td>
</tr>
</tbody>
</table>

**Example usage:**

To initiate the login procedure:
logout

Purpose: To log out a user from the Switch's console.
Syntax: Logout
Description: The `logout` 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:

```
DGS3100# logout
```

ping

Purpose: To test the connectivity between network devices.
Syntax: `ping <ipaddr> {times <value 1-255>} {timeout <sec 1-99>}`
Description: The `ping` command sends Internet Control Message Protocol (ICMP) echo messages to a remote IP address. The remote IP address then 'echos' or returns the message. This is used to confirm connectivity between the Switch and the remote device.
Parameters:
- `<ipaddr>` - The IP address of the host.
- `times <value 1-255>` - The number of individual ICMP echo messages to be sent. The maximum value is 255. The default is 4.
- `timeout <sec 1-99>` - The time-out period while waiting for a response from the remote device. A value of 1 to 99 seconds can be specified. The default is 1 second.
Restrictions: None.

Example usage:
To ping the IP address 10.6.150.34 three times:

```
DGS3100# ping 10.6.150.34 times 3
Pinging 10.6.150.34 with 56 bytes of data:

56 bytes from 10.6.150.34: icmp_seq=1. time=0 ms
56 bytes from 10.6.150.34: icmp_seq=2. time=0 ms
56 bytes from 10.6.150.34: icmp_seq=3. time=0 ms

----10.6.150.34 PING Statistics----
3 packets transmitted, 3 packets received, 0% packet loss
round-trip (ms) min/avg/max = 0/0/0
```
show configuration

Purpose: To display the current or saved version of the configuration settings of the Switch.

Syntax: `show configuration [running | startup]`

Description: The `show configuration` command displays the current or saved version of the configuration settings of the Switch.

Parameters:
- `running`: Displays the current configuration.
- `startup`: Displays the configuration saved in NV-RAM.

Restrictions: None.

Example usage:

To show current configuration information:

```
DGS3100# show configuration running

config snmp system_name DGS-3100
create vlan 2 tag 2
enable 802.1x
config 802.1x auth_protocol radius
config radius add 10.6.41.226 key 123456 auth_port 1812 acct_port 1813 priority first
config ports (1-2,4-7) enable_reauth enable
config ports 3 port_control auto enable_reauth enable
config 802.1x auth_mode ports (1-7) mac_based
config 802.1x guest_vlan 2 state enable
config 802.1x guest_vlan ports 3
config ipif system dhcp
DGS3100#
```

enable jumbo_frame

Purpose: To enable jumbo frames on the device.

Syntax: `enable jumbo_frame`

Description: The `enable jumbo_frame` command enables jumbo frames on the device.

Parameters: None.

Restrictions: Only Administrator or operate-level users can issue this command. Jumbo frames will be enabled after save and restart.
### Example usage:
To enable jumbo frames:

```
DGS3100# enable jumbo_frame
Jumbo frames will be enabled after save and restart.

Success.
DGS3100#
```

### disable jumbo_frame

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To disable jumbo frames on the device.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>disable jumbo_frame</code></td>
</tr>
<tr>
<td>Description</td>
<td>The <code>disable jumbo_frame</code> command disables jumbo frames on the device.</td>
</tr>
<tr>
<td>Parameters</td>
<td>None.</td>
</tr>
<tr>
<td>Restrictions</td>
<td>Only Administrator or operate-level users can issue this command. Jumbo frames will be disabled after save and restart.</td>
</tr>
</tbody>
</table>

### Example usage:
To disable jumbo frames:

```
DGS3100# disable jumbo_frame
Jumbo frames will be disabled after save and restart.

Success.
DGS3100#
```

### show jumbo_frame

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To display the jumbo frame configuration.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>show jumbo_frame</code></td>
</tr>
<tr>
<td>Description</td>
<td>The <code>show jumbo_frame</code> command displays the jumbo frame configuration.</td>
</tr>
<tr>
<td>Parameters</td>
<td>None.</td>
</tr>
<tr>
<td>Restrictions</td>
<td>None.</td>
</tr>
</tbody>
</table>

### Example usage:
To show the jumbo frames configuration status on the device:

```
DGS3100# show jumbo_frame
Jumbo frames are disabled.
DGS3100#
```
### locate

- **Purpose**: To enable the user to locate the device he is working on.
- **Syntax**: `locate`
- **Description**: The `locate` command causes the seven segment display of the currently active switch with Master ID to blink the letter L for 20 seconds.
- **Parameters**: None.
- **Restrictions**: Only Administrator or operate-level users can issue this command.

**Example usage:**

To display the currently active switch:

```
DGS3100# locate
Success.
DGS3100#
```

### enable telnet

- **Purpose**: To enable the telnet.
- **Syntax**: `enable telnet`
- **Description**: The `enable telnet` command enables telnet.
- **Parameters**: None.
- **Restrictions**: Only Administrator or operate-level users can issue this command.

**Example usage:**

To enable telnet:

```
DGS3100# enable telnet
Success.
DGS3100#
```

### disable telnet

- **Purpose**: To disable telnet.
- **Syntax**: `disable telnet`
- **Description**: The `disable telnet` command disables telnet.
- **Parameters**: None.
- **Restrictions**: Only Administrator or operate-level users can issue this command.

**Example usage:**

To disable telnet:

```
DGS3100# disable telnet
```
enable dhcp_relay

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To enable DHCP Relay server on the Switch</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>enable dhcp_relay</td>
</tr>
<tr>
<td>Description</td>
<td>The <code>enable dhcp_relay</code> command sets the DHCP Relay to be globally enabled on the Switch and on all existing VLANs.</td>
</tr>
<tr>
<td>Parameters</td>
<td>None.</td>
</tr>
<tr>
<td>Restrictions</td>
<td>Only Administrator or operate-level users can issue this command.</td>
</tr>
</tbody>
</table>

Example usage:

To enable DHCP Relay on the Switch:

```
DGS-3100# enable dhcp_relay
Success.
DGS-3100# 
```

disable dhcp_relay

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To disable DHCP Relay server on the Switch</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>disable dhcp_relay</td>
</tr>
<tr>
<td>Description</td>
<td>The <code>disable dhcp_relay</code> command sets the DHCP Relay to be globally disabled on the Switch and on all existing VLANs.</td>
</tr>
<tr>
<td>Parameters</td>
<td>None.</td>
</tr>
<tr>
<td>Restrictions</td>
<td>Only Administrator or operate-level users can issue this command.</td>
</tr>
</tbody>
</table>

Example usage:

To disable DHCP Relay on the Switch:

```
DGS-3100# disable dhcp_relay
Success.
DGS-3100# 
```

config dhcp_relay add ipif

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To define a DHCP server as a DHCP Relay server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>config dhcp_relay add ipif &lt;ipaddr&gt;</code></td>
</tr>
<tr>
<td>Description</td>
<td>The <code>config dhcp_relay add ipif</code> command adds DHCP servers as DHCP Relay servers.</td>
</tr>
<tr>
<td>Parameters</td>
<td><code>&lt;ipaddr&gt;</code> – The IP address of the DHCP server. Up to 4 servers can</td>
</tr>
</tbody>
</table>
Example usage:
To add a DHCP server as a DHCP Relay server:

```
DGS-3100# config dhcp_relay add ipif 10.6.150.49
Success.
DGS-3100#
```

Example usage:
To remove a DHCP server from the DHCP Relay server list:

```
DGS-3100# config dhcp_relay delete ipif 10.6.150.49
Success.
DGS-3100#
```

Example usage:
To display DHCP Relay settings:

```
DGS-3100#show dhcp_relay ipif

DHCP Relay Status : Enabled
Server IP
---------------------
```

```
10.6.150.49
DGS-3100#
The Switch Port commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

<table>
<thead>
<tr>
<th>Command</th>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>config ports</td>
<td>[all</td>
</tr>
<tr>
<td>show ports</td>
<td>{&lt;portlist&gt;}</td>
</tr>
<tr>
<td>config ports description</td>
<td>&lt;portlist&gt; &lt;string 1-64&gt;</td>
</tr>
<tr>
<td>delete ports description</td>
<td>&lt;portlist&gt;</td>
</tr>
<tr>
<td>show ports description</td>
<td>{&lt;portlist&gt;}</td>
</tr>
</tbody>
</table>

Each command is listed in detail, as follows:

**config ports**

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To configure the Switch’s Ethernet port settings.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>config ports [all</td>
</tr>
<tr>
<td>Description</td>
<td>The config ports command configures the Switch’s Ethernet port settings. Only the ports listed in the &lt;portlist&gt; are affected.</td>
</tr>
<tr>
<td>Parameters</td>
<td>&lt;portlist&gt; – A port or range of ports to be configured. all – Configures all ports on the Switch. &lt;ch1–32&gt; – A LAG or range of LAGs to be configured. speed – Sets the speed of a port or range of ports, with the addition of one of the following: • auto – Enables auto-negotiation for the specified range of ports. • [10</td>
</tr>
</tbody>
</table>
Restrictions
Only administrator or operate-level users can issue this command.

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

```
DGS3100# config ports 1-3 speed 10_full learning enable state enable
Success.
DGS3100#
```

show ports

Purpose
To display the current configuration of a range of ports.

Syntax
```
show ports {<portlist>}
```

Description
The `show ports` command displays the current configuration of a port or range of ports.

Parameters
- `<portlist>` - A port or range of ports whose settings are to be displayed.

Restrictions
None.

Example usage:
To display the configuration of all ports on the Switch:

```
DGS3100# show ports

<table>
<thead>
<tr>
<th>Port</th>
<th>State</th>
<th>Settings</th>
<th>Connection</th>
<th>Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>1:1</td>
<td>Enabled</td>
<td>Auto/Disabled</td>
<td>Link Down</td>
<td>Enabled</td>
</tr>
<tr>
<td>1:2</td>
<td>Enabled</td>
<td>Auto/Disabled</td>
<td>Link Down</td>
<td>Enabled</td>
</tr>
<tr>
<td>1:3</td>
<td>Enabled</td>
<td>Auto/Disabled</td>
<td>100M/Full/Disabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>1:4</td>
<td>Enabled</td>
<td>Auto/Disabled</td>
<td>100M/Full/Disabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>1:5</td>
<td>Enabled</td>
<td>Auto/Disabled</td>
<td>Link Down</td>
<td>Enabled</td>
</tr>
<tr>
<td>1:6</td>
<td>Enabled</td>
<td>Auto/Disabled</td>
<td>Link Down</td>
<td>Enabled</td>
</tr>
<tr>
<td>1:7</td>
<td>Enabled</td>
<td>Auto/Disabled</td>
<td>Link Down</td>
<td>Enabled</td>
</tr>
<tr>
<td>1:8</td>
<td>Enabled</td>
<td>Auto/Disabled</td>
<td>Link Down</td>
<td>Enabled</td>
</tr>
<tr>
<td>1:9</td>
<td>Enabled</td>
<td>Auto/Disabled</td>
<td>Link Down</td>
<td>Enabled</td>
</tr>
<tr>
<td>1:10</td>
<td>Enabled</td>
<td>Auto/Disabled</td>
<td>Link Down</td>
<td>Enabled</td>
</tr>
<tr>
<td>1:11</td>
<td>Enabled</td>
<td>Auto/Disabled</td>
<td>Link Down</td>
<td>Enabled</td>
</tr>
<tr>
<td>1:12</td>
<td>Enabled</td>
<td>Auto/Disabled</td>
<td>Link Down</td>
<td>Enabled</td>
</tr>
<tr>
<td>1:13</td>
<td>Enabled</td>
<td>Auto/Disabled</td>
<td>Link Down</td>
<td>Enabled</td>
</tr>
<tr>
<td>1:14</td>
<td>Enabled</td>
<td>Auto/Disabled</td>
<td>Link Down</td>
<td>Enabled</td>
</tr>
<tr>
<td>1:15</td>
<td>Enabled</td>
<td>Auto/Disabled</td>
<td>Link Down</td>
<td>Enabled</td>
</tr>
<tr>
<td>1:16</td>
<td>Enabled</td>
<td>Auto/Disabled</td>
<td>Link Down</td>
<td>Enabled</td>
</tr>
<tr>
<td>1:17</td>
<td>Enabled</td>
<td>Auto/Disabled</td>
<td>Link Down</td>
<td>Enabled</td>
</tr>
<tr>
<td>1:18</td>
<td>Enabled</td>
<td>Auto/Disabled</td>
<td>Link Down</td>
<td>Enabled</td>
</tr>
<tr>
<td>1:19</td>
<td>Enabled</td>
<td>Auto/Disabled</td>
<td>Link Down</td>
<td>Enabled</td>
</tr>
</tbody>
</table>
```
### config ports description

**Purpose**
To add a description to an interface or ranges of interface.

**Syntax**
```
config ports description <portlist> <string 1-64>
```

**Description**
The `config ports description` command adds a description to an interface or a range of interfaces.

**Parameters**
- `<portlist>` – A port or range of ports to add a description to.
- `<string 1-64>` – Description content.

**Restrictions**
None.

**Example usage:**
To add a description to port 1:

```
DGS3100# config ports description 1:1 "For testing purposes only"
Success.
DGS3100#
```

### delete ports description

**Purpose**
To delete a description of an interface or a range of interfaces.

**Syntax**
```
delete ports description <portlist>
```

**Description**
The `delete ports description` command deletes a description of an interface or a range of interfaces.

**Parameters**
- `<portlist>` – A port or range of ports to delete descriptions from.

**Restrictions**
None.

**Example usage:**
To delete the description of port 1:

```
DGS3100# delete ports description 1:1
Success.
DGS3100#
```

### show ports description

**Purpose**
To display a description of an interface or a range of interfaces.

**Syntax**
```
show ports description {<portlist>}
```

**Description**
The `show ports description` command displays a description of an interface or a range of interfaces.

**Parameters**
- `<portlist>` – A port or range of ports whose descriptions are to be displayed.
displayed.
Restrictions  None.

Example usage:
To display the description of port 1:

```
DGS3100# show ports description 1:1

<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1:1</td>
<td>For testing purposes only</td>
</tr>
</tbody>
</table>

DGS3100#```
# NETWORK MANAGEMENT (SNMP) COMMANDS

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>create snmp user</td>
<td>&lt;username 24&gt; &lt;groupname 30&gt; [encrypted [by_password auth [md5 &lt;auth_password 1-32&gt;</td>
</tr>
<tr>
<td>delete snmp user</td>
<td>&lt;username 24&gt;</td>
</tr>
<tr>
<td>show snmp user</td>
<td></td>
</tr>
<tr>
<td>create snmp view</td>
<td>&lt;view_name 30&gt; &lt;oid&gt; view_type [included</td>
</tr>
<tr>
<td>delete snmp view</td>
<td>&lt;view_name 30&gt; [all</td>
</tr>
<tr>
<td>show snmp view</td>
<td>(&lt;view_name 30&gt;)</td>
</tr>
<tr>
<td>create snmp community</td>
<td>&lt;community_string 20&gt; view &lt;view_name 30&gt; [read_only</td>
</tr>
<tr>
<td>delete snmp community</td>
<td>&lt;community_string 20&gt;</td>
</tr>
<tr>
<td>show snmp community</td>
<td>(&lt;community_string 20&gt;)</td>
</tr>
<tr>
<td>config snmp engineID</td>
<td>[default</td>
</tr>
<tr>
<td>show snmp engineID</td>
<td></td>
</tr>
<tr>
<td>create snmp group</td>
<td>&lt;groupname 30&gt; [v1</td>
</tr>
<tr>
<td>delete snmp group</td>
<td>&lt;groupname 30&gt;</td>
</tr>
<tr>
<td>show snmp groups</td>
<td></td>
</tr>
<tr>
<td>create snmp host</td>
<td>&lt;ipaddr&gt; [v1&lt;community_string 20&gt;</td>
</tr>
<tr>
<td>delete snmp host</td>
<td>&lt;ipaddr&gt;</td>
</tr>
<tr>
<td>show snmp host</td>
<td>(&lt;ipaddr&gt;)</td>
</tr>
<tr>
<td>create trusted_host</td>
<td>&lt;ipaddr&gt; {&lt;network_address&gt;}</td>
</tr>
<tr>
<td>show trusted_host</td>
<td>(&lt;ipaddr&gt;)</td>
</tr>
<tr>
<td>delete trusted_host</td>
<td>&lt;ipaddr&gt;</td>
</tr>
<tr>
<td>enable snmp traps</td>
<td></td>
</tr>
<tr>
<td>disable snmp traps</td>
<td></td>
</tr>
<tr>
<td>enable snmp authenticate trap</td>
<td></td>
</tr>
</tbody>
</table>
Each command is listed in detail, as follows:

<table>
<thead>
<tr>
<th>Command</th>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>disable snmp</td>
<td></td>
</tr>
<tr>
<td>authenticate</td>
<td></td>
</tr>
<tr>
<td>trap</td>
<td></td>
</tr>
<tr>
<td>show snmp traps</td>
<td></td>
</tr>
<tr>
<td>config snmp</td>
<td>&lt;sw_contact 0-31&gt;</td>
</tr>
<tr>
<td>system_contact</td>
<td></td>
</tr>
<tr>
<td>config snmp</td>
<td>&lt;sw_location 0-31&gt;</td>
</tr>
<tr>
<td>system_location</td>
<td></td>
</tr>
<tr>
<td>config snmp</td>
<td>&lt;sw_name 0-31&gt;</td>
</tr>
<tr>
<td>system_name</td>
<td></td>
</tr>
</tbody>
</table>

**create snmp user**

**Purpose**
To create a new SNMP user and add the user to an SNMP group.

**Syntax**
```
create snmp user <username 24> <groupname 30> [encrypted
[by_password auth [md5 <auth_password 1-32> | sha
<auth_password 1-32>]] by_key auth [md5 <auth_key 32 or
64> sha<auth_key 40 or 72>]]
```

**Description**
The `create snmp user` command creates a new SNMP user and adds the user to an existing SNMP group.

**Parameters**
- `<username 24>` – The new SNMP username, up to 24 alphanumeric characters.
- `<groupname 30>` – The SNMP groupname the new SNMP user is associated with, up to 30 alphanumeric characters.
- `encrypted` – Allows the user to choose a type of authorization for authentication using SNMP. The user may choose:
  - `by_password` – Requires the SNMP user to enter a password for authentication and privacy. The password is defined by specifying the `auth_password` below. This method is recommended.
  - `by_key` – Requires the SNMP user to enter an encryption key for authentication and privacy. The key is defined by specifying the key in hex form below. This method is not recommended.
- `auth` - The user may also choose the type of authentication algorithms used to authenticate the snmp user. The choices are:
  - `md5` – Specifies that the HMAC-MD5-96 authentication level to be used. md5 may be utilized by entering one of the following:
    - `<auth_password 1-32>` - A string of between 1 and 32 alphanumeric characters used to authorize the agent to receive packets for the host.
  - `sha` – Specifies that the HMAC-SHA-96 authentication level will be used.
• `<auth password 1-32>` - A string of between 1 and 32 alphanumeric characters used to authorize the agent to receive packets for the host.
• `<auth_key 40 or 72>` - A string of exactly 40 or 72 alphanumeric characters, in hex form, to define the key used to authorize the agent to receive packets for the host.

Restrictions: Only administrator or operate-level users can issue this command.

Example usage:

To create an SNMP user on the Switch:

```
DGS3100# create snmp user dlink default encrypted by_password auth md5 auth_password priv none
Success.
DGS3100#
```

delete snmp user

Purpose: To remove an SNMP user from an SNMP group and also to delete the associated SNMP group.

Syntax: `delete snmp user <username 24>`

Description: The `delete snmp user` command removes an SNMP user from its SNMP group and then deletes the associated SNMP group.

Parameters: `<username 24>` - A string of up to 24 alphanumeric characters that identifies the SNMP user to be deleted.

Restrictions: Only administrator or operate-level users can issue this command.

Example usage:

To delete a previously created SNMP user on the Switch:

```
DGS3100# delete snmp user dlink
Success.
DGS3100#
```

show snmp user

Purpose: 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 or operator-level users can issue this command.
Example usage:

To display the SNMP users currently configured on the Switch:

```
DGS3100# show snmp user

Username Group Name SNMP Version Auth-Protocol
--------------- --------------- ----------- ---------------
Initial initial V3 None

Total Entries: 1

DGS3100#
```

**create snmp view**

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To assign views to community strings to limit which MIB objects an SNMP manager can access.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>`create snmp view &lt;view_name 30&gt; &lt;oid&gt; view_type [included</td>
</tr>
<tr>
<td>Description</td>
<td>The <code>create snmp view</code> command assigns views to community strings to limit which MIB objects an SNMP manager can access.</td>
</tr>
<tr>
<td>Parameters</td>
<td><code>&lt;view_name 30&gt;</code> – A string of up to 30 alphanumeric characters that identifies the SNMP view to be created.</td>
</tr>
<tr>
<td></td>
<td><code>&lt;oid&gt;</code> – The object ID that identifies an object tree (MIB tree) to be included or excluded from access by an SNMP manager.</td>
</tr>
<tr>
<td></td>
<td><code>included</code> – Includes this object in the list of objects that an SNMP manager can access.</td>
</tr>
<tr>
<td></td>
<td><code>excluded</code> – Excludes this object from the list of objects that an SNMP manager can access.</td>
</tr>
<tr>
<td>Restrictions</td>
<td>Only administrator or operate-level users can issue this command.</td>
</tr>
</tbody>
</table>

Example usage:

To create an SNMP view:

```
DGS3100# create snmp view dlinkview 1.3.6 view_type included

Success.

DGS3100#
```

**delete snmp view**

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To remove an SNMP view entry previously created on the Switch.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>`delete snmp view &lt;view_name 30&gt; [all</td>
</tr>
<tr>
<td>Description</td>
<td>The <code>delete snmp view</code> command removes an SNMP view previously created on the Switch.</td>
</tr>
<tr>
<td>Parameters</td>
<td><code>&lt;view_name 30&gt;</code> – A string of up to 30 alphanumeric characters that identifies the SNMP view to be deleted.</td>
</tr>
</tbody>
</table>
all – Specifies that all of the SNMP views on the Switch will be deleted.

<oid> – The object ID that identifies an object tree (MIB tree) that is deleted from the Switch.

Restrictions Only administrator or operate-level users can issue this command.

Example usage:
To delete a previously configured SNMP view from the Switch:

DGS3100# delete snmp view dlinkview all
Success.
DGS3100#

show snmp view

Purpose To display an SNMP view previously created on the Switch.
Syntax show snmp view {<view_name 30>}
Description The show snmp view command displays an SNMP view previously created on the Switch.
Parameters <view_name 30> – A string of up to 30 alphanumeric characters that identifies the SNMP view to be displayed.
Restrictions None.

Example usage:
To display SNMP view configuration:

DGS3100# show snmp view

<table>
<thead>
<tr>
<th>View Name</th>
<th>Subtree</th>
<th>View Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>iso</td>
<td>included</td>
</tr>
<tr>
<td>Default</td>
<td>snmpNotificationMIB</td>
<td>excluded</td>
</tr>
<tr>
<td>Default</td>
<td>snmpVacmMIB</td>
<td>excluded</td>
</tr>
<tr>
<td>Default</td>
<td>snmpCommunityMIB</td>
<td>excluded</td>
</tr>
<tr>
<td>Default</td>
<td>snmpTargetAddrTable</td>
<td>excluded</td>
</tr>
<tr>
<td>Default</td>
<td>snmpTargetParamsTable</td>
<td>excluded</td>
</tr>
<tr>
<td>Default</td>
<td>usmUser</td>
<td>excluded</td>
</tr>
<tr>
<td>Default</td>
<td>rndCommunityTable</td>
<td>excluded</td>
</tr>
<tr>
<td>DefaultSuper</td>
<td>iso</td>
<td>included</td>
</tr>
</tbody>
</table>

Total Entries: 9
DGS3100#
### create snmp community

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To create an SNMP community string to define the relationship between the SNMP manager and an SNMP agent.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>`create snmp community &lt;community_string 20&gt; view &lt;view_name 30&gt; [read_only</td>
</tr>
<tr>
<td>Description</td>
<td>The <strong>create snmp community</strong> command creates an SNMP community string and assigns access-limiting characteristics to this community string. 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:  &lt;br&gt;  - 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.  &lt;br&gt;  - An MIB view that defines the subset of all MIB objects to be accessible to the SNMP community.  &lt;br&gt;  - Read/write or read-only level permission for the MIB objects accessible to the SNMP community.</td>
</tr>
<tr>
<td>Parameters</td>
<td>- <code>&lt;community_string 20&gt;</code> – A string of up to 20 alphanumeric 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.  &lt;br&gt;  - <code>&lt;view_name 30&gt;</code> – A string of up to 30 alphanumeric characters that is used to identify the group of MIB objects that a remote SNMP manager is allowed to access on the Switch.  &lt;br&gt;  - <code>read_only</code> – Specifies that SNMP community members using the community string created with this command can only read the contents of the MIBs on the Switch.  &lt;br&gt;  - <code>read_write</code> – 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.</td>
</tr>
<tr>
<td>Restrictions</td>
<td>Only administrator or operate-level users can issue this command.</td>
</tr>
</tbody>
</table>

**Example usage:**<br> To create the SNMP community string ‘dlink:’

```
DGS3100# create snmp community dlink view ReadView read_write
Success.
DGS3100#
```

### delete snmp community

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To remove a specific SNMP community string from the Switch.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>delete snmp community &lt;community_string 20&gt;</code></td>
</tr>
<tr>
<td>Description</td>
<td>The <strong>delete snmp community</strong> command removes a previously defined SNMP community string from the Switch.</td>
</tr>
<tr>
<td>Parameters</td>
<td><code>&lt;community_string 20&gt;</code> – A string of up to 20 alphanumeric characters that is used to identify members of an SNMP community</td>
</tr>
</tbody>
</table>
to delete. 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 or operate-level users can issue this command.

Example usage:
To delete the SNMP community string ‘dlink’:

```
DGS3100# delete snmp community dlink
Success.
DGS3100#
```

**show snmp community**

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To display SNMP community strings configured on the Switch.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>show snmp community {&lt;community_string 20&gt;}</code></td>
</tr>
<tr>
<td>Description</td>
<td>The <code>show snmp community</code> command displays SNMP community strings that are configured on the Switch.</td>
</tr>
<tr>
<td>Parameters</td>
<td><code>&lt;community_string 20&gt;</code> - A string of up to 20 alphanumeric 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.</td>
</tr>
<tr>
<td>Restrictions</td>
<td>None.</td>
</tr>
</tbody>
</table>

Example usage:
To display the currently entered SNMP community strings:

```
DGS3100# show snmp community

SNMP Community Table

<table>
<thead>
<tr>
<th>Community Name</th>
<th>View Name</th>
<th>Access Right</th>
</tr>
</thead>
<tbody>
<tr>
<td>dlink</td>
<td>ReadView</td>
<td>read write</td>
</tr>
<tr>
<td>private</td>
<td>CommunityView</td>
<td>read write</td>
</tr>
<tr>
<td>public</td>
<td>CommunityView</td>
<td>read only</td>
</tr>
</tbody>
</table>

Total Entries: 3

DGS3100#
```

**config snmp engineID**

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To configure a name for the SNMP engine on the Switch.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>`config snmp engineID [default</td>
</tr>
<tr>
<td>Description</td>
<td>The <code>config snmp engineID</code> command configures a name for the SNMP engine on the Switch.</td>
</tr>
</tbody>
</table>
Parameters

- **default** - defines the automatically created engineID based on the device mac.
- `<snmp_engineID 10-64>` - A string, of between 10 and 64 alphanumeric characters, to be used to identify the SNMP engine on the Switch.

Restrictions

- Only administrator or operate-level users can issue this command.

**Example usage:**

To give the SNMP agent on the Switch the name ‘2’

```plaintext
DGS3100# config snmp engineid 2
SNMP user will be deleted!
Are you sure? (Y/N)[N] Y

Success.

DGS3100#
```

**show snmp engineID**

**Purpose**

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:

```plaintext
DGS3100# show snmp engineid

SNMP Engine ID : 0000000002

DGS3100#
```

**create snmp group**

**Purpose**

To create a new SNMP group, or a table that maps SNMP users to SNMP views.

**Syntax**

`create snmp group <groupname 30> [v1 | v2c | v3 [noauth_nopriv | auth_nopriv | auth_priv]{notify_view <view_name 30>}][read_view <view_name 30> | write_view <view_name 30>]`}

**Description**

The `create snmp group` command creates a new SNMP group, or a table that maps SNMP users to SNMP views.

**Parameters**

- `<groupname 30>` - A name of up to 30 alphanumeric characters that identifies the SNMP group the new SNMP user is to be associated
with.

- **v1** – Specifies that SNMP version 1 is to be used. The Simple Network Management Protocol (SNMP), version 1, is a network management protocol that provides a means to monitor and control network devices.

- **v2c** – Specifies that SNMP version 2c is to be used. The SNMP v2c supports both centralized and distributed network management strategies. It includes improvements in the Structure of Management Information (SMI) and adds some security features.

- **v3** – Specifies that the SNMP version 3 is to be used. SNMP v3 provides secure access to devices through a combination of authentication and encrypting packets over the network. SNMP v3 adds:
  - Message integrity – Ensures that packets have not been tampered with during transit.
  - Authentication – Determines if an SNMP message is from a valid source.
  - Encryption – Scrambles the contents of messages to prevent it from being viewed by an unauthorized source.

- **noauth_nopriv** – Specifies that there is no authorization and no encryption of packets sent between the Switch and a remote SNMP manager.

- **auth_nopriv** – Specifies that authorization is required, but there is no encryption of packets sent between the Switch and a remote SNMP manager.

- **auth_priv** – Specifies that authorization is required, and that packets sent between the Switch and a remote SNMP manager are encrypted.

- **read_view** – Specifies that the SNMP group being created can request SNMP messages.
  - `<view_name 30>` – A string of up to 30 alphanumeric characters that identifies the group of MIB objects that a remote SNMP manager is allowed to access on the Switch.

- **write_view** – Specifies that the SNMP group being created has write privileges.
  - `<view_name 30>` – A string of up to 30 alphanumeric characters that identifies the group of MIB objects that a remote SNMP manager is allowed to access on the Switch.

- **notify_view** – Specifies that the SNMP group being created can receive SNMP trap messages generated by the Switch’s SNMP agent.
  - `<view_name 30>` – A string of up to 30 alphanumeric characters that identifies the group of MIB objects that a remote SNMP manager is allowed to access on the Switch.

**Restrictions**

Only administrator or operate-level users can issue this command.

**Example usage:**

To create an SNMP group named ‘sg1’:

```
DGS3100# create snmp group sg1 v3 noauth_nopriv read_view v1 write_view v1 notify_view v1
```

Success.
**delete snmp group**

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To remove an SNMP group from the Switch.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>delete snmp group &lt;groupname 30&gt;</td>
</tr>
<tr>
<td>Description</td>
<td>The delete snmp group command removes an SNMP group from the Switch.</td>
</tr>
<tr>
<td>Parameters</td>
<td>&lt;groupname 30&gt; – A string of that identifies the SNMP group the new SNMP user will be associated with. Up to 30 alphanumeric characters.</td>
</tr>
<tr>
<td>Restrictions</td>
<td>Only administrator or operate-level users can issue this command.</td>
</tr>
</tbody>
</table>

**Example usage:**

To delete the SNMP group named ‘sg1’.

DGS3100# delete snmp group sg1

Success.

DGS3100#

**show snmp groups**

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To display the group-names of SNMP groups currently configured on the Switch. The security model, level, and status of each group are also displayed.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>show snmp groups</td>
</tr>
<tr>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td>Parameters</td>
<td>None.</td>
</tr>
<tr>
<td>Restrictions</td>
<td>None.</td>
</tr>
</tbody>
</table>

**Example usage:**

To display the currently configured SNMP groups on the Switch:

DGS3100# show snmp groups

<table>
<thead>
<tr>
<th>Group Name</th>
<th>Model</th>
<th>Level</th>
<th>ReadView</th>
<th>WriteView</th>
<th>NotifyView</th>
</tr>
</thead>
<tbody>
<tr>
<td>g1</td>
<td>V3</td>
<td>NoAuthNoPriv</td>
<td>v1</td>
<td>v1</td>
<td>v1</td>
</tr>
<tr>
<td>g2</td>
<td>V3</td>
<td>authNoPriv</td>
<td>v1</td>
<td>v1</td>
<td>v1</td>
</tr>
<tr>
<td>g3</td>
<td>V3</td>
<td>authPriv</td>
<td>v1</td>
<td>v1</td>
<td>v1</td>
</tr>
</tbody>
</table>

DGS3100#
# create snmp host

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To create a recipient of SNMP traps generated by the Switch’s SNMP agent.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>`create snmp host &lt;ipaddr&gt; [v1&lt;community_string 20&gt;</td>
</tr>
<tr>
<td>Description</td>
<td>The <code>create snmp host</code> command creates a recipient of SNMP traps generated by the Switch’s SNMP agent.</td>
</tr>
<tr>
<td>Parameters</td>
<td><code>&lt;ipaddr&gt;</code> – The IP address of the remote management station to serve as the SNMP host for the Switch.</td>
</tr>
<tr>
<td></td>
<td><code>v1</code> – Specifies that SNMP version 1 is to 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.</td>
</tr>
<tr>
<td></td>
<td><code>v2c</code> – Specifies that SNMP version 2c is to 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.</td>
</tr>
<tr>
<td></td>
<td><code>v3</code> – Specifies that the SNMP version 3 is to be used. SNMP v3 provides secure access to devices through a combination of authentication and encrypting packets over the network. SNMP v3 adds:</td>
</tr>
<tr>
<td></td>
<td>• Message integrity – ensures that packets have not been tampered with during transit.</td>
</tr>
<tr>
<td></td>
<td>• Authentication – determines if an SNMP message is from a valid source.</td>
</tr>
<tr>
<td></td>
<td>• Encryption – scrambles the contents of messages to prevent it being viewed by an unauthorized source.</td>
</tr>
<tr>
<td></td>
<td><code>&lt;community_string 20&gt;</code> – A string of up to 20 alphanumeric characters that identifies 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.</td>
</tr>
<tr>
<td></td>
<td><code>noauth_nopriv</code> – Specifies that there is no authorization and no encryption of packets sent between the Switch and a remote SNMP manager.</td>
</tr>
<tr>
<td></td>
<td><code>auth_nopriv</code> – Specifies that authorization is required, but there is no encryption of packets sent between the Switch and a remote SNMP manager.</td>
</tr>
<tr>
<td></td>
<td><code>auth_priv</code> – Specifies that authorization is required, and that packets sent between the Switch and a remote SNMP manager are encrypted.</td>
</tr>
<tr>
<td></td>
<td><code>&lt;auth_string 24&gt;</code> – A string of up to 24 alphanumeric characters used in SNMP v3 to authorize a remote SNMP manager to access the Switch’s SNMP agent.</td>
</tr>
<tr>
<td>Restrictions</td>
<td>Only Administrator and oper-level users can issue this command</td>
</tr>
</tbody>
</table>

## Example usage:
To create an SNMP host to receive SNMP messages:

```
DGS3100# create snmp host 10.48.74.100 v3 auth_priv public
```
delete snmp host

Purpose: 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 receives SNMP traps generated by the Switch’s SNMP agent.

Restrictions: Only Administrator or operator-level users can issue this command.

Example usage:
To delete an SNMP host entry:

DGS3100# delete snmp host 10.48.74.100
Success.
DGS3100#

show snmp host

Purpose: 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 generated by the Switch’s SNMP agent.

Parameters:
- <ipaddr> - The IP address of a remote SNMP manager that receives SNMP traps generated by the Switch’s SNMP agent.

Restrictions: None.

Example usage:
To display the currently configured SNMP hosts on the Switch:

DGS3100# show snmp host

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

Purpose To create a trusted host.

Syntax `create trusted_host <ipaddr> <network_address>`

Description The `create trusted_host` command creates a trusted host. The Switch allows specifying up to ten IP addresses that are allowed to manage the Switch via in-band based management software. These IP addresses must be members of the Management VLAN. If no IP addresses are specified, then there is nothing to prevent any IP address from accessing the Switch, provided the user knows the Username and Password.

Parameters
- `<ipaddr>` - The IP address of the trusted host to be created.
- `<network_address>` - The network address of the trusted host to be created. This parameter is optional. If not specified, the default subnet mask is 255.255.255.0.

Restrictions Only administrator or operator level users can issue this command.

Example usage:

To create the trusted host:

```
DGS3100# create trusted_host 10.6.150.49 255.255.255.0
Success.
DGS-3100#
```

show trusted_host

Purpose To display a list of trusted hosts entered on the Switch using the `create trusted_host` command above.

Syntax `show trusted_host {<ipaddr>}`

Description The `show trusted_host` command displays a list of trusted hosts entered on the Switch using the `create trusted_host` command above.

Parameters `<ipaddr>` - The IP address of the trusted host.

Restrictions None.

Example usage:

To display the list of trusted hosts:
DGS-3100# show trusted_host

Management Stations
IP Address
--------------
10.6.150.49

Total Entries: 1

DGS-3100#

<table>
<thead>
<tr>
<th>delete trusted_host</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td><strong>Syntax</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td><strong>Parameters</strong></td>
</tr>
<tr>
<td><strong>Restrictions</strong></td>
</tr>
</tbody>
</table>

**Example usage:**
To delete a trusted host with an IP address 10.48.74.121:

DGS3100# delete trusted_host 10.48.74.121
Success.
DGS3100#

<table>
<thead>
<tr>
<th>enable snmp traps</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td><strong>Syntax</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td><strong>Parameters</strong></td>
</tr>
<tr>
<td><strong>Restrictions</strong></td>
</tr>
</tbody>
</table>

**Example usage:**
To enable SNMP trap support on the Switch:

DGS3100# enable snmp traps
Success.
DGS3100#
### disable snmp traps

**Purpose**
To disable SNMP trap support on the Switch.

**Syntax**
```
disable snmp traps
```

**Description**
The `disable snmp traps` command disables SNMP trap support on the Switch.

**Parameters**
None.

**Restrictions**
Only Administrator or operator-level users can issue this command.

**Example usage:**
To prevent SNMP traps from being sent from the Switch:

```
DGS3100# disable snmp traps
Success.
DGS3100#
```

### enable snmp authenticate trap

**Purpose**
To enable SNMP authentication trap support.

**Syntax**
```
enable snmp authenticate trap
```

**Description**
The `enable snmp authenticate trap` command enables SNMP authentication trap support on the Switch.

**Parameters**
None.

**Restrictions**
Only Administrator or operator-level users can issue this command.

**Example usage:**
To turn on SNMP authentication trap support:

```
DGS3100# enable snmp authenticate trap
Success.
DGS3100#
```

### disable snmp authenticate trap

**Purpose**
To disable SNMP authentication trap support.

**Syntax**
```
disable snmp authenticate trap
```

**Description**
The `disable snmp authenticate trap` command disables SNMP authentication trap support on the Switch.

**Parameters**
None.

**Restrictions**
Only Administrator or operator-level users can issue this command.

**Example usage:**
To disable the SNMP authentication trap support:

```
DGS3100# disable snmp authenticate trap
```

### show snmp traps

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To display SNMP trap support status on the Switch.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>show snmp traps</code></td>
</tr>
<tr>
<td>Description</td>
<td>The <code>show snmp traps</code> command displays the SNMP trap support status currently configured on the Switch.</td>
</tr>
<tr>
<td>Parameters</td>
<td>None.</td>
</tr>
<tr>
<td>Restrictions</td>
<td>None</td>
</tr>
</tbody>
</table>

**Example usage:**

To view the current SNMP trap support:

```
DGS3100# show snmp traps
SNMP Traps : enabled
Authenticate Trap : enabled

DGS3100#
```

### config snmp system_contact

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To enter identification information of a contact person who is responsible for the Switch.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>config snmp system_contact &lt;sw_contact 0-31&gt;</code></td>
</tr>
<tr>
<td>Description</td>
<td>The <code>config snmp system_contact</code> command enters the name and/or other information to identify a contact person who is responsible for the Switch. A maximum of 31 characters can be used.</td>
</tr>
<tr>
<td>Parameters</td>
<td><code>&lt;sw_contact 0-31&gt;</code> - A maximum of 31 characters is allowed. A NULL string is accepted if there is no contact.</td>
</tr>
<tr>
<td>Restrictions</td>
<td>Only Administrator or operator-level users can issue this command</td>
</tr>
</tbody>
</table>

**Example usage:**

To configure the Switch contact to ‘MIS Department II’:

```
DGS3100# config snmp system_contact MIS Department II
Success.

DGS3100#
```
**config snmp system_location**

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To enter a description of the location of the Switch.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>config snmp system_location &lt;sw_location 0-31&gt;</code></td>
</tr>
<tr>
<td>Description</td>
<td>The <code>config snmp system_location</code> command enters a description of the location of the Switch. A maximum of 31 characters can be used.</td>
</tr>
<tr>
<td>Parameters</td>
<td><code>&lt;sw_location 0-31&gt;</code> - A maximum of 31 characters is allowed. A NULL string is accepted if there is no location desired.</td>
</tr>
<tr>
<td>Restrictions</td>
<td>Only Administrator or operator-level users can issue this command</td>
</tr>
</tbody>
</table>

**Example usage:**

To configure the Switch location for ‘HQ 5F’:

```
DGS3100# config snmp system_location HQ 5F
Success.
DGS3100#
```

**config snmp system_name**

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To define the name for the Switch.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>config snmp system_name &lt;sw_name 0-31&gt;</code></td>
</tr>
<tr>
<td>Description</td>
<td>The <code>config snmp system_name</code> command defines the name of the Switch.</td>
</tr>
<tr>
<td>Parameters</td>
<td><code>&lt;sw_name 0-31&gt;</code> - A maximum of 31 characters is allowed. A NULL string is accepted if no name is desired.</td>
</tr>
<tr>
<td>Restrictions</td>
<td>Only Administrator or operator-level users can issue this command</td>
</tr>
</tbody>
</table>

**Example usage:**

To configure the Switch name as ‘DGS-3100 Switch’:

```
DGS3100# config snmp system_name DGS-3100 Switch
Success.
DGS-3100 Switch#
```
DOWNLOAD/UPLOAD COMMANDS

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>download</td>
<td>configuration &lt;ipaddr&gt; &lt;path_filename 1-64&gt; [firmware &lt;ipaddr&gt; &lt;path_filename 1-64&gt;</td>
</tr>
<tr>
<td>upload</td>
<td>configuration &lt;ipaddr&gt; &lt;path_filename 1-64&gt; {startup</td>
</tr>
<tr>
<td>config dhcp_auto enable</td>
<td>[ enable</td>
</tr>
<tr>
<td>show dhcp_auto</td>
<td></td>
</tr>
<tr>
<td>config firmware</td>
<td>{unit &lt;unit_id 1-6&gt;} image_id &lt;init 1-2&gt;</td>
</tr>
<tr>
<td>show firmware info</td>
<td></td>
</tr>
</tbody>
</table>

Each command is listed in detail, as follows:

**download**

**Purpose**: To download and install a firmware, boot, or switch configuration file from a TFTP server.

**Syntax**: `download [configuration <ipaddr> <path_filename 1-64> firmware <ipaddr> <path_filename 1-64> | boot <ipaddr> <path_filename 1-64> | {startup | running}]`

**Description**: The `download` command downloads a firmware, boot, or switch configuration file from a TFTP server.

**Parameters**

- `firmware` – Downloads and installs firmware on the Switch from a TFTP server.
- `boot` – Downloads a boot file from a TFTP server.
- `configuration` – Downloads a switch configuration file from a TFTP server.
- `<ipaddr>` – The IP address of the TFTP server.
- `<path_filename 64>` – The DOS path and filename of the firmware or switch configuration file, up to 64 characters, on the TFTP server. For example, C:\31xx.had.
- `startup` – Indicates the Configuration file is to be downloaded to the startup config.
- `running` – Indicates the Configuration file is to be downloaded to the running config.

**Restrictions**: None.

**Example usage**: To download a firmware file:
To download a configuration file:

```
DGS3100# download configuration 10.48.74.121 c:\cfg\setting.txt
Overwrite file [startup-config]?[Yes/press any key for no]....
01-Jan-200003:19:46%COPY-I-FILECPY:FilesCopy-source URL tftp://10.48.74.121/1.txt destination URL flash://startup-config
Success.
Success.
.....01-Jan-2000 03:18:40 %COPY-N-TRAP: The copy operation was completed successfully!
Copy: 267 bytes copied in 00:00:08 [hh:mm:ss]
DGS3100#
```

### upload

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To upload the current switch settings to a TFTP server.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax</strong></td>
<td>`upload configuration &lt;ipaddr&gt; &lt;path_filename 1-64&gt; {startup</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>The <code>upload</code> command uploads the Switch’s current settings to a TFTP server.</td>
</tr>
<tr>
<td><strong>Parameters</strong></td>
<td><code>configuration</code> – Specifies that the Switch’s current settings are to be uploaded to the TFTP server.</td>
</tr>
<tr>
<td></td>
<td><code>&lt;ipaddr&gt;</code> – The IP address of the TFTP server. The TFTP server must be on the same IP subnet as the Switch.</td>
</tr>
<tr>
<td></td>
<td><code>&lt;path_filename 1-64&gt;</code> – The location of the Switch configuration file on the TFTP server.</td>
</tr>
</tbody>
</table>
**startup** – Indicates the Startup Configuration file is to be uploaded.

**running** – Indicates the Running Configuration file is to be uploaded.

Restrictions None.

**Example usage:**

```
DGS3100# upload configuration 1.1.1.23 1\running—config
01–Jan–2000 01:26:16 %COPY–W–TRAP: The copy operation was completed successfully!
158 bytes copied in 00:00:05 [hh:mm:ss]
DGS3100#
```

**config dhcp_auto enable**

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To automatically update the switch’s firmware and configuration files via the web, using options 66 and 67 of the DHCP packets.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>`config dhcp_auto [enable</td>
</tr>
<tr>
<td>Description</td>
<td>The <strong>config dhcp_auto enable</strong> command enables/disables Auto update feature.</td>
</tr>
<tr>
<td>Parameters</td>
<td><code>enable</code> – Enables the Auto-Update feature.</td>
</tr>
<tr>
<td></td>
<td><code>disable</code> – Disables the Auto-Update feature.</td>
</tr>
<tr>
<td>Restrictions</td>
<td>None.</td>
</tr>
</tbody>
</table>

**Example usage:**

To automatically update the switch’s firmware and configuration files:

```
DGS3100# config dhcp_auto enable

The configuration will take place on the next time the device will get DHCP address.

Success
DGS3100#
```

**show dhcp_auto**

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To display the current state of the auto update feature.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>show dhcp_auto</code></td>
</tr>
<tr>
<td>Description</td>
<td>The <strong>show dhcp_auto</strong> command displays the current state of the auto update feature.</td>
</tr>
<tr>
<td>Parameters</td>
<td>None.</td>
</tr>
<tr>
<td>Restrictions</td>
<td>None.</td>
</tr>
</tbody>
</table>

**Example usage:**
To display the current state of the auto update feature:

DGS3100# show dhcp_auto
Dhcp auto update status: Disable
DGS3100#

**config firmware**

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To specify the system image that the device will load at reboot.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>config firmware {unit &lt;unit_id 1-6&gt;} image_id &lt;init 1-2&gt;</code></td>
</tr>
<tr>
<td>Description</td>
<td>The <code>config firmware</code> command specifies the system image that the device loads at startup.</td>
</tr>
</tbody>
</table>
| Parameters | `unit` − Specifies the unit ID number. (Range: 1-6)  
`image_id` − Specifies the system image ID number. |
| Restrictions | None. |

**Example usage:**

To specify the system image:

DGS3100# config firmware unit 1 image_id 1
Success
DGS3100#

**show firmware information**

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To display the active system image file loaded by the device.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>show firmware information</code></td>
</tr>
<tr>
<td>Description</td>
<td>The <code>show firmware information</code> command displays the currently stored image files, and indicates those that are currently active.</td>
</tr>
<tr>
<td>Parameters</td>
<td>None</td>
</tr>
<tr>
<td>Restrictions</td>
<td>None.</td>
</tr>
</tbody>
</table>

**Example usage:**

To display the active system image file:

DGS3100# show firmware information

<table>
<thead>
<tr>
<th>Unit</th>
<th>Image</th>
<th>Version</th>
<th>Update Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>*2</td>
<td>2.00.10</td>
<td>20-Nov-2007 15:21:24</td>
</tr>
<tr>
<td>4</td>
<td>*2</td>
<td>2.00.10</td>
<td>20-Nov-2007 15:21:24</td>
</tr>
<tr>
<td>5</td>
<td>*2</td>
<td>2.00.10</td>
<td>20-Nov-2007 15:21:24</td>
</tr>
</tbody>
</table>

DGS3100#
NETWORK MONITORING COMMANDS

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>show packet ports</td>
<td>&lt;portlist&gt;</td>
</tr>
<tr>
<td>show error ports</td>
<td>&lt;portlist&gt;</td>
</tr>
<tr>
<td>show utilization</td>
<td>[ports</td>
</tr>
<tr>
<td>clear counters</td>
<td></td>
</tr>
<tr>
<td>clear log</td>
<td></td>
</tr>
<tr>
<td>show log</td>
<td>{index &lt;value&gt;}</td>
</tr>
<tr>
<td>enable syslog</td>
<td></td>
</tr>
<tr>
<td>disable syslog</td>
<td></td>
</tr>
<tr>
<td>show syslog</td>
<td></td>
</tr>
<tr>
<td>create syslog host</td>
<td>&lt;index 1-4&gt; ipaddr &lt;ipaddr&gt; {severity [informational</td>
</tr>
<tr>
<td>config syslog host</td>
<td>[all</td>
</tr>
<tr>
<td>delete syslog host</td>
<td>[&lt;index 1-4&gt;</td>
</tr>
<tr>
<td>show syslog host</td>
<td>{&lt;index 1-4&gt;}</td>
</tr>
</tbody>
</table>

Each command is listed in detail, as follows:

**show packet ports**

**Purpose**
To display statistics about the packets sent and received in frames per second by the Switch.

**Syntax**
```
show packet ports <portlist>
```

**Description**
The `show packet ports` command displays statistics about packets sent and received by ports specified in the port list. The results are separated into three tables, labeled A, B, and C in the window below. Table A is relevant to the size of the packets, Table B is relevant to the type of packets and Table C is relevant to the type of frame associated with these packets.

**Parameters**
- `<portlist>` - A port or range of ports whose statistics are to be displayed.

**Restrictions**
None.
Example usage:

To display the packets analysis for port 7:

```
DGS3100# show packet ports 7
Port number : 7               A                                                      B
Frame Size     Frame Counts   Frames/sec   Frame Type  Total    Total/sec
------------------   --------------------   ----------------   -----------------   -------    -------------
64                     3275                  10                   RX Bytes       408973  1657
65-127              755                    10                   RX Frames    4395      19
128-255               316                    1                  TX Bytes        7918       178
256-511            145                    0                  TX Frames     111         2
1024-1518            0                    0
1519-10240         0                        0
C
Unicast Rx      152                    1
Multicast Rx    557                   2
Broadcast Rx  3686                 16
```

More: <space>, Quit: q, One line: <return>

---

**show error ports**

Purpose: To display the error statistics for a port or a range of ports.

Syntax: `show error ports <portlist>`

Description: The `show error ports` command displays all of the packet error statistics collected and logged by the Switch for a given port list.

Parameters: `<portlist>` - A port or range of ports whose error statistics are to be displayed.

Restrictions: None.

Example usage:

To display the errors of port 3:

```
DGS3100# show errors port 3
Port number : 3
Error Type      RX Frames  Error Type            TX Frames
---------------  ----------  ---------------------  ---------
CRC Error       0          Excessive Deferra     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
DGS3100#
```
**show utilization**

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To display real-time port utilization statistics.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>`show utilization [ports</td>
</tr>
<tr>
<td>Description</td>
<td>The <code>show utilization</code> command displays the real-time port utilization statistics in bits per second (bps) for the Switch.</td>
</tr>
<tr>
<td>Parameters</td>
<td>`[ports</td>
</tr>
<tr>
<td>Restrictions</td>
<td>None.</td>
</tr>
</tbody>
</table>

**Example usage:**

To display the port utilization statistics:

```
DGS3100# show utilization

<table>
<thead>
<tr>
<th>Port</th>
<th>TX/sec</th>
<th>RX/sec</th>
<th>Util</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>8</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>9</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>10</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>11</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>12</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>13</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>14</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>15</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>16</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>17</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>18</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>19</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```

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

**clear counters**

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To clear the Switch’s statistics counters.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>clear counters</code></td>
</tr>
<tr>
<td>Description</td>
<td>The <code>clear counters</code> command clears the counters used by the Switch to compile statistics.</td>
</tr>
<tr>
<td>Parameters</td>
<td>None.</td>
</tr>
<tr>
<td>Restrictions</td>
<td>Only Administrator or operator-level users can issue this command.</td>
</tr>
</tbody>
</table>

**Example usage:**

To clear the Switch’s statistics counters:
To clear the counters:

```
DGS3100# clear counters
Success.
DGS3100#
```

**clear log**

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To clear the Switch’s history log.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>clear log</td>
</tr>
<tr>
<td>Description</td>
<td>The <code>clear log</code> command clears the Switch’s history log.</td>
</tr>
<tr>
<td>Parameters</td>
<td>None.</td>
</tr>
<tr>
<td>Restrictions</td>
<td>Only administrator-level users can issue this command.</td>
</tr>
</tbody>
</table>

**Example usage:**

To clear the log information:

```
DGS3100# clear log
Success.
DGS3100#
```

**show log**

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To display the Switch history log.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>show log {index &lt;value&gt;}</code></td>
</tr>
<tr>
<td>Description</td>
<td>The <code>show log</code> command displays the contents of the Switch’s history log.</td>
</tr>
<tr>
<td>Parameters</td>
<td><code>index &lt;value&gt;</code> – The number of entries in the history log to display.</td>
</tr>
<tr>
<td>Restrictions</td>
<td>None.</td>
</tr>
</tbody>
</table>

**Example usage:**

To display the Switch history log:

```
DGS3100# show log

<table>
<thead>
<tr>
<th>Index</th>
<th>Time</th>
<th>Log Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>03-Jan-2000 17:48:21</td>
<td>%AAA-I-CONNECT: User CLI session for user admin over telnet, source 10.6.150.34 destination 10.6.41.37 ACCEPTED</td>
</tr>
<tr>
<td>2</td>
<td>03-Jan-2000 17:48:02</td>
<td>%AAA-I-DISCONNECT: User CLI session for user admin over telnet, source 10.6.150.34 destination 10.6.41.37 TERMINATED. The Telnet/SSH session may still be connected.</td>
</tr>
<tr>
<td>3</td>
<td>03-Jan-2000 17:38:46</td>
<td>%AAA-I-DISCONNECT: User CLI session for user admin o</td>
</tr>
</tbody>
</table>
```
enable syslog

Purpose: 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 or operator-level users can issue this command.

Example usage:

To enable the syslog function on the Switch:

```
DGS3100# enable syslog
Success.
DGS3100#
```

disable syslog

Purpose: To disable the system log from being sent to a remote host.

Syntax: 

```
disable syslog
```

Description: The `disable syslog` command disables the system log from being sent to a remote host.

Parameters: None.

Restrictions: Only Administrator or operator-level users can issue this command.

Example usage:

To disable the syslog function on the Switch:

```
DGS3100# disable syslog
Success.
DGS3100#
```
### show syslog

**Purpose**
To display the syslog protocol status.

**Syntax**
```
show syslog
```

**Description**
The `show syslog` command displays the syslog status (enabled or disabled).

**Parameters**
None.

**Restrictions**
None.

**Example usage:**
To display the current status of the syslog function:

```
DGS3100# show syslog
Syslog Global State: Enabled
DGS3100#
```

### create syslog host

**Purpose**
To create a new syslog host.

**Syntax**
```
create syslog host <index 1-4> ipaddress <ipaddr> {severity [informational | warning | all] | facility [local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7] | udp_port <udp_port_number>}
```

**Description**
The `create syslog host` command creates a new syslog host.

**Parameters**
- `<index 1-4>` – The syslog host index id. There are four available indices, numbered 1 to 4.
- `ipaddress <ipaddr>` – The IP address of the remote host to which syslog messages are to be sent.
- `severity` – The message severity level indicator. These are described in the table below (Bold font indicates that the corresponding severity level is currently supported on the Switch):

<table>
<thead>
<tr>
<th>Numerical Code</th>
<th>Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Emergency: system is unusable</td>
</tr>
<tr>
<td>1</td>
<td>Alert: action must be taken immediately</td>
</tr>
<tr>
<td>2</td>
<td>Critical: critical conditions</td>
</tr>
<tr>
<td>3</td>
<td>Error: error conditions</td>
</tr>
<tr>
<td><strong>4</strong></td>
<td>Warning: warning conditions</td>
</tr>
<tr>
<td>5</td>
<td>Notice: normal but significant condition</td>
</tr>
<tr>
<td><strong>6</strong></td>
<td>Informational: informational messages</td>
</tr>
<tr>
<td>7</td>
<td>Debug: debug-level messages</td>
</tr>
</tbody>
</table>

- `facility` – The syslog facility indicator.
- `udp_port <udp_port_number>` – The UDP port number of the remote host.
informational – Specifies that informational messages are to be sent to the remote host. This corresponds to number 6 from the list above.

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

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

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

<table>
<thead>
<tr>
<th>Numerical Code</th>
<th>Facility</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>kernel messages</td>
</tr>
<tr>
<td>1</td>
<td>user-level messages</td>
</tr>
<tr>
<td>2</td>
<td>mail system</td>
</tr>
<tr>
<td>3</td>
<td>system daemons</td>
</tr>
<tr>
<td>4</td>
<td>security/authorization messages</td>
</tr>
<tr>
<td>5</td>
<td>messages generated internally by syslog</td>
</tr>
<tr>
<td>6</td>
<td>line printer subsystem</td>
</tr>
<tr>
<td>7</td>
<td>network news subsystem</td>
</tr>
<tr>
<td>8</td>
<td>UUCP subsystem</td>
</tr>
<tr>
<td>9</td>
<td>clock daemon</td>
</tr>
<tr>
<td>10</td>
<td>security/authorization messages</td>
</tr>
<tr>
<td>11</td>
<td>FTP daemon</td>
</tr>
<tr>
<td>12</td>
<td>NTP subsystem</td>
</tr>
<tr>
<td>13</td>
<td>log audit</td>
</tr>
<tr>
<td>14</td>
<td>log alert</td>
</tr>
<tr>
<td>15</td>
<td>clock daemon</td>
</tr>
<tr>
<td>16</td>
<td>local use 0 (local0)</td>
</tr>
<tr>
<td>17</td>
<td>local use 1 (local1)</td>
</tr>
<tr>
<td>18</td>
<td>local use 2 (local2)</td>
</tr>
<tr>
<td>19</td>
<td>local use 3 (local3)</td>
</tr>
<tr>
<td>20</td>
<td>local use 4 (local4)</td>
</tr>
<tr>
<td>21</td>
<td>local use 5 (local5)</td>
</tr>
<tr>
<td>22</td>
<td>local use 6 (local6)</td>
</tr>
<tr>
<td>23</td>
<td>local use 7 (local7)</td>
</tr>
</tbody>
</table>

local0 – Specifies that local use 0 messages are to be sent to the remote host. This corresponds to number 16 from the list above.

local1 – Specifies that local use 1 messages are to be sent to the remote host. This corresponds to number 17 from the list above.

local2 – Specifies that local use 2 messages are to be sent to the remote host. This corresponds to number 18 from the list above.
local3 − Specifies that local use 3 messages are to be sent to the remote host. This corresponds to number 19 from the list above.
local4 − Specifies that local use 4 messages are to be sent to the remote host. This corresponds to number 20 from the list above.
local5 − Specifies that local use 5 messages are to be sent to the remote host. This corresponds to number 21 from the list above.
local6 − Specifies that local use 6 messages are to be sent to the remote host. This corresponds to number 22 from the list above.
local7 − Specifies that local use 7 messages is sent to the remote host. This corresponds to number 23 from the list above.

udp_port <udp_port_number> − Specifies the UDP port number that the syslog protocol is to use to send messages to the remote host.

state [enable | disable] − Allows the sending of syslog messages to the remote host, specified above, to be enabled and disabled.

Restrictions Only Administrator or operator-level users can issue this command.

Example usage:
To create syslog host:

```
DGS3100# create syslog host 1 ipaddress 10.53.13.94 severity all facility local0
Success.
DGS3100#
```

---

### config syslog host

**Purpose**
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 <udp_port_number> | ipaddress <ipaddr>
```

**Description**
The `config syslog host` command configures the syslog protocol to send system log information to a remote host.

**Parameters**
- `all` − Specifies that the command applies to all hosts.
- `<index 1-4>` − Specifies that the command applies to an index of hosts. There are four available indices, numbered 1 to 4.
- `ipaddress <ipaddr>` − The IP address of the remote host to which syslog messages are to be sent.
- `severity` − The message severity level indicator. These are described in the following table (Bold font indicates that the corresponding severity level is currently supported on the Switch):

<table>
<thead>
<tr>
<th>Code</th>
<th>Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Emergency: system is unusable</td>
</tr>
<tr>
<td>1</td>
<td>Alert: action must be taken immediately</td>
</tr>
<tr>
<td>2</td>
<td>Critical: critical conditions</td>
</tr>
</tbody>
</table>
3                      Error: error conditions
4                      Warning: warning conditions
5                      Notice: normal but significant condition
6                      Informational: informational messages
7                      Debug: debug-level messages

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

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

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

*facility* – Some of the operating system daemons and processes have been assigned Facility values. Processes and daemons that have not been explicitly assigned a Facility may use any of the ‘local use’ facilities or they may use the ‘user-level’ Facility. Those Facilities that have been designated are shown in the following:

Bold font indicates the facility values that the Switch currently supports.

<table>
<thead>
<tr>
<th>Numerical Code</th>
<th>Facility</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>kernel messages</td>
</tr>
<tr>
<td>1</td>
<td>user-level messages</td>
</tr>
<tr>
<td>2</td>
<td>mail system</td>
</tr>
<tr>
<td>3</td>
<td>system daemons</td>
</tr>
<tr>
<td>4</td>
<td>security/authorization messages</td>
</tr>
<tr>
<td>5</td>
<td>messages generated internally by syslog</td>
</tr>
<tr>
<td>6</td>
<td>line printer subsystem</td>
</tr>
<tr>
<td>7</td>
<td>network news subsystem</td>
</tr>
<tr>
<td>8</td>
<td>UUCP subsystem</td>
</tr>
<tr>
<td>9</td>
<td>clock daemon</td>
</tr>
<tr>
<td>10</td>
<td>security/authorization messages</td>
</tr>
<tr>
<td>11</td>
<td>FTP daemon</td>
</tr>
<tr>
<td>12</td>
<td>NTP subsystem</td>
</tr>
<tr>
<td>13</td>
<td>log audit</td>
</tr>
<tr>
<td>14</td>
<td>log alert</td>
</tr>
<tr>
<td>15</td>
<td>clock daemon</td>
</tr>
<tr>
<td>16</td>
<td>local use 0 (local0)</td>
</tr>
<tr>
<td>17</td>
<td>local use 1 (local1)</td>
</tr>
<tr>
<td>18</td>
<td>local use 2 (local2)</td>
</tr>
<tr>
<td>19</td>
<td>local use 3 (local3)</td>
</tr>
<tr>
<td>20</td>
<td>local use 4 (local4)</td>
</tr>
<tr>
<td>21</td>
<td>local use 5 (local5)</td>
</tr>
<tr>
<td>22</td>
<td>local use 6 (local6)</td>
</tr>
<tr>
<td>23</td>
<td>local use 7 (local7)</td>
</tr>
</tbody>
</table>

*local0* – Specifies that local use 0 messages are to be sent to the
remote host. This corresponds to number 16 from the list above.

- `local1` - Specifies that local use 1 messages are to be sent to the remote host. This corresponds to number 17 from the list above.
- `local2` - Specifies that local use 2 messages are to be sent to the remote host. This corresponds to number 18 from the list above.
- `local3` - Specifies that local use 3 messages are to be sent to the remote host. This corresponds to number 19 from the list above.
- `local4` - Specifies that local use 4 messages are to be sent to the remote host. This corresponds to number 20 from the list above.
- `local5` - Specifies that local use 5 messages are to be sent to the remote host. This corresponds to number 21 from the list above.
- `local6` - Specifies that local use 6 messages are to be sent to the remote host. This corresponds to number 22 from the list above.
- `local7` - Specifies that local use 7 messages are to be sent to the remote host. This corresponds to number 23 from the list above.

- `udp_port <udp_port_number>` - Specifies the UDP port number that the syslog protocol is to use to send messages to the remote host.
- `ipaddress <ipaddr>` - Specifies the IP address of the remote host to which syslog messages are to 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 or operator-level users can issue this command.

**Example usage:**

To configure a syslog host:

```
DGS3100# config syslog host all severity all facility local0
Success.
DGS3100#
```

---

**delete syslog host**

Purpose

To remove a previously configured syslog host from the Switch.

Syntax

```
delete syslog host [index 1-4] | all
```

Description

The `delete syslog host` command removes a previously configured syslog host from the Switch.

Parameters

- `<index 1-4>` - The syslog host index id. There are four available indices, numbered 1 to 4.
- `all` - Specifies that the command applies to all hosts.

Restrictions

Only Administrator or operator-level users can issue this command.

**Example usage:**

To delete a previously configured syslog host:

```
DGS3100# delete syslog host 4
Success.
DGS3100#
```
### show syslog host

**Purpose**
To display the syslog hosts currently configured on the Switch.

**Syntax**
`show syslog host {<index 1-4>}`

**Description**
The `show syslog host` command displays the syslog hosts that are currently configured on the Switch.

**Parameters**
- `<index 1-4>` – The syslog host index id. There are four available indices, numbered 1 to 4.

**Restrictions**
None.

#### Example usage:

To show Syslog host information:

```
DGS3100# show syslog host

Syslog Global State: Disabled

<table>
<thead>
<tr>
<th>Host Id</th>
<th>Host IP address</th>
<th>Severity</th>
<th>Facility</th>
<th>UDP port</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>10.1.1.2</td>
<td>All</td>
<td>Local0</td>
<td>514</td>
</tr>
<tr>
<td>2</td>
<td>10.40.2.3</td>
<td>All</td>
<td>Local0</td>
<td>514</td>
</tr>
<tr>
<td>3</td>
<td>10.21.13.1</td>
<td>All</td>
<td>Local0</td>
<td>514</td>
</tr>
</tbody>
</table>

Total Entries: 3
```

DGS3100#
The Spanning Tree commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

<table>
<thead>
<tr>
<th>Command</th>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>config stp</td>
<td>{maxage &lt;value 6-40&gt;</td>
</tr>
<tr>
<td>config stp version</td>
<td>[mstp</td>
</tr>
<tr>
<td>enable stp</td>
<td></td>
</tr>
<tr>
<td>disable stp</td>
<td></td>
</tr>
<tr>
<td>show stp</td>
<td></td>
</tr>
<tr>
<td>show stp ports</td>
<td>{&lt;portlist&gt;</td>
</tr>
<tr>
<td>show stp instance_id</td>
<td>&lt;value 0-15&gt;</td>
</tr>
<tr>
<td>show stp mst_config_id</td>
<td></td>
</tr>
<tr>
<td>config stp instance_id</td>
<td>&lt;value 1-15&gt; [add_vlan</td>
</tr>
<tr>
<td>config stp priority</td>
<td>&lt;value 0-61440&gt; instance_id &lt;value 0-15&gt;</td>
</tr>
<tr>
<td>config stp mst_config_id</td>
<td>{revision_level &lt;int 0-65535&gt;</td>
</tr>
<tr>
<td>config stp mst_ports</td>
<td>[&lt;portlist&gt;</td>
</tr>
</tbody>
</table>

Each command is listed in detail, as follows:

**config stp**

**Purpose**: To setup STP, RSTP and MSTP on the Switch.

**Syntax**

```
config stp {maxage <value 6-40> | maxhops <value 1-20> | hellotime <value 1-10> | forwarddelay <value 4-30> | fbpdu [enable | disable] | lbd [enable | disable] | lbd_recover_time <value 30-86400> ]
```

**Description**: The `config stp` command configures the Spanning Tree Protocol (STP) for the entire switch. All commands here are implemented for the STP version that is currently set on the Switch.

**Parameters**

- `maxage <value 6-40>` - This value may be set to ensure that old information does not endlessly circulate through redundant paths in the network, preventing the effective propagation of the new information. Set by the Root Bridge, this value aids in determining
that the Switch has spanning tree configuration values consistent
with other devices on the bridged LAN. If the value ages out and a
BPDU has still not been received from the Root Bridge, the Switch
starts sending its own BPDU to all other switches for permission to
become the Root Bridge. If your switch has the lowest priority, it
becomes the Root Bridge. The user may choose a time between 6
and 40 seconds. The default value is 20.

**maxhops <value 1-20>** – The number of hops between devices in a
spanning tree region before the BPDU (bridge protocol data unit)
packet sent by the Switch will be discarded. Each switch on the hop
count will reduce the hop count by one until the value reaches zero.
The Switch will then discard the BDPU packet and the information
held for the port will age out. The value may be between 1 and 20.
The default is 20.

**hellotime <value 1-10>** – The user may set the time interval between
transmission of configuration messages by the root device in STP,
or by the designated router, thus stating that the Switch is still
functioning. The value may be between 1 and 10 seconds. The
default value is 2 seconds.

**forwarddelay <value 4-30>** – The amount of time (in seconds) that
the root device will wait before changing from Blocking to Listening,
and from Listening to Learning states. The value may be between 4
and 30 seconds. The default is 15 seconds.

**fbpdu [enable | disable]** – Allows the forwarding of STP BPDU
packets from other network devices when STP is disabled on the
Switch. The default is disable.

**lbd [enable | disable]** – To enable or disable the loopback Detection
feature.

**lbd_recover_timer [<value 30-86400>]** – Time in second for the loop
detection recovery, it means that after this time there will be a check
whether the loop still exists, if it doesn’t exist the port state will be
changed to active.

Restrictions Only administrator or operator-level users can issue this command.

**Example usage:**
To configure STP with maxage 18, maxhops of 15, enabling lbd and defining the lbd recovery time as 55:

```
DGS3100# config stp maxage 18 maxhops 15 lbd enable
lbd_recover_time 55
Success.
DGS3100#
```

**config stp ports**

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To setup STP on the port level.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>`config stp ports [&lt;portlist&gt;</td>
</tr>
<tr>
<td>Description</td>
<td>The <strong>config stp ports</strong> command configures STP for a group of ports.</td>
</tr>
<tr>
<td>Parameters</td>
<td><code>&lt;portlist&gt;</code> – A port or range of ports to be configured. The port list is</td>
</tr>
</tbody>
</table>
specified by listing switch number and the beginning port number on that switch, separated by a colon. Then the highest port number of the range is specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 1:22 specifies switch number 1, port 22. 1:3-22 specifies all of the ports of switch 1, between port 3 and port 22 – in numerical order.

<ch1-32> – a port-channel.

externalCost – Defines a metric that indicates the relative cost of forwarding packets to the specified port list. Port cost can be set automatically or as a metric value. The default value is auto.

- **auto** – Automatically sets the speed for forwarding packets to the specified port(s) in the list for optimal efficiency. Default port cost: 10Mbps port = 2000000, 100Mbps port = 200000, Gigabit port = 20000. Port-channel = 20000.

- **<value 1-200000000>** - Defines a value between 1 and 200000000 to determine the external cost. The lower the number, the greater the probability the port will be chosen to forward packets.

**edge [true | false]** – true designates the port as an edge port. Edge ports cannot create loops, however an edge port can lose edge port status if a topology change creates a potential for a loop. An edge port normally should not receive BPDU packets. If a BPDU packet is received it automatically loses edge port status. false indicates that the port does not have edge port status. The default setting for this parameter is false.

**p2p [true | false | auto]** – true indicates a point-to-point (P2P) link. P2P ports transition to a forwarding state rapidly thus benefiting from RSTP. A p2p value of false indicates that the port cannot have p2p status. auto allows the port to have p2p status whenever possible and operate as if the p2p status were true. (A port that operates in full-duplex is assumed to be point-to-point, while a half-duplex port is considered as a shared port). If the port cannot maintain this status (for example if the port is forced to half-duplex operation) the p2p status changes to operate as if the p2p value were false. The default setting for this parameter is auto.

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

**fbpdu [enable | disable | system]** – If enabled - allows the forwarding of STP BPDU packets from other network devices. Disable – blocking STP BPDU packets from other network devices. System – indicates that port will behave as global switch’s fbpdu value configured. Fbpdu value valid only when STP port state is disabled or global STP state is disabled. The default is system.

Restrictions Only administrator or operator-level users can issue this command.

Example usage:
To configure STP with path cost 19 and state enable for ports 1-5 of module 1.

```
DGS3100# config stp ports 1:1-5 externalCost 19 state enable
Success.
DGS3100#
```
**config stp version**

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To globally set the version of STP on the Switch.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>`config stp version [mstp</td>
</tr>
<tr>
<td>Description</td>
<td>The <code>config stp version</code> command sets the version of the spanning tree to be implemented on the Switch.</td>
</tr>
<tr>
<td>Parameters</td>
<td><code>mstp</code> – Sets the Multiple Spanning Tree Protocol (MSTP) globally on the Switch.</td>
</tr>
<tr>
<td></td>
<td><code>rstp</code> – Sets the Rapid Spanning Tree Protocol (RSTP) globally on the Switch.</td>
</tr>
<tr>
<td></td>
<td><code>stp</code> – Sets the Spanning Tree Protocol (STP) globally on the Switch.</td>
</tr>
<tr>
<td>Restrictions</td>
<td>Only administrator or operator-level users can issue this command.</td>
</tr>
</tbody>
</table>

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

```
DGS3100# config stp version mstp
Success.
DGS3100#
```

**enable stp**

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To globally enable STP on the Switch.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>enable stp</code></td>
</tr>
<tr>
<td>Description</td>
<td>The <code>enable stp</code> command sets the Spanning Tree Protocol to be globally enabled on the Switch.</td>
</tr>
<tr>
<td>Parameters</td>
<td>None.</td>
</tr>
<tr>
<td>Restrictions</td>
<td>Only administrator or operator-level users can issue this command.</td>
</tr>
</tbody>
</table>

**Example usage:**
To enable STP, globally, on the Switch:

```
DGS3100# enable stp
Success.
DGS3100#
```

**disable stp**

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To globally disable STP on the Switch.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>disable stp</code></td>
</tr>
<tr>
<td>Description</td>
<td>The <code>disable stp</code> command sets the Spanning Tree Protocol to be globally disabled on the Switch.</td>
</tr>
<tr>
<td>Parameters</td>
<td>None.</td>
</tr>
</tbody>
</table>

Example usage:
To disable STP, globally, on the Switch:

```
DGS3100# disable stp
```
### Restrictions
Only administrator or operator-level users can issue this command.

#### Example usage:

To disable STP on the Switch:

```plaintext
DGS3100# disable stp
Success.
DGS3100#
```

#### show stp

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To display the Switch's current STP configuration.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>show stp</code></td>
</tr>
<tr>
<td>Description</td>
<td>The <code>show stp</code> command displays the Switch's current STP configuration.</td>
</tr>
<tr>
<td>Parameters</td>
<td>None.</td>
</tr>
<tr>
<td>Restrictions</td>
<td>None.</td>
</tr>
</tbody>
</table>

#### Example usage:

To display the status of STP on the Switch:

**Status 1: STP enabled with STP compatible version**

```plaintext
DGS3100# show stp

STP Status          : Enabled
STP Version         : STP Compatible
Max Age             : 20
Hello Time           : 2
Forward Delay        : 15
Max Hops             : 20
Forwarding BPDU     : Enabled
Loopback Detection   : Enabled
Loopback Detection Interval : 60

DGS3100#
```

**Status 2: STP enabled for RSTP**

```plaintext
DGS3100# show stp

STP Status          : Enabled
STP Version         : RSTP
Max Age             : 20
Hello Time           : 2
Forward Delay        : 15
```
Max Age : 20
Forwarding BPDU : Enabled
Loopback Detection : Enabled
Loopback Detection Interval : 60

DGS3100#

Status 3: STP enabled for MSTP

DGS3100# show stp

STP Status : Enabled
STP Version : MSTP
Max Age : 20
Hello Time : 2
Forward Delay : 15
Max Age : 20
Forwarding BPDU : Enabled
Loopback Detection : Enabled
Loopback Detection Interval : 60

DGS3100#

## show stp ports

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To display the Switch’s current instance_id configuration.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>`show stp ports {&lt;portlist&gt;</td>
</tr>
<tr>
<td>Description</td>
<td>The <code>show stp ports</code> command displays the STP Instance Settings and STP Instance Operational Status currently implemented on the Switch.</td>
</tr>
<tr>
<td>Parameters</td>
<td><code>&lt;portlist&gt;</code> – A port or range of ports to be configured. The port list is specified by listing switch number and the beginning port number on that switch, separated by a colon. Then the highest port number of the range is specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 1:22 specifies switch number 1, port 22. 1:3-22 specifies all of the ports of switch 1, between port 3 and port 22 – in numerical order. <code>&lt;ch1-32&gt;</code> – a port-channel.</td>
</tr>
<tr>
<td>Restrictions</td>
<td>None.</td>
</tr>
</tbody>
</table>

**Example usage:**

To show stp port 9 on switch one:

```
DGS3100# show stp ports 1:9

MSTP Port Information

-----------------------------
Port Index : 1:9, Port STP enabled
External PathCost : Auto/200000, Edge Port : No/No, P2P : Auto/Yes
```
<table>
<thead>
<tr>
<th>Msti</th>
<th>Designated Bridge</th>
<th>Internal PathCost</th>
<th>Prio</th>
<th>Status</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>8000 00:23:27:26:46:00</td>
<td>200000</td>
<td>128</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

DGS3100#

**show stp instance_id**

**Purpose**
To display the Switch’s STP instance configuration

**Syntax**
show stp instance_id <value 0-15>

**Description**
The show stp instance_id command displays the Switch’s current STP Instance Settings and the STP Instance Operational Status.

**Parameters**
<value 0-15> - The value of the previously configured instance_id on the Switch. The value may be between 0 and 15. An entry of 0 displays the STP configuration for the CIST internally set on the Switch.

**Restrictions**
None.

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

DGS3100# show stp instance 0

Instance Type : CIST
Instance Status : Enabled
Instance Priority : 32768

STP Instance Operational Status

<table>
<thead>
<tr>
<th>Designated Root Bridge</th>
<th>32768/00:00:b9:89:46:79</th>
</tr>
</thead>
<tbody>
<tr>
<td>External Root Cost</td>
<td>200012</td>
</tr>
<tr>
<td>Regional Root Bridge</td>
<td>32768/00:23:27:26:46:00</td>
</tr>
<tr>
<td>Internal Root Cost</td>
<td>0</td>
</tr>
<tr>
<td>Root Port</td>
<td>1:3</td>
</tr>
<tr>
<td>Max Age</td>
<td>20</td>
</tr>
<tr>
<td>Forward Delay</td>
<td>15</td>
</tr>
<tr>
<td>Last Topology Change</td>
<td>23542964</td>
</tr>
<tr>
<td>Topology Changes Count</td>
<td>6</td>
</tr>
</tbody>
</table>

DGS3100#

**show stp mst_config_id**

**Purpose**
To display the MSTP configuration identification.

**Syntax**
show stp mst_config_id
Description
The `show stp mst_config_id` command displays the Switch's current MSTP configuration identification.

Parameters
None.

Restrictions
None.

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

```
DGS3100# show stp mst_config_id
Current MST Configuration Identification
----------------------------------------
Configuration Name : 00:53:13:1A:33:24   Revision Level :0
MSTI ID   Vid list
-----------     --------------------------------------------------------------
CIST          2-4094
1             1

DGS3100#
```

```
config stp instance_id
Purpose
To add or delete VLANs of STP instance ID.
Syntax
config stp instance_id <value 1-15> [add_vlan | remove_vlan] <vidlist>
Description
The `config stp instance_id` command maps VIDs (VLAN IDs) STP instances on the Switch. A STP instance may have multiple members with the same MSTP configuration. There is no limit to the number of STP regions in a network but each region only supports a maximum of 16 spanning tree instances (instance 0 – is one unchangeable default entry). VIDs can belong to only one spanning tree instance at a time.

Note that switches in the same spanning tree region having the same STP instance_id must be mapped identically, and have the same configuration revision_level number and the same name.

Parameters
`<value 1-15>` - The value of the instance_id. The value may be between 1 and 15. The Switch supports 16 STP regions with one unchangeable default instance ID set as 0.

`add_vlan` – Indicates that VIDs specified in the `<vidlist>` parameter are to be added to the STP instance_id.

`remove_vlan` – Indicates that VIDs specified in the `<vidlist>` parameter are to be removed from the STP instance_id.

`<vidlist>` – Specifies the range of VIDs to add to or remove from the STP instance_id. Supported VIDs on the Switch range from ID number 1 to 4094. By default each created vlan belongs to instance 0.

Restrictions
Only administrator or operator-level users can issue this command.

Example usage:
To configure instance id 2 to add VID 10:
DGS3100# config stp instance_id 2 add_vlan 10
Success.
DGS3100#

To remove VID 10 from instance id 2:

DGS3100# config stp instance_id 2 remove_vlan 10
Success.
DGS3100#

### config stp priority

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To update the STP instance configuration.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>config stp priority &lt;value 0-61440&gt; instance_id &lt;value 0-15&gt;</code></td>
</tr>
<tr>
<td>Description</td>
<td>The <code>config stp priority</code> command updates the STP instance configuration settings on the Switch. The MSTP uses the priority in selecting the root bridge, root port and designated port. Assigning higher priorities to STP regions instructs the Switch to give precedence to the selected instance_id for forwarding packets. A lower value indicates a higher priority.</td>
</tr>
<tr>
<td>Parameters</td>
<td><code>priority &lt;value 0-61440&gt;</code> - The priority for a specified <code>instance_id</code> for forwarding packets. The value may be between 0 and 61440, and must be divisible by 4096. A lower value indicates a higher priority.</td>
</tr>
<tr>
<td></td>
<td><code>instance_id &lt;value 0-15&gt;</code> - The value of the previously configured instance id for which the user wishes to set the priority value. An instance_id of 0 denotes the default instance_id (CIST) internally set on the Switch.</td>
</tr>
<tr>
<td>Restrictions</td>
<td>Only administrator or operator-level users can issue this command.</td>
</tr>
</tbody>
</table>

**Example usage:**

To set the priority value for instance_id 2 as 4096:

DGS3100# config stp priority 4096 instance_id 2
Success.
DGS3100#

### config stp mst_config_id

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To update the MSTP configuration identification.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>`config stp mst_config_id [revision_level &lt;int 0-65535&gt;</td>
</tr>
<tr>
<td>Description</td>
<td>The <code>config stp mst_config_id</code> command uniquely identifies the MSTP configuration currently configured on the Switch. Information</td>
</tr>
</tbody>
</table>
entered here is attached to BDPU packets as an identifier for the MSTP region to which it belongs. Switches having the same revision_level, name and identical vlans mapped for STP instance_ids are considered to be part of the same MSTP region.

Parameters

- **revision_level <int 0-65535>** - The MSTP configuration revision number. The value may be between 0 and 65535. This value, along with the name and identical vlans mapped for STP instance_ids identifies the MSTP region configured on the Switch. The default setting is 0.
- **name <string>** - A string of up to 32 alphanumeric characters to uniquely identify the MSTP region on the Switch. This name, along with the revision_level value and identical vlans mapped for STP instance_ids identifies the MSTP region configured on the Switch. If no name is entered, the default name is the MAC address of the device.

Restrictions

- Only administrator or operator-level users can issue this command.

**Example usage:**

To configure the MSTP region of the Switch with revision_level 10 and the name ‘Trinity’:

```
DGS3100# config stp mst_config_id revision_level 10 name Trinity
Success.
DGS3100#
```

---

**config stp mst_ports**

**Purpose**

To update the port configuration for a MSTP instance.

**Syntax**

```
config stp mst_ports [<portlist> | <ch1-32>] instance_id<value 0-15> {internalCost [auto | value 1-200000000] | priority <value 0-240>}
```

**Description**

The `config stp mst_ports` command updates the port configuration for a STP instance_id. If a loop occurs, the MSTP function uses the port cost to select an interface to put into the forwarding state (if the switch isn’t Root). If the switch is Root, then higher priority value for interfaces will influence on selected ports to be forwarding first at connected network devices. In instances where the priority value is identical, the MSTP function implements the lowest port number into the forwarding state and other interfaces are blocked. Remember that lower priority values mean higher priorities for forwarding packets.

**Parameters**

- **<portlist>** – A port or range of ports to be configured. The port list is specified by listing switch number and the beginning port number on that switch, separated by a colon. Then the highest port number of the range is specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 1:22 specifies switch number 1, port 22. 1:3-22 specifies all of the ports of switch 1, between port 3 and port 22 – in numerical order.
- **<ch1-32>** – a port-channel.
- **instance_id <value 0-15>** - The value may be between 0 and 15. An entry of 0 denotes the CIST (Common and Internal Spanning Tree).
internalCost – The relative cost of forwarding packets to specified ports when an interface is selected within an STP instance. The default setting is auto. There are two options:

- **auto** – Specifies setting the quickest route automatically and optimally for an interface. The default value is derived from the media speed of the interface.
- **value 1-200000000** – Specifies setting the quickest route when a loop occurs. The value may be in the range of 1-200000000. A lower internalCost represents a quicker transmission.

`priority <value 0-240>` - The priority for the port interface. The value may be between 0 and 240. A lower number denotes a higher priority. A higher priority designates the interface to forward packets first.

**Restrictions**

Only administrator or operator-level users can issue this command.

**Example usage:**

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

```
DGS3100# config stp mst_ports 1:1-5 instance_id 2 internalCost auto priority 16
Success.
DGS3100#
```
FORWARDING DATABASE COMMANDS

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>create fdb</td>
<td>&lt;vlan_name 32&gt; &lt;macaddr&gt; port &lt;port&gt;</td>
</tr>
<tr>
<td>create multicast_fdb</td>
<td>&lt;vlan_name 32&gt; &lt;macaddr&gt;</td>
</tr>
<tr>
<td>config multicast_fdb</td>
<td>&lt;vlan_name 32&gt; &lt;macaddr&gt; [add</td>
</tr>
<tr>
<td>config fdb aging_time</td>
<td>&lt;value 10-630&gt;</td>
</tr>
<tr>
<td>delete fdb</td>
<td>&lt;vlan_name 32&gt; &lt;macaddr&gt;</td>
</tr>
<tr>
<td>clear fdb</td>
<td>All</td>
</tr>
<tr>
<td>show multicast_fdb</td>
<td>{vlan &lt;vlan_name 32&gt;</td>
</tr>
<tr>
<td>show fdb</td>
<td>{port &lt;port&gt;</td>
</tr>
<tr>
<td>config multicast</td>
<td>filtering_mode [{&lt;portlist&gt; &lt;ch1-32&gt;</td>
</tr>
<tr>
<td>show multicast</td>
<td>filtering_mode {&lt;portlist&gt; &lt;ch1-32&gt;</td>
</tr>
<tr>
<td>config dlf</td>
<td>filtering_mode [{&lt;portlist&gt;</td>
</tr>
<tr>
<td>show dlf filtering</td>
<td>mode {ports&lt;portlist&gt;</td>
</tr>
</tbody>
</table>

Each command is listed in detail, as follows:

**create fdb**

**Purpose**: To create a static entry in the unicast MAC address forwarding table (database)

**Syntax**: create fdb <vlan_name 32> <macaddr> port <port>

**Description**: The `create fdb` command creates a static entry in the Switch’s unicast MAC address forwarding database.

**Parameters**

- `<vlan_name 32>` – The name of the VLAN on which the MAC address resides.
- `<macaddr>` – The MAC address to be added to the forwarding table.
- `port <port>` – The port number corresponding to the MAC destination address. The Switch will always forward traffic to the specified device through this port.

**Restrictions**: Only Administrator or operator-level users can issue this command.

**Example usage:**

To create a unicast MAC FDB entry:
DGS3100# create fdb default 00-00-00-00-01-02 port 2
Success.
DGS3100#

create multicast_fdb

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To create a static entry in the multicast MAC address forwarding table (database).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>create multicast_fdb &lt;vlan_name 32&gt; &lt;macaddr&gt;</td>
</tr>
<tr>
<td>Description</td>
<td>The create multicast_fdb command creates a static entry in the multicast MAC address forwarding table (database).</td>
</tr>
<tr>
<td>Parameters</td>
<td>&lt;vlan_name 32&gt; – The name of the VLAN on which the MAC address resides.</td>
</tr>
<tr>
<td></td>
<td>&lt;macaddr&gt; – The MAC address that will be added to the forwarding table.</td>
</tr>
<tr>
<td>Restrictions</td>
<td>Only Administrator or operator-level users can issue this command.</td>
</tr>
</tbody>
</table>

Example usage:
To create multicast MAC forwarding:

DGS3100# create multicast_fdb default 01-00-5E-00-00-00
Success.
DGS3100#

config multicast_fdb

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To configure the Switch’s multicast MAC address forwarding database.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>config multicast_fdb &lt;vlan_name 32&gt;&lt;macaddr&gt; [add</td>
</tr>
<tr>
<td>Description</td>
<td>The config multicast_fdb command configures the multicast MAC address forwarding table.</td>
</tr>
<tr>
<td>Parameters</td>
<td>&lt;vlan_name 32&gt; – The name of the VLAN on which the MAC address resides.</td>
</tr>
<tr>
<td></td>
<td>&lt;macaddr&gt; – The MAC address that will be added to the forwarding table.</td>
</tr>
<tr>
<td></td>
<td>add – Specifies that the MAC address is to be added to the forwarding table.</td>
</tr>
<tr>
<td></td>
<td>delete – Specifies that the MAC address is to be removed from the forwarding table.</td>
</tr>
<tr>
<td></td>
<td>&lt;portlist&gt; – A port or range of ports to be configured.</td>
</tr>
<tr>
<td>Restrictions</td>
<td>Only Administrator or operator-level users can issue this command.</td>
</tr>
</tbody>
</table>
### Example usage:

To add multicast MAC forwarding:

```
DGS3100# config multicast_fdb default 01-00-5E-00-00-00 add 1
Success.
DGS3100#
```

### config fdb aging_time

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To set the aging time of the forwarding database.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>config fdb aging_time &lt;value 10-630&gt;</code></td>
</tr>
<tr>
<td>Description</td>
<td>The <code>config fdb aging_time</code> command sets the aging time of the forwarding database. 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 0 to 630 minutes with a default value of 5 minutes. 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.</td>
</tr>
<tr>
<td>Parameters</td>
<td><code>&lt;value 0-630&gt;</code> – The aging time for the MAC address forwarding database value, in minutes.</td>
</tr>
<tr>
<td>Restrictions</td>
<td>Only Administrator or operator-level users can issue this command.</td>
</tr>
</tbody>
</table>

**Example usage:**

To set the `fdb aging_time`:

```
DGS3100# config fdb aging_time 300
Success.
DGS3100#
```

### delete fdb

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To delete an entry in the Switch’s forwarding database.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>delete fdb &lt;vlan_name 32&gt; &lt;macaddr&gt;</code></td>
</tr>
<tr>
<td>Description</td>
<td>The <code>delete fdb</code> command deletes an entry in the Switch’s MAC address forwarding database.</td>
</tr>
<tr>
<td>Parameters</td>
<td><code>&lt;vlan_name 32&gt;</code> – The name of the VLAN on which the MAC address resides.</td>
</tr>
<tr>
<td></td>
<td><code>&lt;macaddr&gt;</code> – The MAC address to be removed from the forwarding table.</td>
</tr>
<tr>
<td>Restrictions</td>
<td>Only Administrator or operator-level users can issue this command.</td>
</tr>
</tbody>
</table>

**Example usage:**

To delete an entry:  

```
DGS3100# delete fdb default 01-00-5E-00-00-00 add 1
Success.
DGS3100#
```
To delete a permanent FDB entry:

```
DGS3100# delete fdb default 00-00-00-00-01-02
Success.
DGS3100#
```

**clear fdb**

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To clear the Switch’s forwarding database of all dynamically learned MAC addresses.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>clear fdb all</td>
</tr>
<tr>
<td>Description</td>
<td>The <code>clear fdb</code> command clears dynamically learned entries from the Switch’s forwarding database.</td>
</tr>
<tr>
<td>Parameters</td>
<td>all – Clears all dynamic entries in the Switch’s forwarding database.</td>
</tr>
<tr>
<td>Restrictions</td>
<td>Only Administrator or operator-level users can issue this command.</td>
</tr>
</tbody>
</table>

**Example usage:**

To clear all FDB dynamic entries:

```
DGS3100# clear fdb all
Success.
DGS3100#
```

**show multicast_fdb**

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To display the contents of the Switch’s multicast forwarding database.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>`show multicast_fdb {vlan &lt;vlan_name 32&gt;</td>
</tr>
<tr>
<td>Description</td>
<td>The <code>show multicast_fdb</code> command displays the current contents of the Switch’s multicast MAC address forwarding database.</td>
</tr>
<tr>
<td>Parameters</td>
<td><code>vlan &lt;vlan_name 32&gt;</code> – The name of the VLAN on which the MAC address resides.</td>
</tr>
<tr>
<td></td>
<td><code>mac_address &lt;macaddr&gt;</code> – The MAC address that will be added to the forwarding table.</td>
</tr>
<tr>
<td>Restrictions</td>
<td>None.</td>
</tr>
</tbody>
</table>

**Example usage:**

To display multicast MAC address table:

```
DGS3100# show multicast_fdb
```

<table>
<thead>
<tr>
<th>VLAN Name</th>
<th>MAC Address</th>
<th>Egress Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>01-00-5E-00-00-00</td>
<td>1-5,26</td>
</tr>
</tbody>
</table>
show fdb

Purpose: 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: The `show fdb` command displays the current contents of the Switch's forwarding database.

Parameters:
- `<port>` - The port number corresponding to the MAC destination address. The Switch always forwards traffic to the specified device through this port.
- `<vlan_name 32>` - The name of the VLAN on which the MAC address resides.
- `<macaddr>` - The MAC address entry in the forwarding table.
- `static` - Specifies that static MAC address entries are to be displayed.
- `aging_time` - Displays the aging time for the MAC address forwarding database.

Restrictions: None.

Example usage:
To display unicast MAC address table:

```
DGS3100# show fdb
Unicast MAC Address Ageing Time = 300

VID  VLAN Name    MAC Address          Port  Type
----  ------------  ---------------------  ---  ----------------
 1    default      00-00-39-34-66-9A    10    Dynamic
 1    default      00-00-51-43-70-00    10    Dynamic
 1    default      00-00-5E-00-01-01    10    Dynamic
 1    default      00-00-74-60-72-2D    10    Dynamic
 1    default      00-00-81-05-00-80    10    Dynamic
 1    default      00-00-81-05-02-00    10    Dynamic
 1    default      00-00-81-48-70-01    10    Dynamic
 1    default      00-00-E2-4F-57-03    10    Dynamic
 1    default      00-00-E2-61-53-18    10    Dynamic
 1    default      00-00-E2-6B-BC-F6    10    Dynamic
 1    default      00-00-E2-7F-6B-53    10    Dynamic
 1    default      00-00-E2-82-7D-90    10    Dynamic
 1    default      00-00-F8-7C-1C-29    10    Dynamic
 1    default      00-01-02-03-04-00    CPU  Self
 1    default      00-01-02-03-04-05    10    Dynamic
```
To display the aging time:

```
DGS3100# show fdb aging_time

Unicast MAC Address Aging Time = 5

DGS3100#
```

**config multicast filtering_mode**

**Purpose**
To configure multicast filtering.

**Syntax**
```
config multicast filtering_mode [<portlist> | <ch1-32> | all][forward_unregistered_groups | filter_unregistered_groups]
```

**Description**
The `config multicast filtering_mode` command enables filtering of multicast addresses.

**Parameters**
- `<portlist>` - A port or range of ports to be configured.
- `<ch1–32>` - A LAG or range of LAGs to be configured.
- `all` - All ports to be configured.
- `forward_unregistered_groups` - Forwards unregistered multicast packets.
- `filter_unregistered_groups` - Filter unregistered multicast packets.

**Restrictions**
Only Administrator or operator-level users can issue this command.

**Example usage:**
To configure multicast filtering

```
DGS3100# config multicast filtering_mode 1
filter_unregistered_groups

Success.

DGS3100#
```

**show multicast filtering_mode**

**Purpose**
To display multicast filtering settings on the Switch.

**Syntax**
```
show multicast filtering_mode {portlist|<ch1-32>|all }
```

**Description**
The `show multicast filtering_mode` command displays the multicast filtering settings.

**Parameters**
- `<portlist>` - A port or range of ports to be configured.
- `<ch1–32>` - A LAG or range of LAGs to be configured.
- `all` - All ports to be configured.

**Restrictions**
Only Administrator or operator-level users can issue this command.
Example usage:
To show multicast filtering settings:

```
DGS3100# show multicast filtering_mode
Success.
DGS3100#
```

**config dlf filtering_mode**

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To configure DLF filtering on the Switch.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>`config dlf filtering_mode [&lt;portlist&gt;</td>
</tr>
<tr>
<td>Description</td>
<td>The <code>config DLF filtering_mode</code> command defines DLF filtering or forwarding on selected ports/LAGs or all ports and LAGs.</td>
</tr>
<tr>
<td>Parameters</td>
<td><code>&lt;portlist&gt;</code> – A port or range of ports to be configured.</td>
</tr>
<tr>
<td></td>
<td><code>&lt;ch1–32&gt;</code> – A LAG or range of LAGs to be configured.</td>
</tr>
<tr>
<td></td>
<td><code>all</code> – All ports and LAGs to be configured.</td>
</tr>
<tr>
<td></td>
<td><code>forward_dlf</code> – Forwards DLF packets.</td>
</tr>
<tr>
<td></td>
<td><code>filter_dlf</code> – Filters DLF packets.</td>
</tr>
<tr>
<td>Restrictions</td>
<td>Only Administrator or operator-level users can issue this command.</td>
</tr>
</tbody>
</table>

Example usage:
To configure DLF filtering

```
DGS-3100# config dlf filtering_mode all filter_dlf
Success.
DGS-3100#
```

**show dlf filtering_mode**

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To display DLF filtering settings on the Switch.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>`show dlf filtering_mode {portlist}</td>
</tr>
<tr>
<td>Description</td>
<td>The <code>show dlf filtering_mode</code> command displays the DLF filtering settings.</td>
</tr>
<tr>
<td>Parameters</td>
<td><code>&lt;portlist&gt;</code> – A port or range of ports to be configured.</td>
</tr>
<tr>
<td></td>
<td><code>&lt;ch1-32&gt;</code> – A LAG or range of LAGs to be configured.</td>
</tr>
<tr>
<td></td>
<td><code>all</code> – All ports and LAGs to be configured.</td>
</tr>
<tr>
<td>Restrictions</td>
<td>Only Administrator or operator-level users can issue this command.</td>
</tr>
</tbody>
</table>

Example usage:
To show DLF filtering settings:

```
DGS-3100# show dlf filtering
```
<table>
<thead>
<tr>
<th>Port DLF Filtering Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>1:1 Forward_DLF_Packets</td>
</tr>
<tr>
<td>1:2 Forward_DLF_Packets</td>
</tr>
<tr>
<td>1:3 Forward_DLF_Packets</td>
</tr>
<tr>
<td>1:4 Forward_DLF_Packets</td>
</tr>
<tr>
<td>1:5 Forward_DLF_Packets</td>
</tr>
<tr>
<td>1:6 Forward_DLF_Packets</td>
</tr>
<tr>
<td>1:7 Forward_DLF_Packets</td>
</tr>
<tr>
<td>1:8 Forward_DLF_Packets</td>
</tr>
<tr>
<td>1:9 Forward_DLF_Packets</td>
</tr>
<tr>
<td>1:10 Forward_DLF_Packets</td>
</tr>
<tr>
<td>1:11 Forward_DLF_Packets</td>
</tr>
<tr>
<td>1:12 Forward_DLF_Packets</td>
</tr>
<tr>
<td>1:13 Forward_DLF_Packets</td>
</tr>
<tr>
<td>1:14 Forward_DLF_Packets</td>
</tr>
<tr>
<td>1:15 Forward_DLF_Packets</td>
</tr>
<tr>
<td>1:16 Forward_DLF_Packets</td>
</tr>
<tr>
<td>1:17 Forward_DLF_Packets</td>
</tr>
<tr>
<td>1:18 Forward_DLF_Packets</td>
</tr>
<tr>
<td>1:19 Forward_DLF_Packets</td>
</tr>
</tbody>
</table>

DGS-3100#
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.

<table>
<thead>
<tr>
<th>Command</th>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>config traffic control</td>
<td>{{&lt;[portlist]&gt;</td>
</tr>
<tr>
<td>show traffic control</td>
<td>{ports &lt;portlist&gt;}</td>
</tr>
</tbody>
</table>

Each command is listed in detail, as follows:

**config traffic control**

**Purpose**
To configure broadcast / multicast / unknown unicast traffic control.

**Syntax**

```
config traffic control {{<[portlist]> | all} state [enable | disable] | storm_type [broadcast | multicast | broadcast_multicast | dlf_multicast_broadcast | threshold <int 3500-1000000>}
```

**Description**
The `config traffic control` command configures broadcast, multicast and unknown unicast storm control.

**Parameters**
- `<portlist>` - A port or range of ports to be configured.
- `all` - Specifies all ports on the Switch are to be configured.
- `storm_type` - The type of broadcast storm for which to configure the traffic control. The options are:
  - `broadcast` - Enables broadcast storm control only.
  - `multicast_broadcast` - Enables broadcast and multicast storm control.
  - `dlf_multicast_broadcast` - Enables broadcast, multicast and unknown unicast storm control.
- `<int 3500-1000000>` - The upper threshold at which the specified traffic control is switched on. The value is the number of broadcast/multicast/dlf packets, in Kbps, received by the Switch that will trigger the storm traffic control measures. The value ranges in size from 3500 to 1000000 Kbps.

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

**Example usage:**
To configure traffic control and enable broadcast storm control system wide:

```
DGS3100# config traffic control all state enable threshold 15000
storm_type multicast_broadcast
Success.
DGS3100#
```
### show traffic control

**Purpose**  
To display current traffic control settings.

**Syntax**  
```
show traffic control {ports <portlist>}
```

**Description**  
The `show traffic control` command displays the current storm traffic control configuration on the Switch.

**Parameters**  
- `ports <portlist>` - A port or range of ports whose settings are to be displayed.

**Restrictions**  
None.

**Example usage:**

To display traffic control setting for ports 1-5:

```
DGS3100# show traffic control

<table>
<thead>
<tr>
<th>Port</th>
<th>Threshold</th>
<th>Broadcast Storm</th>
<th>Multicast Storm</th>
<th>Destination Lookup Fail</th>
</tr>
</thead>
<tbody>
<tr>
<td>1:1</td>
<td>3500</td>
<td>disable</td>
<td>disable</td>
<td>disable</td>
</tr>
<tr>
<td>1:2</td>
<td>3500</td>
<td>disable</td>
<td>disable</td>
<td>disable</td>
</tr>
<tr>
<td>1:3</td>
<td>3500</td>
<td>disable</td>
<td>disable</td>
<td>disable</td>
</tr>
<tr>
<td>1:4</td>
<td>3500</td>
<td>disable</td>
<td>disable</td>
<td>disable</td>
</tr>
<tr>
<td>1:5</td>
<td>3500</td>
<td>disable</td>
<td>disable</td>
<td>disable</td>
</tr>
<tr>
<td>1:6</td>
<td>3500</td>
<td>disable</td>
<td>disable</td>
<td>disable</td>
</tr>
<tr>
<td>1:7</td>
<td>3500</td>
<td>disable</td>
<td>disable</td>
<td>disable</td>
</tr>
<tr>
<td>1:8</td>
<td>3500</td>
<td>disable</td>
<td>disable</td>
<td>disable</td>
</tr>
<tr>
<td>1:9</td>
<td>3500</td>
<td>disable</td>
<td>disable</td>
<td>disable</td>
</tr>
<tr>
<td>1:10</td>
<td>3500</td>
<td>disable</td>
<td>disable</td>
<td>disable</td>
</tr>
<tr>
<td>1:11</td>
<td>3500</td>
<td>disable</td>
<td>disable</td>
<td>disable</td>
</tr>
<tr>
<td>1:12</td>
<td>3500</td>
<td>disable</td>
<td>disable</td>
<td>disable</td>
</tr>
<tr>
<td>1:13</td>
<td>3500</td>
<td>disable</td>
<td>disable</td>
<td>disable</td>
</tr>
<tr>
<td>1:14</td>
<td>3500</td>
<td>disable</td>
<td>disable</td>
<td>disable</td>
</tr>
<tr>
<td>1:15</td>
<td>3500</td>
<td>disable</td>
<td>disable</td>
<td>disable</td>
</tr>
<tr>
<td>1:16</td>
<td>3500</td>
<td>disable</td>
<td>disable</td>
<td>disable</td>
</tr>
<tr>
<td>1:17</td>
<td>3500</td>
<td>disable</td>
<td>disable</td>
<td>disable</td>
</tr>
</tbody>
</table>
```

CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a ALL
QOS COMMANDS

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>config scheduling</td>
<td>&lt;class_id 0-3&gt; max_packet &lt;value 0-15&gt;</td>
</tr>
<tr>
<td>show scheduling</td>
<td></td>
</tr>
<tr>
<td>config bandwidth_control</td>
<td>[&lt;portlist&gt;</td>
</tr>
<tr>
<td>show bandwidth_control</td>
<td>[&lt;portlist&gt;</td>
</tr>
<tr>
<td>config 802.1p user_priority</td>
<td>&lt;priority 0-7&gt; &lt;class_id 0-3&gt;</td>
</tr>
<tr>
<td>show 802.1p user_priority</td>
<td></td>
</tr>
<tr>
<td>config 802.1p default_priority</td>
<td>[&lt;portlist&gt;</td>
</tr>
<tr>
<td>show 802.1p default_priority</td>
<td>&lt;portlist&gt;</td>
</tr>
<tr>
<td>config scheduling_mechanism</td>
<td>&lt;class_id 0-3&gt; [strict</td>
</tr>
<tr>
<td>show scheduling_mechanism</td>
<td></td>
</tr>
<tr>
<td>config rate_limit</td>
<td>[&lt;portlist&gt;</td>
</tr>
<tr>
<td>show rate_limit</td>
<td>[&lt;portlist&gt;</td>
</tr>
</tbody>
</table>

Each command is listed in detail, as follows:

### config scheduling

**Purpose**
To configure traffic scheduling for each of the Switch’s QoS queues.

**Syntax**
```
config scheduling <class_id 0-3> max_packet <value 0-15>
```

**Description**
The `config scheduling` command configures traffic scheduling for each of the Switch’s QoS queues.

The Switch contains four hardware classes of service. Incoming packets must be mapped to one of these four hardware queues. This command is used to specify the rotation by which these four hardware queues are emptied.

The Switch’s default (if the `config scheduling` command is not used) is to empty the hardware queues in order – from the highest priority queue (hardware class 3) to the lowest priority queue (hardware class 0). Each hardware queue transmits 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.

The max_packets parameter allows the user to specify the maximum number of packets a given hardware priority queue can transmit before allowing the next lowest hardware priority queue to begin transmitting its packets. A value between 0 and 15 can be specified. For example, if a value of 3 is specified for all the queues, then the highest hardware priority queue (number 3) will be allowed to transmit 3 packets – then the next lowest hardware priority queue (number 2) will be allowed to transmit 3 packets, and so on, until all of the queues have transmitted 3 packets. The process will then repeat.

**Parameters**

<class_id 0-3> – The hardware classes of service to which the config scheduling command is to be applied. The four hardware classes of service are identified by number (from 0 to 3) with class 3 having the highest priority.

max_packet <value 0-15> – Specifies the maximum number of packets the above specified priority class of service is allowed to transmit before allowing the next lower priority class of service to transmit its packets. The value may be between 0 and 15 packets. The default value is 1 for class_id 0, 2 for class_id 1, 4 for class_id 2, and 8 for class_id 3.

**Restrictions**

Only administrator or operator level users can issue this command. This command is usable only if the device was configured to work in round robin scheduling (config scheduling_mechanism).

**Example usage:**

To configure traffic scheduling:

```
DGS3100# config scheduling 3 max_packet 15
Success.
DGS3100#
```

**show scheduling**

**Purpose**

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_packet) value assigned to the four priority classes of service on the Switch. The Switch empties the four hardware queues in order, from the highest priority (class 3) to the lowest priority (class 0).

**Parameters**

None.

**Restrictions**

None.

**Example usage:**

To display the current scheduling configuration:

```
DGS3100# show scheduling
```
QOS Output Scheduling

<table>
<thead>
<tr>
<th>Class</th>
<th>MAX. Packet</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class-0</td>
<td>1</td>
</tr>
<tr>
<td>Class-1</td>
<td>2</td>
</tr>
<tr>
<td>Class-2</td>
<td>3</td>
</tr>
<tr>
<td>Class-3</td>
<td>4</td>
</tr>
</tbody>
</table>

DGS3100#

**config bandwidth_control**

**Purpose**
To configure bandwidth control on the Switch.

**Syntax**
```
config bandwidth_control [portlist | all] {rx_rate [no_limit | <value 3500-1000000>] | tx_rate [no_limit | <value 64-1000000>]}
```

**Description**
The `config bandwidth_control` command defines bandwidth control.

**Parameters**
- `portlist` - A port or range of ports to be configured.
- `all` - Specifies that the `config bandwidth_control` command applies to all ports on the Switch.
- `rx_rate` - Enables ingress rate limiting
  - `no_limit` – Indicates no limit is defined.
  - `<value 3500-1000000>` – Indicates a range between 3500-100000 kbps.
- `tx_rate` - Enables egress rate limiting
  - `no_limit` – Indicates no limit is defined.
  - `<value 64-1000000>` – Indicates a range between 64-1000000 kbps.

**Restrictions**
None.

**Example usage:**
To configure bandwidth control configuration::

```
DGS3100# config bandwidth_control all rx_rate no_limit
Success.
DGS3100#
```

**show bandwidth_control**

**Purpose**
To display bandwidth control settings on the Switch.

**Syntax**
```
show bandwidth control [portlist | all]
```

**Description**
The `show bandwidth_control` command displays bandwidth control.

**Parameters**
- `portlist` - A port or range of ports to be configured.
- `all` - Specifies that the `show bandwidth_control` command applies
to all ports on the Switch.

Restrictions None.

Example usage:
To display the bandwidth control configuration:

```
DGS3100# show bandwidth_control all
Bandwidth Control Table

<table>
<thead>
<tr>
<th>Port</th>
<th>RX Rate</th>
<th>TX Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>no_limit</td>
<td>no_limit</td>
</tr>
<tr>
<td>2</td>
<td>no_limit</td>
<td>no_limit</td>
</tr>
<tr>
<td>3</td>
<td>no_limit</td>
<td>no_limit</td>
</tr>
<tr>
<td>4</td>
<td>no_limit</td>
<td>no_limit</td>
</tr>
<tr>
<td>5</td>
<td>no_limit</td>
<td>no_limit</td>
</tr>
<tr>
<td>6</td>
<td>no_limit</td>
<td>no_limit</td>
</tr>
<tr>
<td>7</td>
<td>no_limit</td>
<td>no_limit</td>
</tr>
<tr>
<td>8</td>
<td>no_limit</td>
<td>no_limit</td>
</tr>
<tr>
<td>9</td>
<td>no_limit</td>
<td>no_limit</td>
</tr>
<tr>
<td>10</td>
<td>no_limit</td>
<td>no_limit</td>
</tr>
<tr>
<td>11</td>
<td>no_limit</td>
<td>no_limit</td>
</tr>
<tr>
<td>12</td>
<td>no_limit</td>
<td>no_limit</td>
</tr>
<tr>
<td>13</td>
<td>no_limit</td>
<td>no_limit</td>
</tr>
<tr>
<td>14</td>
<td>no_limit</td>
<td>no_limit</td>
</tr>
<tr>
<td>15</td>
<td>no_limit</td>
<td>no_limit</td>
</tr>
<tr>
<td>16</td>
<td>no_limit</td>
<td>no_limit</td>
</tr>
<tr>
<td>17</td>
<td>no_limit</td>
<td>no_limit</td>
</tr>
</tbody>
</table>

Total entries : 17
DGS3100#```

---

**config 802.1p user_priority**

Purpose To map the 802.1p user priority of an incoming packet to one of the four hardware classes of service 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 configures the way the Switch maps an incoming packet, based on its 802.1p user priority tag, to one of the four hardware priority classes of service available on the Switch. The Switch’s default is to map the incoming 802.1p priority values to the four hardware classes of service according to the following chart:

<table>
<thead>
<tr>
<th>802.1p value</th>
<th>Switch Priority Queue</th>
<th>Switch Priority Queue(stack)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
### Parameters

- **<priority 0-7>** – The 802.1p priority value (0 to 7) to map to one of the Switch’s four hardware priority classes of service.
- **<class_id 0-3>** – The Switch’s hardware priority class of service (0 to 3) to map to the 802.1p priority value specified above.

### Restrictions

Only administrator or operator level users can issue this command.

---

### Example usage:

To configure 802.1 user priority on the Switch:

```
DGS3100# config 802.1p user_priority 1 3
Success.
DGS3100#
```

### show 802.1p user_priority

#### Purpose

To display the current mapping between an incoming packet’s 802.1p priority value and one of the Switch’s eight hardware priority classes of service.

#### 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:

```
DGS3100# show 802.1p user_priority

QOS Class of Traffic

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

DGS3100#
```
**config 802.1p default_priority**

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To assign an 802.1p priority tag to an incoming untagged packet that has no 802.1p priority tag.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>`config 802.1p default_priority [&lt;portlist&gt;</td>
</tr>
<tr>
<td>Description</td>
<td>The <code>config 802.1p default_priority</code> command specifies the 802.1p priority value an untagged, incoming packet is assigned before being forwarded to its destination.</td>
</tr>
<tr>
<td>Parameters</td>
<td>&lt;portlist&gt; – A port or range of ports to be configured.</td>
</tr>
<tr>
<td></td>
<td>all – Specifies that the <code>config 802.1p default_priority</code> command applies to all ports on the Switch.</td>
</tr>
<tr>
<td></td>
<td>&lt;priority 0-7&gt; – The 802.1p priority value that an untagged, incoming packet is granted before being forwarded to its destination.</td>
</tr>
<tr>
<td>Restrictions</td>
<td>Only administrator or operator level users can issue this command.</td>
</tr>
</tbody>
</table>

**Example usage:**

To configure 802.1p default priority on the Switch:

```
DGS3100# config 802.1p default_priority all 5
Success.
DGS3100#
```

**show 802.1p default_priority**

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To display the currently configured 802.1p priority value that is assigned to an incoming, untagged packet before being forwarded to its destination.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>show 802.1p default_priority {&lt;portlist&gt;}</code></td>
</tr>
<tr>
<td>Description</td>
<td>The <code>show 802.1p default_priority</code> command displays the currently configured 802.1p priority value that is assigned to an incoming, untagged packet before being forwarded to its destination.</td>
</tr>
<tr>
<td>Parameters</td>
<td>&lt;portlist&gt; – A port or range of ports to be displayed.</td>
</tr>
<tr>
<td>Restrictions</td>
<td>None.</td>
</tr>
</tbody>
</table>

**Example usage:**

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

```
DGS3100# show 802.1p default_priority

<table>
<thead>
<tr>
<th>Port</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
</tr>
</tbody>
</table>
```
# config scheduling_mechanism

**Purpose** To configure the scheduling mechanism for the QoS function.

**Syntax**

```
config scheduling_mechanism <class_id 0-3> [strict | round_robin]
```

**Description**
The `config scheduling_mechanism` command configures the scheduling mechanism for the QoS function. It allows the user to select between a round robin (WRR) and a strict mechanism for emptying the priority classes of service of the QoS function. The Switch contains four hardware priority classes of service. Incoming packets must be mapped to one of these four hardware priority classes of service, or queues. This command is used to specify the rotation by which these four hardware priority queues are emptied.

The Switch's default is to empty the four hardware priority queues in order – from the highest priority hardware queue (class 3) to the lowest priority hardware queue (class 0). Each queue will transmit all of the packets in its buffer before allowing the next lower priority queue to transmit its packets. A lower priority hardware queue will be pre-empted from emptying its queue if a packet is received on a higher priority hardware queue. The packet received on the higher priority hardware queue transmits its packet before allowing the lower priority hardware queue to resume clearing its queue.

**Parameters**

- `<class_id 0-3>` – This specifies to which of the four hardware classes of service the `config scheduling_mechanism` command applies. The four hardware classes of service are identified by number (from 0 to 3), with the 0 queue having the lowest priority.
- `strict` – Specifies that the highest class of service is the first to be processed. That is, the highest class of service should finish emptying before the others begin.
- `round_robin` – Specifies that the priority classes of service are to empty packets in a weighted roundrobin (WRR) order.

**Restrictions**

Only administrator or operator level users can issue this command.
Example usage:

To configure the traffic scheduling mechanism for each COS queue:

```
DGS3100# config scheduling_mechanism 2 strict
Success.
DGS3100#
```

```
show scheduling_mechanism

Purpose To display the current traffic scheduling mechanisms in use on the Switch.

Syntax `show scheduling_mechanism`

Description The `show scheduling_mechanism` command displays the current traffic scheduling mechanisms in use on the Switch.

Parameters None.

Restrictions None.
```

Example usage:

To show the scheduling mechanism:

```
DGS3100# show scheduling_mechanism

QOS scheduling_mechanism
CLASS ID    Mechanism
---------    ------------
Class-0      strict
Class-1      strict
Class-2      strict
Class-3      strict

DGS3100#
```

```
config rate_limit

Purpose To enable rate limitation of specific ingress ports.

Syntax `config rate_limit [<portlist> | all] [disable | <value 3500-1000000>]`

Description The `config rate_limit` command enables setting of rate limitation of ingress ports.

Parameters

- `<portlist>` – A port or range of ports to be set.
- `all` – Specifies that all ports are to be configured.
- `disable` – Disables rate limiting.
- `<value 3500-1000000>` The rate limit value. The value may be between 3500 and 1000000.

Restrictions None.
```
Example usage:
To configure a rate limit of egress port 1:

```
DGS3100# config rate_limit 1:1
Success.
DGS3100#
```

**show rate_limit**

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To show the rate limit of specific egress ports.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>`show rate_limit [&lt;portlist&gt;</td>
</tr>
<tr>
<td>Description</td>
<td>The <code>show rate_limit</code> command displays the rate limit of an egress port.</td>
</tr>
<tr>
<td>Parameters</td>
<td><code>&lt;portlist&gt;</code> – A port or range of ports whose rate limit is to be displayed.</td>
</tr>
<tr>
<td></td>
<td><code>all</code> – Specifies that all ports are to be displayed.</td>
</tr>
<tr>
<td>Restrictions</td>
<td>None.</td>
</tr>
</tbody>
</table>

Example usage:
To show a port’s rate limit:

```
DGS3100# show rate_limit all

Current rate limit

<table>
<thead>
<tr>
<th>Port</th>
<th>Rate Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>3500</td>
</tr>
<tr>
<td>2</td>
<td>3500</td>
</tr>
<tr>
<td>3</td>
<td>3500</td>
</tr>
<tr>
<td>4</td>
<td>3500</td>
</tr>
<tr>
<td>5</td>
<td>3500</td>
</tr>
<tr>
<td>6</td>
<td>3500</td>
</tr>
<tr>
<td>7</td>
<td>3500</td>
</tr>
<tr>
<td>8</td>
<td>3500</td>
</tr>
<tr>
<td>9</td>
<td>3500</td>
</tr>
<tr>
<td>10</td>
<td>3500</td>
</tr>
<tr>
<td>11</td>
<td>3500</td>
</tr>
<tr>
<td>12</td>
<td>3500</td>
</tr>
<tr>
<td>13</td>
<td>3500</td>
</tr>
<tr>
<td>14</td>
<td>3500</td>
</tr>
<tr>
<td>15</td>
<td>3500</td>
</tr>
<tr>
<td>16</td>
<td>3500</td>
</tr>
<tr>
<td>17</td>
<td>3500</td>
</tr>
</tbody>
</table>

CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a ALL
```
PORT MIRRORING COMMANDS

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>config mirror</td>
<td>target &lt;port&gt; source &lt;port&gt; direction [ingress</td>
</tr>
<tr>
<td>delete mirror</td>
<td>target &lt;port&gt; source &lt;port&gt;</td>
</tr>
<tr>
<td>show mirror</td>
<td></td>
</tr>
</tbody>
</table>

Each command is listed in detail, as follows:

**config mirror**

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To configure a mirror port – source port pair on the Switch.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>config mirror target &lt;port&gt; source &lt;port&gt; direction [ingress</td>
</tr>
<tr>
<td>Description</td>
<td>The config mirror command allows a port to have all of its traffic also sent to a designated port, where a network sniffer or other device can monitor the network traffic. In addition, one can specify that only traffic received by or sent by one or both is mirrored to the target port.</td>
</tr>
<tr>
<td>Parameters</td>
<td>target &lt;port&gt; – Specifies the port that mirrors traffic forwarding. source &lt;port&gt; – Specifies the port or ports being mirrored. This cannot include the target port.</td>
</tr>
<tr>
<td></td>
<td>ingress – Allows mirroring of packets received by (flowing into) the source port.</td>
</tr>
<tr>
<td></td>
<td>egress – Allows mirroring of packets sent to (flowing out of) the source port.</td>
</tr>
<tr>
<td></td>
<td>both – Allows mirroring of all the packets received or sent by the source port.</td>
</tr>
<tr>
<td>Comment</td>
<td>The user can define up to 8 source ports and one destination port. One source port can be configured each time using one CLI command, So in order to configure multiple source ports, multiple CLI commands should be used.</td>
</tr>
<tr>
<td>Restrictions</td>
<td>A target port cannot be listed as a source port. Only Administrator or operator-level users can issue this command.</td>
</tr>
</tbody>
</table>

**Example usage:**

To add the mirroring ports:

```
DGS3100# config mirror source 1 target port 2 direction ingress
Success.
DGS3100#
```
### delete mirror

<table>
<thead>
<tr>
<th><strong>Purpose</strong></th>
<th>To remove a previously entered port mirroring configuration.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax</strong></td>
<td><strong>delete mirror target</strong> <code>&lt;port&gt;</code> <strong>source</strong> <code>&lt;port&gt;</code></td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>The <em>delete mirror</em> command removes a previously configured mirror port - source port pair on the Switch.</td>
</tr>
<tr>
<td><strong>Parameters</strong></td>
<td></td>
</tr>
<tr>
<td>target <code>&lt;port&gt;</code></td>
<td>Specifies the port that mirrors traffic forwarding.</td>
</tr>
<tr>
<td>source <code>&lt;port&gt;</code></td>
<td>Specifies the port or ports being mirrored. This cannot include the target port.</td>
</tr>
<tr>
<td><strong>Comment</strong></td>
<td>One source port can be deleted each time using one CLI command, so in order to delete multiple source ports, multiple CLI commands should be used.</td>
</tr>
<tr>
<td><strong>Restrictions</strong></td>
<td>Only Administrator or operator-level users can issue this command.</td>
</tr>
</tbody>
</table>

**Example usage:**

To delete a mirroring configuration:

```
DGS3100# delete mirror source 1 target port 2 ingress
Success.
DGS3100#
```

### show mirror

<table>
<thead>
<tr>
<th><strong>Purpose</strong></th>
<th>To show the current port mirroring configuration on the Switch.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax</strong></td>
<td><strong>show mirror</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>The <em>show mirror</em> command displays the current port mirroring configuration on the Switch.</td>
</tr>
<tr>
<td><strong>Parameters</strong></td>
<td>None.</td>
</tr>
<tr>
<td><strong>Restrictions</strong></td>
<td>None.</td>
</tr>
</tbody>
</table>

**Example usage:**

To display mirroring configuration:

```
DGS3100# show mirror

Current Settings
Mirror Status : Enabled
Target Port for Ingress : 2
Target Port for Egress : 3
Mirrored Port : 1
```

DGS3100#
The VLAN commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

<table>
<thead>
<tr>
<th>Command</th>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>create vlan</td>
<td><code>&lt;vlan_name 32&gt; {tag &lt;vlanid 2-4094&gt;}</code></td>
</tr>
<tr>
<td>delete vlan</td>
<td><code>&lt;vlan_name 32&gt;</code></td>
</tr>
<tr>
<td>config vlan</td>
<td>`&lt;vlan_name 32&gt; [add [tagged</td>
</tr>
<tr>
<td>config gvrp</td>
<td>`[&lt;portlist&gt;</td>
</tr>
<tr>
<td>enable gvrp</td>
<td></td>
</tr>
<tr>
<td>disable gvrp</td>
<td></td>
</tr>
<tr>
<td>show vlan</td>
<td><code>{&lt;vlan_name 32&gt;}</code></td>
</tr>
<tr>
<td>show gvrp</td>
<td>`{&lt;portlist&gt;</td>
</tr>
<tr>
<td>enable vlan_trunk</td>
<td></td>
</tr>
<tr>
<td>disable vlan_trunk</td>
<td></td>
</tr>
<tr>
<td>show vlan_trunk</td>
<td></td>
</tr>
<tr>
<td>config vlan_trunk ports</td>
<td>`&lt;portlist&gt; state [enable</td>
</tr>
<tr>
<td>enable asymmetric_vlan</td>
<td></td>
</tr>
<tr>
<td>disable asymmetric_vlan</td>
<td></td>
</tr>
<tr>
<td>show asymmetric_vlan</td>
<td></td>
</tr>
</tbody>
</table>

Each command is listed in detail, as follows:

**create vlan**

**Purpose**: To create a VLAN on the Switch.

**Syntax**: `create vlan <vlan_name 32> {tag <vlanid 2-4094>}`

**Description**: The `create vlan` command creates a VLAN on the Switch.

**Parameters**

- `<vlan_name 32>` – The name of the VLAN to be created.
- `tag <vlanid 2-4094>` – The VLAN ID of the VLAN to be created. The allowed values range from 2 to 4094.

**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 or operator-level users can issue this command.
Example usage:
To create a VLAN v1, tag 2:

```
DGS3100# create vlan v1 tag 2
Success.
DGS3100#
```

**delete vlan**

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To delete a previously configured VLAN on the Switch.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>delete vlan &lt;vlan_name 32&gt;</code></td>
</tr>
<tr>
<td>Description</td>
<td>The <code>delete vlan</code> command deletes a previously configured VLAN on the Switch.</td>
</tr>
<tr>
<td>Parameters</td>
<td><code>&lt;vlan_name 32&gt;</code> – The name of the VLAN to be deleted.</td>
</tr>
<tr>
<td>Restrictions</td>
<td>Only administrator or operator-level users can issue this command. A user is required to disable Guest VLAN before deleting a VLAN.</td>
</tr>
</tbody>
</table>

Example usage:
To remove a vlan v1:

```
DGS3100# delete vlan v1
Success.
DGS3100#
```

**config vlan**

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To add additional ports to a previously configured VLAN.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>`config vlan &lt;vlan_name 32&gt; [add</td>
</tr>
<tr>
<td>Description</td>
<td>The <code>config vlan</code> command allows the user to add or delete ports to the port list of a previously configured VLAN. You can specify the additional ports as tagging, untagging, or forbidden. The default is to assign the ports as untagged.</td>
</tr>
<tr>
<td>Parameters</td>
<td><code>&lt;vlan_name 32&gt;</code> – The name of the VLAN to which to add ports. <code>add</code> – Specifies that ports are to be added to a previously created vlan. <code>delete</code> – Specifies that ports are to be deleted from a previously created vlan. <code>tagged</code> – Specifies the additional ports as tagged. <code>untagged</code> – Specifies the additional ports as untagged. <code>forbidden</code> – Specifies the additional ports as forbidden. <code>&lt;portlist&gt;</code> – A port or range of ports to be added to or deleted from the VLAN. <code>&lt;ch1-32&gt;</code> – assigns ports to a port-channel.</td>
</tr>
</tbody>
</table>

97
Restrictions

Only administrator or operator-level users can issue this command.

Example usage:

To add ports 4 through 8 at device #1 as tagged ports to the VLAN v2:

```
DGS3100# config vlan v2 add tagged 1:4-8
Success.
```

```
DGS3100#
```
below, is used to enable and disable GVRP on the Switch, without changing the GVRP configuration on the ports and the LAGs.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>None.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restrictions</td>
<td>Only administrator or operator-level users can issue this command.</td>
</tr>
</tbody>
</table>

Example usage:

To enable the generic VLAN Registration Protocol (GVRP):

```
DGS3100# enable gvrp
Success.
DGS3100#
``` 

```
DGS3100# disable gvrp
Success.
DGS3100#
``` 

**disable gvrp**

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To disable GVRP on the Switch.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>disable gvrp</code></td>
</tr>
<tr>
<td>Description</td>
<td>The <code>disable gvrp</code> command, along with the <code>enable gvrp</code> command above, is used to enable and disable GVRP on the Switch, without changing the GVRP configuration on the ports and the LAGs.</td>
</tr>
<tr>
<td>Parameters</td>
<td>None.</td>
</tr>
<tr>
<td>Restrictions</td>
<td>Only administrator or operator-level users can issue this command.</td>
</tr>
</tbody>
</table>

Example usage:

To disable the Generic VLAN Registration Protocol (GVRP):

```
DGS3100# disable gvrp
Success.
DGS3100#
``` 

```
DGS3100# show vlan {<vlan_name 32>}
```

**show vlan**

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To display the current VLAN configuration on the Switch</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>show vlan {&lt;vlan_name 32&gt;}</code></td>
</tr>
<tr>
<td>Description</td>
<td>The <code>show vlan</code> 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.</td>
</tr>
<tr>
<td>Parameters</td>
<td><code>&lt;vlan_name 32&gt;</code> – The name of the VLAN whose settings are to be displayed.</td>
</tr>
<tr>
<td>Restrictions</td>
<td>None.</td>
</tr>
</tbody>
</table>

Example usage:

To display the Switch’s current VLAN settings:

```
DGS3100# show vlan
```
VID: 1  VLAN Name: default
VLAN TYPE: static
Member ports: 1-24
Static ports: 1-24
Untagged ports: 1-24g
Forbidden ports: 
Total Entries: 1

DGS3100#

show gvrp

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To display the GVRP status for a port list or port channel on the Switch.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>`show gvrp {&lt;portlist&gt;</td>
</tr>
<tr>
<td>Description</td>
<td>The <code>show gvrp</code> command displays the GVRP status for a port list or a port channel on the Switch.</td>
</tr>
<tr>
<td>Parameters</td>
<td><code>&lt;portlist&gt;</code> – Specifies a port or range of ports for which the GVRP status is to be displayed. <code>&lt;ch1-32&gt;</code> – Specifies a port-channel.</td>
</tr>
<tr>
<td>Restrictions</td>
<td>None.</td>
</tr>
</tbody>
</table>

Example usage:

To display GVRP port status:

DGS3100# show gvrp 1:1-5

Global GVRP : Disabled

<table>
<thead>
<tr>
<th>Port</th>
<th>PVID</th>
<th>GVRP</th>
<th>Ingress Checking</th>
<th>Acceptable Frame Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1:1</td>
<td>1</td>
<td>Disabled</td>
<td>Enabled</td>
<td>All Frames</td>
</tr>
<tr>
<td>1:2</td>
<td>1</td>
<td>Disabled</td>
<td>Enabled</td>
<td>All Frames</td>
</tr>
<tr>
<td>1:3</td>
<td>1</td>
<td>Disabled</td>
<td>Enabled</td>
<td>All Frames</td>
</tr>
<tr>
<td>1:4</td>
<td>1</td>
<td>Disabled</td>
<td>Enabled</td>
<td>All Frames</td>
</tr>
<tr>
<td>1:5</td>
<td>1</td>
<td>Disabled</td>
<td>Enabled</td>
<td>All Frames</td>
</tr>
</tbody>
</table>

Total Entries: 5

enable vlan_trunk

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To enable VLAN trunking on the switch.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>enable vlan_trunk</code></td>
</tr>
<tr>
<td>Description</td>
<td>The <code>enable vlan_trunk</code> command, along with the <code>disable vlan_trunk</code> command below, is used to enable and disable VLAN</td>
</tr>
</tbody>
</table>
trunking on the Switch, without changing the VLAN trunking configuration on the ports.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>None.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restrictions</td>
<td>Only administrator or operator-level users can issue this command.</td>
</tr>
</tbody>
</table>

**Example usage:**

To enable vlan_trunk on the switch:

```
DGS-3100# enable vlan_trunk
```

Success.

```
DGS-3100#
```

### disable vlan_trunk

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To disable VLAN Trunking on the switch.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>disable vlan_trunk</td>
</tr>
<tr>
<td>Description</td>
<td>The <code>disable vlan_trunk</code> command, along with the <code>enable vlan_trunk</code> command below, is used to disable and enable VLAN Trunking on the Switch, without changing the VLAN Trunking configuration on the ports.</td>
</tr>
<tr>
<td>Parameters</td>
<td>None.</td>
</tr>
<tr>
<td>Restrictions</td>
<td>Only administrator or operator-level users can issue this command.</td>
</tr>
</tbody>
</table>

**Example usage:**

To disable vlan_trunk on the switch:

```
DGS-3100# disable vlan_trunk
```

Success.

```
DGS-3100#
```

### show vlan_trunk

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To display the current VLAN Trunking configuration on the Switch</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>show vlan_trunk</code></td>
</tr>
<tr>
<td>Description</td>
<td>The <code>show vlan_trunk</code> command displays summary information about VLAN trunking status and configured ports.</td>
</tr>
<tr>
<td>Parameters</td>
<td>None.</td>
</tr>
<tr>
<td>Restrictions</td>
<td>Only administrator or operator-level users can issue this command.</td>
</tr>
</tbody>
</table>

**Example usage:**

To display the Switch’s current VLAN_trunk settings:

```
DGS-3100# show vlan_trunk
```

```
Vlan Trunking : Enabled
```

101
**config vlan_trunk ports**

**Purpose**
To configure VLAN Trunking port settings on the Switch.

**Syntax**
```
config vlan_trunk ports <portlist> state [enable | disable]
```

**Description**
The `config vlan_trunk ports` command configures the VLAN trunking port settings on the Switch. The user can enable VLAN Trunking and define ports to be added to the VLAN Trunking settings.

**Parameters**
- `<portlist>` - A port or range of ports for which to configure VLAN Trunking.
- `state [enable | disable]` - enable and disable VLAN trunking.

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

**Example usage:**

To define VLAN Trunking:

```
DGS3100# config vlan_trunk ports 1-2 state disable
Success.
DGS3100#
```

---

**enable asymmetric_vlan**

**Purpose**
To enable Asymmetric VLAN on the switch.

**Syntax**
```
enable asymmetric_vlan
```

**Description**
The `enable asymmetric_vlan` command, along with the `disable asymmetric_vlan` command below, is used to enable and disable Asymmetric VLAN on the Switch.

**Parameters**
None.

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

**Example usage:**

To enable Asymmetric VLAN on the switch:

```
DGS-3100# enable asymmetric_vlan
Success.
DGS-3100#
```
disable asymmetric_vlan

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To disable Asymmetric VLAN on the switch.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>disable asymmetric_vlan</td>
</tr>
<tr>
<td>Description</td>
<td>The <code>disable asymmetric_vlan</code> command, along with the <code>enable asymmetric_vlan</code> command below, is used to disable and enable Asymmetric VLAN on the Switch.</td>
</tr>
<tr>
<td>Parameters</td>
<td>None.</td>
</tr>
<tr>
<td>Restrictions</td>
<td>Only administrator or operator-level users can issue this command.</td>
</tr>
</tbody>
</table>

**Example usage:**
To disable asymmetric_vlan on the switch:

```
DGS-3100# disable asymmetric_vlan
Success.
DGS-3100#
```

show asymmetric_vlan

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To display the Asymmetric VLAN status on the Switch.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>show asymmetric_vlan</td>
</tr>
<tr>
<td>Description</td>
<td>The <code>show asymmetric_vlan</code> command displays the Asymmetric VLAN status on the Switch.</td>
</tr>
<tr>
<td>Parameters</td>
<td>None.</td>
</tr>
<tr>
<td>Restrictions</td>
<td>Only administrator or operator-level users can issue this command.</td>
</tr>
</tbody>
</table>

**Example usage:**
To display Asymmetric VLAN status:

```
DGS-3100# show asymmetric_vlan
Asymmetric VLAN : Enable
DGS-3100#
```
LINK AGGREGATION COMMANDS

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>create link_aggregation</td>
<td>group_id &lt;value 1-32&gt; {type [lacp</td>
</tr>
<tr>
<td>delete link_aggregation</td>
<td>group_id &lt;value 1-32&gt;</td>
</tr>
<tr>
<td>config link_aggregation</td>
<td>group_id &lt;value 1-32&gt; { ports &lt;portlist&gt;</td>
</tr>
<tr>
<td>show link_aggregation</td>
<td>{group_id &lt;value 1-32&gt;}</td>
</tr>
</tbody>
</table>

Each command is listed in detail, as follows:

**create link_aggregation**

**Purpose**
To create a link aggregation group on the Switch.

**Syntax**
create link_aggregation group_id <value 1-32> {type [lacp | static]}

**Description**
The **create link_aggregation** command creates a link aggregation group with a unique identifier.

**Parameters**
- **group_id <value 1-32>** – Specifies the group ID. The Switch allows up to 32 link aggregation groups to be configured. The group number identifies each of the groups.
- **type** – Specify the type of link aggregation used for the group. If the type is not specified the default type is static.
  - **lacp** – This designates the port group as LACP compliant. LACP allows dynamic adjustment to the aggregated port group. LACP compliant ports may be further configured (see config lacp_ports). LACP compliant must be connected to LACP compliant devices. The maximum ports that can be configure in the same LACP are 16.
  - **static** – This designates the aggregated port group as static. Static port groups can not be changed as easily as LACP compliant port groups since both linked devices must be manually configured if the configuration of the trunked group is changed. If static link aggregation is used, be sure that both ends of the connection are properly configured and that all ports have the same speed/duplex settings. The maximum ports that can be configure in the same static LAG are 8.

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

**Example usage:**
To create a link aggregation group:

```
DGS3100# create link_aggregation group_id 1
```
**delete link_aggregation**

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To delete a previously configured link aggregation group.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>delete link_aggregation group_id &lt;value 1-32&gt;</td>
</tr>
<tr>
<td>Description</td>
<td>The <code>delete link_aggregation group_id</code> command deletes a previously configured link aggregation group.</td>
</tr>
<tr>
<td>Parameters</td>
<td>group_id &lt;value 1-32&gt; - Specifies the group ID. The Switch allows up to 32 link aggregation groups to be configured. The group number identifies each of the groups.</td>
</tr>
<tr>
<td>Restrictions</td>
<td>Only administrator or operator-level users can issue this command.</td>
</tr>
</tbody>
</table>

**Example usage:**

To delete link aggregation group:

```
DGS3100# delete link_aggregation group_id 1
Success.
DGS3100#
```

**config link_aggregation**

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To configure a previously created link aggregation group.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>config link_aggregation group_id &lt;value 1-32&gt; { ports &lt;portlist&gt;</td>
</tr>
<tr>
<td>Description</td>
<td>The <code>config link_aggregation</code> command configures a link aggregation group created with the <code>create link_aggregation</code> command above.</td>
</tr>
<tr>
<td>Parameters</td>
<td>group_id &lt;value 1-32&gt; - Specifies the group ID. The Switch allows up to 32 link aggregation groups to be configured. The group number identifies each of the groups.</td>
</tr>
<tr>
<td></td>
<td>ports &lt;portlist&gt; - Specifies a list of ports to belong to the link aggregation group. Ports will be listed in only one aggregation group and link aggregation groups can not overlap to each other. The user must configure at least two ports in LAG.</td>
</tr>
<tr>
<td></td>
<td>state [enable</td>
</tr>
<tr>
<td>Restrictions</td>
<td>Only administrator or operator-level users can issue this command. Link aggregation groups may not overlap.</td>
</tr>
</tbody>
</table>

**Example usage:**

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

```
DGS3100# config link_aggregation group_id 1 ports 5-7,9
```
**show link_aggregation**

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To display the current link aggregation configuration on the Switch.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>show link_aggregation {group_id &lt;value 1-32&gt;}</code></td>
</tr>
<tr>
<td>Description</td>
<td>The <code>show link_aggregation</code> command displays the current link aggregation configuration of the Switch.</td>
</tr>
<tr>
<td>Parameters</td>
<td><code>group_id &lt;value 1-32&gt;</code> - Specifies the group ID. The Switch allows up to 32 link aggregation groups to be configured. The group number identifies each of the groups.</td>
</tr>
<tr>
<td>Restrictions</td>
<td>None.</td>
</tr>
</tbody>
</table>

**Example usage:**

To display Link Aggregation configuration:

```
DGS3100# show link_aggregation

Group ID : 1
Member Port : 5-7,9
Active Port : 
Status : Disabled

DGS3100#
```
BASIC IP COMMANDS

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>config ipif system</td>
<td>[[ipaddress &lt;network_address&gt;</td>
</tr>
<tr>
<td>show ipif</td>
<td>{system}</td>
</tr>
</tbody>
</table>

Each command is listed in detail, as follows:

**config ipif system**

- **Purpose**: To configure the System IP interface.
- **Syntax**: `config ipif system [ipaddress <network_address> | vlan <vlan_name 32> | state [enable | disable] | dhcp | vlan <vlan_name 32>]]`
- **Description**: The `config ipif system` command configures the System IP interface on the Switch.
- **Parameters**
  - `system` - The IP interface name to be configured. The default IP Interface name on the Switch is ‘System’. All IP interface configurations done are executed through this interface name.
  - `<network_address>` - IP address and netmask of the IP interface to be created. The address and mask information may be specified by using the traditional format (for example, 10.1.2.3/255.0.0.0 or in CIDR format, 10.1.2.3/16).
  - `<vlan_name 32>` - The name of the VLAN corresponding to the System IP interface.
  - `state [enable | disable]` - Enables or disables the IP interface.
  - `dhcp | vlan <vlan_name 32>` - Specifies the DHCP protocol for the assignment of an IP address to the Switch’s System IP interface and the VLAN name to use for the DHCP Protocol.
- **Restrictions**: Only Administrator or operator-level users can issue this command.

**Example usage:**

To configure the IP interface System:

```
DGS3100# config ipif System ipaddress 10.48.74.122/8
Success.
DGS3100#
```
### show ipif

**Purpose**
To display the configuration of an IP interface on the Switch.

**Syntax**
`show ipif {system}`

**Description**
The `show ipif` command displays the configuration of an IP interface on the Switch.

**Parameters**
- `<system>` - The name of the IP interface whose settings are to be displayed (Always System).

**Restrictions**
None.

#### Example usage:
To display IP interface settings:

```
DGS3100# show ipif System

<table>
<thead>
<tr>
<th>Interface Name</th>
<th>IP Address</th>
<th>Subnet Mask</th>
<th>Vlan Name</th>
<th>Member port</th>
<th>Admin. State</th>
<th>Link Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>System</td>
<td>10.6.41.46 (dhcp)</td>
<td>255.255.255.224</td>
<td>default</td>
<td>1-24</td>
<td>Enabled</td>
<td>Link Up</td>
</tr>
</tbody>
</table>

DGS3100#
```
IGMP SNOOPING COMMANDS

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>config igmp_snooping</td>
<td>[&lt;vlan_name 32&gt;</td>
</tr>
<tr>
<td>config igmp_snooping querier</td>
<td>[vlan &lt;vlan_name 32&gt;</td>
</tr>
<tr>
<td>config router_port</td>
<td>&lt;vlan_name 32&gt; [add</td>
</tr>
<tr>
<td>config router_port_forbidden</td>
<td>&lt;vlan_name 32&gt; [add</td>
</tr>
<tr>
<td>enable igmp_snooping</td>
<td></td>
</tr>
<tr>
<td>disable igmp_snooping</td>
<td></td>
</tr>
<tr>
<td>show igmp_snooping</td>
<td>{vlan &lt;vlan_name 32&gt;}</td>
</tr>
<tr>
<td>show igmp_snooping group</td>
<td>{vlan &lt;vlan_name 32&gt;}</td>
</tr>
<tr>
<td>show igmp_snooping forwarding</td>
<td>{vlan &lt;vlan_name 32&gt;}</td>
</tr>
<tr>
<td>show router_port</td>
<td>{vlan &lt;vlan_name 32&gt;</td>
</tr>
</tbody>
</table>

Each command is listed in detail, as follows:

**config igmp_snooping**

**Purpose**
To configure IGMP snooping on the Switch.

**Syntax**
```
config igmp_snooping [<vlan_name 32> | all] {host_timeout <sec 60-16711450> | router_timeout <sec 1-16711450> | leave_timer <sec 0-16711450> | state [enable | disable]}
```

**Description**
The `config igmp_snooping` command configures IGMP snooping on the Switch.

**Parameters**
- `<vlan_name 32>` – The name of the VLAN for which IGMP snooping is to be configured.
- `all` – Specifies that IGMP snooping is to be configured for all VLANs on the Switch.
- `host_timeout <sec 60-16711450>` – Specifies the maximum amount of time a host can be a member of a multicast group without the Switch receiving a host membership report. The default is 260 seconds.
- `router_timeout <sec 1-16711450>` – Specifies the maximum amount of time a route can be a member of a multicast group without the Switch receiving a host membership report. The default is 300 seconds.
Example usage:
To configure the igmp snooping:

```
DGS3100# config igmp_snooping default host_timeout 250 state enable
Success.
DGS3100#
```

```
DGS3100# config igmp_snooping all state enable querier_version IGMPv2
Success.
DGS3100#
```
enabled router - regardless of protocol, etc.

Parameters

<vlan_name 32> – The name of the VLAN on which the router port resides. Up to 32 characters can be used.
[add | delete] – Specifies whether to add or delete ports defined in the following parameter <portlist>, to the router port function.

<portlist> – A port or range of ports that will be configured as router ports.

Restrictions

Only administrator or operator-level users can issue this command.

Example usage:

To set up static router ports:

DGS3100# config router_port default add 1-10
Success.
DGS3100#

config router_port_forbidden

Purpose

To deny ports becoming router ports.

Syntax

config router_port_forbidden <vlan_name 32> [add | delete] <portlist>

Description

The config router_port_forbidden command denies a range of ports access to multicast-enabled routers. This ensures all packets with such a router as its destination will not reach the multicast-enabled router - regardless of protocol, etc.

Parameters

<vlan_name 32> – The name of the VLAN on which the router port resides. Up to 32 characters can be used.
[add | delete] – Specifies whether to deny ports defined in the following parameter <portlist>, to the router port function.
<brportlist> – A port or range of ports that will be denied access as router ports.

Restrictions

Only administrator or operator-level users can issue this command.

Example usage:

To deny router ports:

DGS3100# config router_port_forbidden default add all
Success.
DGS3100#

enable igmp_snooping

Purpose

To enable IGMP snooping on the Switch.

Syntax

enable igmp_snooping

Description

The enable igmp_snooping command enables IGMP snooping on
### enable igmp_snooping

**Purpose**
To enable IGMP snooping on the Switch.

**Syntax**
```
enable igmp_snooping
```

**Description**
The `enable igmp_snooping` command enables IGMP snooping on the Switch. IGMP snooping can be enabled only if IP multicast routing is not being used. Enabling IGMP snooping allows all IGMP and IP multicast traffic to flood within a given IP interface.

**Parameters**
None.

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

**Example usage:**
To enable IGMP snooping on the Switch:

```
DGS3100# enable igmp_snooping
Success.
DGS3100#
```

### disable igmp_snooping

**Purpose**
To disable IGMP snooping on the Switch.

**Syntax**
```
disable igmp_snooping
```

**Description**
The `disable igmp_snooping` 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 or operator-level users can issue this command.

**Example usage:**
To disable IGMP snooping on the Switch:

```
DGS3100# disable igmp_snooping
Success.
DGS3100#
```

### show igmp_snooping

**Purpose**
To show the current status of IGMP snooping on the Switch.

**Syntax**
```
show igmp_snooping [vlan <vlan_name 32>]
```

**Description**
The `show igmp_snooping` command displays the current IGMP snooping configuration on the Switch.

**Parameters**
`<vlan_name 32>` - The name of the VLAN for which IGMP snooping configuration is to be displayed. Up to 32 characters can be used.

**Restrictions**
None.

**Example usage:**
To show igmp snooping:

```
DGS3100# show igmp_snooping
IGMP Snooping Global State : Disabled
```
show igmp_snooping group

Purpose: To display the current IGMP snooping group configuration on the Switch.

Syntax: show igmp_snooping group {vlan <vlan_name 32>}

Description: The `show igmp_snooping group` command displays the current IGMP snooping group configuration on the Switch.

Parameters:
- `<vlan_name 32>` - The name of the VLAN for which IGMP snooping group configuration information is to be displayed. Up to 32 characters can be used.

Restrictions: None.

Example usage:
To show igmp snooping group:

```
DGS3100# 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 : 3,4
Total Entries : 1

DGS3100#
```
Example usage:
To view the IGMP snooping forwarding table for VLAN ‘Trinity’:

```
DGS3100# show igmp_snooping forwarding vlan default
VLAN Name       : Trinity
Multicast group : 224.0.0.2
MAC address     : 01-00-5E-00-00-02
Port Member     : 3,4
Total Entries   : 1
```

```
DGS3100#
```

**show router_port**

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To display the currently configured router ports on the Switch.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>`show router_port {vlan &lt;vlan_name 32&gt;</td>
</tr>
<tr>
<td>Description</td>
<td>The <code>show router_port</code> command displays the router ports currently configured on the Switch.</td>
</tr>
<tr>
<td>Parameters</td>
<td><code>vlan &lt;vlan_name 32&gt;</code> – The name of the VLAN on which the router port resides. Up to 32 characters can be used.</td>
</tr>
<tr>
<td></td>
<td><code>static</code> – Displays router ports that have been statically configured.</td>
</tr>
<tr>
<td></td>
<td><code>dynamic</code> – Displays router ports that have been dynamically learned.</td>
</tr>
<tr>
<td></td>
<td><code>forbidden</code> – Displays router ports that have been forbidden configured.</td>
</tr>
</tbody>
</table>

Restrictions None.

Example usage:
To display the router ports.

```
DGS3100# show router_port
VLAN Name    : default
Static router port : 1-10
Dynamic router port : 
Total Entries: 1
```

DGS3100#
MLD SNOOPING COMMANDS

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable mld_snooping</td>
<td></td>
</tr>
<tr>
<td>disable mld_snooping</td>
<td></td>
</tr>
<tr>
<td>config mld_snooping</td>
<td>[&lt;vlan_name 32&gt;</td>
</tr>
<tr>
<td>config mld_snooping mrouter_port</td>
<td>&lt;vlan_name 32&gt; [add</td>
</tr>
<tr>
<td>config mld_snooping mrouter_port_forbidden</td>
<td>&lt;vlan_name 32&gt; [add</td>
</tr>
<tr>
<td>show mld_snooping</td>
<td>{vlan &lt;vlan_name 32&gt;}</td>
</tr>
<tr>
<td>show mld_snooping forwarding</td>
<td>{vlan &lt;vlan_name 32&gt;}</td>
</tr>
<tr>
<td>show mld_snooping group</td>
<td>{vlan &lt;vlan_name 32&gt;}</td>
</tr>
<tr>
<td>show mld_snooping mrouter_port</td>
<td>{vlan &lt;vlan_name 32&gt;</td>
</tr>
</tbody>
</table>

Each command is listed in detail, as follows:

**enable mld_snooping**

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To enable MLD snooping on the Switch.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>enable mld snooping</td>
</tr>
<tr>
<td>Description</td>
<td>The <strong>enable mld snooping</strong> command enables MLD snooping on the Switch.</td>
</tr>
<tr>
<td>Parameters</td>
<td>None</td>
</tr>
<tr>
<td>Restrictions</td>
<td>Only administrator or operator–level users can issue this command</td>
</tr>
</tbody>
</table>

Example usage:

To enable the MLD snooping:

```
DGS3100# enable mld_snooping

Success.
DGS3100#
```
**disable mld_snooping**

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To disable MLD snooping on the Switch.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>disable mld snooping</td>
</tr>
<tr>
<td>Description</td>
<td>The disable mld snooping command disables MLD snooping on the Switch.</td>
</tr>
<tr>
<td>Parameters</td>
<td>None</td>
</tr>
<tr>
<td>Restrictions</td>
<td>Only administrator or operator-level users can issue this command</td>
</tr>
</tbody>
</table>

**Example usage:**

To disable the MLD snooping:

DGS3100# disable mld_snooping

Success.
DGS3100#

**config mld_snooping**

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To configure mld snooping.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>config mld_snooping [&lt;vlan_name 32&gt;</td>
</tr>
<tr>
<td>Description</td>
<td>The config mld_snooping command defines mld snooping on the VLAN.</td>
</tr>
<tr>
<td>Parameters</td>
<td>vlan_name 32 – specifies that the mld snooping applies only to this previously created VLAN. all – specifies that MLD snooping is to be configured for all VLANs on the Switch. host_timeout – Specifies the maximum amount of time a host can be a member of a multicast group without the Switch receiving a host membership report. The default is 260 seconds. router_timeout – Specifies the maximum amount of time a route can be a member of a multicast group without the Switch receiving a host membership report done timer. The default is 300 seconds. done_timer – Specifies the maximum amount of time a host can be a member of a multicast group after sending a done timer membership report. The default is 10 seconds. state – Allows the user to enable or disable MLD snooping for the specified VLAN.</td>
</tr>
<tr>
<td>Restrictions</td>
<td>Only administrator or operator-level users can issue this command</td>
</tr>
</tbody>
</table>

**Example usage:**

To configure mld snooping:

DGS3100# config mld_snooping

Command:  config mld_snooping
mrouter_port Config Mld Snooping Router Port
mrouter_port_forbidden Config Mld Snooping Forbidden Router Port
### config mld_snooping mrouter_port

**Purpose**
To enable mld mrouter ports.

**Syntax**
```
config mld_snooping mrouter_port <vlan_name 32> [add | delete] <portlist>
```

**Description**
The `config mld_snooping mrouter_port` command defines a port that is connected to a multicast router port.

**Parameters**
- `vlan_name 32` – specifies that the mld snooping applies only to this previously created VLAN.
- `add` – Adds a specified port to the mld snooping mrouter port.
- `delete` – Deletes a specified port to the mld snooping mrouter port.
- `portlist` – Defines the ports to be included from the mld snooping mrouter group.

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

Separate non-consecutive Ethernet ports with a comma and no spaces; use a hyphen to designate a range of ports. These ports are defined as connected to a multicast router.

**Example usage:**
To enable mld mrouter ports:
```
DGS3100# config mld_snooping mrouter_port default add 1
Success.
DGS3100#
```
To define the MLD snooping mrouter forbidden:

DGS3100# config mld_snooping mrouter_port_forbidden default add all
Success.
DGS3100#

show mld snooping

Purpose To display mld snooping settings on the Switch.
Syntax `show mld snooping {vlan <vlan_name 32>}`
Description The `show mld snooping` command displays a port from being defined as a multicast router port by static configuration or by automatic learning.
Parameters `vlan_name 32` – Specifies that the mld snooping applies only to this previously created VLAN.
Restrictions Only administrator or operator-level users can issue this command

Example usage:
To show the MLD snooping:

DGS3100# show mld_snooping
MLD Snooping Global State : Disabled
Multicast Filtering : Enabled
Vlan Name : default
Host Timeout : 260
Done Timer : 10
Route Timeout : 300
State : Disabled
DGS3100#

show mld_snooping forwarding

Purpose To display mld snooping settings on the Switch.
Syntax `show mld_snooping forwarding {vlan <vlan_name 32>}`
Description The `show mld_snooping forwarding` command displays the current MLD snooping forwarding table entries currently configured on the Switch.
Parameters `vlan_name 32` – Specifies that the mld snooping applies only to this previously created VLAN.
Restrictions Only administrator or operator-level users can issue this command.

Example usage:
To display the MLD snooping forwarding:
show mld_snooping groups

**Purpose**
To display mld snooping group settings on the Switch.

**Syntax**
```
show mld_snooping groups {vlan <vlan_name 32>}
```

**Description**
The `show mld_snooping groups` command displays the multicast groups that were learned by MLD snooping.

**Parameters**
- `vlan <vlan_name 32>` – Specifies on which VLAN mld snooping groups should be shown.

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

**Example usage:**
To show the MLD snooping groups:

```
DGS3100#
```

TBD

```
DGS3100#
```

show mld_snooping mrouter_port

**Purpose**
To display information on dynamically learnt and static multicast router interfaces.

**Syntax**
```
show mld_snooping mrouter_port {vlan <vlan_name 32> | static | dynamic | forbidden}
```

**Description**
The `show mld_snooping mrouter_port` command displays on dynamically learnt and static multicast router interfaces.

**Parameters**
- `vlan_name 32` – Displays MLD router ports on specific VLAN.
- `Static` – Displays statically configured MLD router ports.
- `Dynamic` – Displays dynamically configured MLD router ports.
- `Forbidden` – Displays forbidden MLD ports

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

Separate non-consecutive Ethernet ports with a comma and no spaces; use a hyphen to designate a range of ports. These ports are defined as connected to a multicast router.

**Example usage:**
To show the MLD_snooping mrouterport:

```
DGS3100# show mld_snooping mrouter_port
VLAN Name : default
Static router port : (1–48)
```

```
Dynamic router port :
Forbidden router port :

Total Entries: 1

DGS3100#

Success.

DGS3100#
### 802.1X COMMANDS

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable 802.1x</td>
<td></td>
</tr>
<tr>
<td>disable 802.1x</td>
<td></td>
</tr>
<tr>
<td>config 802.1x</td>
<td>&lt;feap&gt; [enable</td>
</tr>
<tr>
<td>show 802.1x auth_state</td>
<td>{ports &lt;portlist&gt;}</td>
</tr>
<tr>
<td>show 802.1x auth_configuration</td>
<td>{ports &lt;portlist&gt;}</td>
</tr>
<tr>
<td>config 802.1x auth_parameter ports</td>
<td>[&lt;portlist&gt;</td>
</tr>
<tr>
<td>config 802.1x init</td>
<td>port_based ports [&lt;portlist&gt;</td>
</tr>
<tr>
<td>config 802.1x auth_protocol</td>
<td>[radius</td>
</tr>
<tr>
<td>config 802.1x reauth</td>
<td>port_based ports [&lt;portlist&gt;</td>
</tr>
<tr>
<td>config radius add</td>
<td>&lt;server_ip&gt;</td>
</tr>
<tr>
<td>config radius delete</td>
<td>&lt;server_ip&gt;</td>
</tr>
<tr>
<td>config radius</td>
<td>&lt;server_ip&gt;</td>
</tr>
<tr>
<td>show radius</td>
<td></td>
</tr>
<tr>
<td>config 802.1x auth_mode</td>
<td>ports &lt;portlist&gt;</td>
</tr>
<tr>
<td>create 802.1x guest_vlan</td>
<td>&lt;vlan_name 32&gt; state [enable</td>
</tr>
<tr>
<td>delete 802.1x guest_vlan</td>
<td></td>
</tr>
<tr>
<td>config 802.1x guest_vlan ports</td>
<td>&lt;portlist&gt; state [enable</td>
</tr>
<tr>
<td>show 802.1x guest_vlan</td>
<td></td>
</tr>
</tbody>
</table>

Each command is listed in detail, as follows:
**enable 802.1x**

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To enable the 802.1x server on the Switch.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>enable 802.1x</code></td>
</tr>
<tr>
<td>Description</td>
<td>The <code>enable 802.1x</code> command enables the 802.1x Port-based Network Access control server application on the Switch.</td>
</tr>
<tr>
<td>Parameters</td>
<td>None.</td>
</tr>
<tr>
<td>Restrictions</td>
<td>Only Administrator or operator-level users can issue this command.</td>
</tr>
</tbody>
</table>

**Example usage:**

To enable 802.1x switch wide:

```plaintext
DGS3100# enable 802.1x
Success.
DGS3100#
```

**disable 802.1x**

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To disable the 802.1x server on the Switch.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>disable 802.1x</code></td>
</tr>
<tr>
<td>Description</td>
<td>The <code>disable 802.1x</code> command disables the 802.1x Port-based Network Access control server application on the Switch.</td>
</tr>
<tr>
<td>Parameters</td>
<td>None.</td>
</tr>
<tr>
<td>Restrictions</td>
<td>Only Administrator or operator-level users can issue this command.</td>
</tr>
</tbody>
</table>

**Example usage:**

To disable 802.1x on the Switch:

```plaintext
DGS3100# disable 802.1x
Success.
DGS3100#
```

**config 802.1x**

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To configure the 802.1x feap on the Switch.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>`config 802.1x &lt;feap&gt; [enable</td>
</tr>
<tr>
<td>Description</td>
<td>The <code>config 802.1x</code> command configure the 802.1x feap on the Switch.</td>
</tr>
<tr>
<td>Parameters</td>
<td>`&lt;feap&gt; [enable</td>
</tr>
<tr>
<td>Restrictions</td>
<td>Only Administrator or operator-level users can issue this command.</td>
</tr>
</tbody>
</table>

**Example usage:**

To configure 802.1x feap on the Switch:
show 802.1x auth_state

Purpose
To display the current authentication state of the 802.1x server on the Switch.

Syntax
show 802.1x auth_state {ports <portlist>}

Description
The show 802.1x auth_state command displays the current 802.1x authentication state of the specified ports of the Port-based Network Access Control server application on the Switch.

The following details are displayed:
- Port number - Shows the physical port number on the Switch.
- Auth PAE State: Initialize / Disconnected / Connecting / Authenticating / Authenticated / Held / ForceAuth / ForceUnauth - Shows the current state of the Authenticator PAE.
- Backend State: Request / Response / Fail / Idle / Initialize / Success / Timeout - Shows the current state of the Backend Authenticator.
- Port Status: Authorized / Unauthorized - Shows the result of the authentication process. Authorized means that the user was authenticated, and can access the network. Unauthorized means that the user was not authenticated, and cannot access the network.

Parameters
ports <portlist> - A port or range of ports whose settings are to be displayed.

Restrictions
Only Administrator or operator-level users can issue this command.

Example usage:
To display the 802.1x authentication states (stacking disabled) for Port-based 802.1x:

DGS3100# show 802.1x auth_state ports 1:1-5

<table>
<thead>
<tr>
<th>Port</th>
<th>Auth PAE State</th>
<th>Backend State</th>
<th>Port Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>forceAuth</td>
<td>initialize</td>
<td>authorized</td>
</tr>
<tr>
<td>2</td>
<td>initialize</td>
<td>initialize</td>
<td>authorized</td>
</tr>
<tr>
<td>3</td>
<td>initialize</td>
<td>initialize</td>
<td>authorized</td>
</tr>
<tr>
<td>4</td>
<td>initialize</td>
<td>initialize</td>
<td>authorized</td>
</tr>
<tr>
<td>5</td>
<td>forceAuth</td>
<td>initialize</td>
<td>authorized</td>
</tr>
</tbody>
</table>

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

show 802.1x auth_configuration

Purpose
To display the current configuration of the 802.1x server on the Switch.
**Syntax**

```
show 802.1x auth_configuration {ports <portlist>}
```

**Description**

The `show 802.1x auth_configuration` command displays the current configuration of the 802.1x Port-based Network Access Control server application on the Switch.

The following details are displayed:

- **802.1x**: Enabled/Disabled - Shows the current status of 802.1x functions on the Switch.
- **Authentication Mode**: Port-based/Mac-based/None - Shows the 802.1x authorization mode.
- **Authentication Method**: Remote/none - Shows the type of authentication protocol suite in use between the Switch and a RADIUS server.
- **Port number** - Shows the physical port number on the Switch.
- **AdminCrlDir**: Both/In - Shows whether a controlled Port that is unauthorized will exert control over communication in both receiving and transmitting directions, or just the receiving direction.
- **OpenCrlDir**: Both/In - Shows whether a controlled Port that is unauthorized will exert control over communication in both receiving and transmitting directions, or just the receiving direction.
- **Port Control**: ForceAuth/ForceUnauth/Auto - Shows the administrative control over the port's authorization status. ForceAuth forces the Authenticator of the port to become Authorized. ForceUnauth forces the port to become Unauthorized.
- **QuietPeriod** - Shows the time interval between authentication failure and the start of a new authentication attempt.
- **TxPeriod** - Shows the time to wait for a response from a supplicant (user) to send EAP Request/Identity packets.
- **SuppTimeout** - Shows the time to wait for a response from a supplicant (user) for all EAP packets, except for the Request/Identity packets.
- **ServerTimeout** - Shows the length of time to wait for a response from a RADIUS server.
- **MaxReq** - Shows the maximum number of times to retry sending packets to the supplicant.
- **ReAuthPeriod** - Shows the time interval between successive reauthentications.
- **ReAuthenticate**: true/false - Shows whether or not to reauthenticate.

**Parameters**

*ports <portlist>* - Specifies a port or range of ports to be viewed.

**Restrictions**

Only Administrator or operator-level users can issue this command.

---

**Example usage:**

To display the 802.1x configurations:

```
DGS3100# show 802.1x auth_configuration ports 1

<table>
<thead>
<tr>
<th>802.1X</th>
<th>: Enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Mode</td>
<td>: Port_based</td>
</tr>
<tr>
<td>Authentication Method</td>
<td>: None</td>
</tr>
<tr>
<td>Port number</td>
<td>: 1</td>
</tr>
<tr>
<td>AdminCrlDir</td>
<td>: both</td>
</tr>
</tbody>
</table>
```
**OpenCrlDir** : both
**Port Control** : forceAuthorized
**QuietPeriod** : 60 sec
**TxPeriod** : 30 sec
**SuppTimeout** : 30 sec
**ServerTimeout** : 30 sec
**MaxReq** : 2 times
**ReAuthPeriod** : 3600 sec
**ReAuthenticate** : false

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

---

### config 802.1x auth_parameter ports

**Purpose**
To configure the 802.1x authentication parameters on a range of ports. The default parameter returns all ports in the specified range to their default 802.1x settings.

**Syntax**
```
cfg 802.1x auth_parameter ports [<portlist> | all] [default | { port_control [force_unauth | auto | force_auth] | quiet_period <sec 0-65535> | tx_period <sec 1-65535> | supp_timeout <sec 1-65535> | server_timeout <sec 1-65535> | max_req <value 1-10> | reauth_period <sec 300-4294967295> | enable_reauth [enable | disable]]]
```

**Description**
The `config 802.1x auth_parameter ports` command configures the 802.1x authentication parameters on a range of ports. The default parameter returns all ports in the specified range to their default 802.1x settings.

**Parameters**
- `<portlist>` – A port or range of ports to be configured.
- `all` – Specifies all of the ports on the Switch.
- `default` – Returns all of the ports in the specified range to their 802.1x default settings.
- `port_control` – Configures the administrative control over the authentication process for the range of ports. The options are:
  - `force_auth` – Forcibly authenticates the port to become authorized. Network access is allowed.
  - `auto` – Allows the port’s status to reflect the outcome of the authentication process.
  - `force_unauth` – Forcibly de-authenticates the port to become unauthorized. Network access is blocked.
- `quiet_period <sec 0-65535>` – Configures the time interval between authentication failure and the start of a new authentication attempt.
- `tx_period <sec 1-65535>` - Configures the time to wait for a response from a supplicant (user) to send EAP Request/Identity packets.
- `supp_timeout <sec 1-65535>` - Configures the time to wait for a response from a supplicant (user) for all EAP packets, except for the Request/Identity packets.
- `server_timeout <sec 1-65535>` - Configures the length of time to wait for a response from a RADIUS server.
- `max_req <value 1-10>` – Configures the number of times to retry
sending packets to a supplicant (user).

\texttt{reauth\_period \textless sec 300-4294967295\textgreater } – Configures the time interval between successive re-authentications.

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

\begin{center}
\textbf{Restrictions}
Only Administrator or operator-level users can issue this command.
\end{center}

\textbf{Example usage:}
To configure 802.1x authentication parameters for ports 1 – 20:

\begin{center}
\verb|DGS3100# config 802.1x auth\_parameter ports 1–20 direction both|
\end{center}

\verb|Success.|

\begin{center}
\verb|DGS3100#|
\end{center}

\begin{center}
\textbf{config 802.1x init}
\end{center}

\begin{center}
\textbf{Purpose} To initialize the 802.1x function on a range of ports.
\textbf{Syntax} \texttt{config 802.1x init port\_based ports \textless portlist\textgreater | all}
\textbf{Description} The \texttt{config 802.1x init} command initializes the 802.1x functions on a specified range of ports or for specified MAC addresses operating from a specified range of ports.
\textbf{Parameters} \texttt{port\_based} – Instructs the Switch to initialize 802.1x functions based only on the port number. Ports approved for initialization can then be specified.
\texttt{ports \textless portlist\textgreater} – A port or range of ports to be configured.
\texttt{all} – Specifies all of the ports on the Switch.
\textbf{Restrictions} Only Administrator or operator-level users can issue this command.
\end{center}

\textbf{Example usage:}
To initialize the authentication state machine of all ports:

\begin{center}
\verb|DGS3100# config 802.1x init port\_based ports all|
\end{center}

\verb|Success.|

\begin{center}
\verb|DGS3100#|
\end{center}

\begin{center}
\textbf{config 802.1x auth\_protocol}
\end{center}

\begin{center}
\textbf{Purpose} To configure the 802.1x authentication protocol on the Switch.
\textbf{Syntax} \texttt{config 802.1x auth\_protocol [radius | none]}
\textbf{Description} The \texttt{config 802.1x auth\_protocol} command enables configuration of the authentication protocol.
\textbf{Parameters} \texttt{radius} – Uses the list of RADIUS servers for authentication.
\end{center}
none – Uses no authentication.

Restrictions Only Administrator or operator-level users can issue this command.

Example usage:
To configure the RADIUS (AAA) authentication protocol on the Switch:

```
DGS3100# config 802.1x auth_protocol radius
Success.
DGS3100#
```

`config 802.1x reauth` Purpose To configure the 802.1x re-authentication feature of the Switch.

Syntax `config 802.1x reauth port_based ports [<portlist> | all]`

Description The `config 802.1x reauth` command re-authenticates a previously authenticated device based on port number.

Parameters `port_based` – Instructs the Switch to re-authorize 802.1x functions based only on the port number. Ports approved for re-authorization can then be specified.
`ports <portlist>` – A port or range of ports to be re-authorized.
`all` – Specifies all of the ports on the Switch.

Restrictions Only Administrator or operator-level users can issue this command.

Example usage:
To configure 802.1x reauthentication for ports 1-18:

```
DGS3100# config 802.1x reauth port_based ports 1-18
Success.
DGS3100#
```

`config radius add` Purpose To configure the settings the Switch uses to communicate with a RADIUS server.

Syntax `config radius add [server_ip] [key passwd 128] [default | {auth_port <udp_port_number 1-65535> | acct_port <udp_port_number 1-65535>}]`

Description The `config radius add` command configures the settings the Switch uses to communicate with a RADIUS server.

Parameters `server_ip` – The IP address of the RADIUS server.
`key` – Specifies that a password and encryption key are to be used between the Switch and the RADIUS server.
`passwd 128` – The shared-secret key used by the RADIUS server and the Switch. Up to 128 characters can be used.
default – Uses the default udp port number in both the auth_port and acct_port settings.
auth_port <udp_port_number 1-65535> – The UDP port number for authentication requests. The default is 1812.
acct_port <udp_port_number 1-65535> – The UDP port number for accounting requests. The default is 1813.

Restrictions Only Administrator or operator-level users can issue this command.

Example usage:
To configure the RADIUS server communication settings:

```
DGS3100# config radius add 10.48.74.121 key dlink default
Success.
DGS3100#
```

```
config radius delete
Purpose To delete a previously entered RADIUS server configuration.
Syntax config radius delete <server_ip>
Description The config radius delete command deletes a previously entered RADIUS server configuration.
Parameters <server_ip> – The IP address of the RADIUS server.
Restrictions Only Administrator or operator-level users can issue this command.
Example usage:
To delete previously configured RADIUS server communication settings:

```
DGS3100# config radius delete 10.48.74.121
Success.
DGS3100#
```

```
config radius
Purpose To configure the Switch’s RADIUS settings.
Syntax config radius <server_ip> { | key <passwd 128> | auth_port <udp_port_number 1-65535> | acct_port <udp_port_number 1-65535> }
Description The config radius command configures the Switch’s RADIUS settings.
Parameters <server_ip> – The IP address of the RADIUS server.
key – Specifies that a password and encryption key are to be used between the Switch and the RADIUS server.
  • <passwd 128> – The shared-secret key used by the RADIUS server and the Switch. Up to 128 characters can be used.
```
auth_port <udp_port_number 1-65535> – The UDP port number for authentication requests. The default is 1812.
acct_port <udp_port_number 1-65535> – The UDP port number for accounting requests. The default is 1813.

Restrictions
Only Administrator or operator-level users can issue this command.

Example usage:
To configure the RADIUS settings:

DGS3100# config radius 10.48.74.121 key dlink default
Success.
DGS3100#

show radius

Purpose
To display the current RADIUS configurations on the Switch.

Syntax
show radius

Description
The show radius command displays the current RADIUS configurations on the Switch.

Parameters
None.

Restrictions
None.

Example usage:
To display RADIUS settings on the Switch:

DGS3100# show radius

<table>
<thead>
<tr>
<th>Index</th>
<th>IP Address</th>
<th>Auth-Port Number</th>
<th>Acct-Port Number</th>
<th>Status</th>
<th>Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>10.1.1.1</td>
<td>1812</td>
<td>1813</td>
<td>Active</td>
<td>switch</td>
</tr>
</tbody>
</table>

DGS3100#

config 802.1x auth_mode

Purpose
To configure the 802.1x authentication mode on the Switch.

Syntax
config 802.1x auth_mode ports <portlist> [port_based | mac_based]

Description
The config 802.1x auth_mode command enables either the port-based or MAC-based 802.1x authentication feature on the Switch.

Parameters
portlist – A port or a range of ports to be configured.
[port_based | mac_based] – Specifies whether 802.1x authentication is by port or MAC address.

Restrictions
Only Administrator or operator-level users can issue this command.
Example usage:
To configure 802.1x authentication by MAC address:

```
DGS3100# config 802.1x auth_mode mac_based
Success.
DGS3100#
```

<table>
<thead>
<tr>
<th>create 802.1x guest_vlan</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td><strong>Syntax</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td><strong>Parameters</strong></td>
</tr>
<tr>
<td><strong>Restrictions</strong></td>
</tr>
</tbody>
</table>

Example usage:
To create a 802.1x Guest VLAN:

```
DGS3100# create 802.1x guest_vlan
DGS3100#
```

<table>
<thead>
<tr>
<th>delete 802.1x guest_vlan ports</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td><strong>Syntax</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td><strong>Parameters</strong></td>
</tr>
<tr>
<td><strong>Restrictions</strong></td>
</tr>
</tbody>
</table>

Example usage:
To delete a 802.1x Guest VLAN

```
DGS3100# delete 802.1x guest_vlan
DGS3100#
```
### config 802.1x guest_vlan ports

**Purpose**
Defines a port or range of ports to be members of the Guest VLAN.

**Syntax**
```
config 802.1x guest_vlan ports <portlist> state [enable | disable]
```

**Description**
The `config 802.1x guest_vlan ports` command defines a port or range of ports to be members of the 802.1x Guest VLAN. The 802.1x Guest VLAN can be configured to provide limited network access to authorized member ports. If a member port is denied network access via port–based authorization, but the 802.1x Guest VLAN is enabled, the member port receives limited network access. For example, a network administrator can use the 802.1x Guest VLAN to deny internal network access via port–based authentication, but grant Internet access to unauthorized users.

**Parameters**
- `portlist` – A port or range of ports to be configured to the Guest VLAN.
- `All` – Indicates all ports to be configured to the guest vlan.

**Restrictions**
Only Administrator or operator–level users can issue this command.

**Example usage:**
To configure ports to the Guest VLAN

```
DGS3100# config 802.1x guest_vlan ports 1 enable
DGS3100#
```

### show 802.1x guest_vlan

**Purpose**
Displays configuration information for the Guest VLAN.

**Syntax**
```
show 802.1x guest_vlan
```

**Description**
The `show 802.1x guest_vlan` command displays the Guest VLAN name, state, and member ports.

**Parameters**
None.

**Restrictions**
None.

**Example usage:**
To display the Guest VLAN configuration information:

```
DGS3100# show 802.1x guest_vlan
Guest VLAN Table
Guest VLAN            : Enable
Guest VLAN name : guestusers
Member                   : 1
DGS3100#
```
MAC AUTHENTICATION COMMANDS

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable mac_based_access_control</td>
<td></td>
</tr>
<tr>
<td>disable mac_based_access_control</td>
<td></td>
</tr>
<tr>
<td>config mac_based_access_control</td>
<td>{ports [&lt;portlist&gt;</td>
</tr>
<tr>
<td>show mac_based_access_control</td>
<td>{ports [&lt;portlist&gt;</td>
</tr>
</tbody>
</table>

Each command is listed in detail, as follows:

**enable mac_based_access_control**

- **Purpose**: To globally enable MAC based access control.
- **Syntax**: `enable mac_based_access_control`
- **Description**: The `enable mac_based_access_control` command enables the functionality of MAC-based access control globally on the switch. This command also enables 802.1x globally if it is disabled, as 802.1x functionality is used to activate MAC authentication. If ports on the switch are configured to MAC-based mode, this command sets the port state to auto. To achieve this, the `enable` command runs the following 802.1x command on these ports:
  - `config 802.1x auth_parameter ports 1:2 port_control auto`
- **Parameters**: None.
- **Restrictions**: None.

**Example usage:**

To enable MAC Based Access Control:

```
DGS3100# enable mac_based_access_control
DGS3100#
```
### disable mac_based_access_control

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To globally disable MAC based access control.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>disable mac_based_access_control</code></td>
</tr>
<tr>
<td>Description</td>
<td>The <code>disable mac_based_access_control</code> command disables the functionality of MAC-based access control globally on the switch. This command disables 802.1x if it is enabled, as 802.1x functionality is used to activate MAC authentication. However, if ports activated to the standard ‘Port Based 802.1x’ exist, 802.1x is not disabled globally, and only the MAC Based authentication configured ports move to a ‘Forced Authorized’ state.</td>
</tr>
<tr>
<td>Parameters</td>
<td>None.</td>
</tr>
<tr>
<td>Restrictions</td>
<td>None.</td>
</tr>
</tbody>
</table>

Example usage:
To disable MAC Based Access Control:

```
DGS3100# disable mac_based_access_control
DGS3100#
```

### config mac_based_access_control

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To enable/disable MAC based access control on a port(s).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>`config mac_based_access_control {ports [&lt;portlist&gt;</td>
</tr>
</tbody>
</table>
| Description      | The `config mac_based_access_control` command enables or disables the functionality of MAC-based access control on a port(s). When using command to enable functionality: This command enables 802.1x on the port(s), as 802.1x functionality is used to activate MAC authentication. This command also configures RADIUS as the authenticating protocol for 802.1x. To achieve this, the enable command runs the following 802.1x commands:  
- `config 802.1x auth_parameter ports 1:2 enable_reauth enable`  
- `config 802.1x auth_parameter ports 1:2 port_control auto`  
- `config 802.1x auth_mode mac_base ports 1:2`  
- `config 802.1x auth_protocol radius`  

**Important note:** In order to complete the activation of MAC authentication, the related ports must be configured as members in the guest VLAN. When using this command to disable functionality on a port or ports, this command returns the port(s) to the default settings. To achieve this, the disable command removes the following commands (configured by the enable command) from port:  
- `config 802.1x auth_parameter ports 1:2 enable_reauth enable`  
- `config 802.1x auth_parameter ports 1:2 port_control auto`  
- `config 802.1x auth_mode mac_base ports 1:2`  

<table>
<thead>
<tr>
<th>Parameters</th>
<th><code>&lt;portlist&gt;</code> – A port or range of ports whose MAC authentication is enabled/disabled on it.</th>
</tr>
</thead>
</table>
<state> – This parameter defines whether the port or range of ports will be enabled or disabled.

Restrictions This command can only be entered if the global command 'enable mac_based_access_control' was previously entered.

Example usage:
To enable MAC Based Access Control on port or port list:

DGS3100# config mac_based_access_control ports 1:1-5 state enable
DGS3100#

show mac_based_access_control

Purpose To show the port MAC authentication status.
Syntax show mac_based_access_control {ports [<portlist> | all]}
Description The `show mac_based_access_control` command displays MAC authentication status on the configured ports.
Parameters <portlist> – A port or range of ports displayed with the MAC authentication status.
all – displays all ports with the MAC authentication status.
Restrictions None.

Example usage:
To display MAC Based Access Control on port or port list:

DGS3100# show mac_based_access_control
MAC Based Access Control
----------------------------------------
State : Enabled
Method : Radius
DGS3100# show mac_based_access_control ports 1:5

Port State
-------- --------
5 Enabled

DGS3100#
PORT SECURITY COMMANDS

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>config port_security</td>
<td>[&lt;portlist&gt;</td>
</tr>
<tr>
<td>show port_security</td>
<td>&lt;portlist&gt;</td>
</tr>
</tbody>
</table>

Each command is listed in detail, as follows:
### config port_security

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To configure port security settings.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>config port_security [&lt;portlist&gt;</td>
</tr>
<tr>
<td>Description</td>
<td>The <code>config port_security</code> command configures port security settings for specific ports.</td>
</tr>
</tbody>
</table>
| Parameters | **portlist** – A port or range of ports to be configured.  
**all** – Configures port security for all ports on the Switch.  
**admin_state [enable | disable]** – Enables or disables port security for the listed ports.  
**max_learning_addr <int 0-64>** -  
1-64 Limits the number of MAC addresses dynamically listed in the FDB for the ports.  
**lock_address_mode** – Defines the TBD and contains the following options:  
- **Permenant** – Learns up to the maximum number of dynamic addresses allowed on the port. The learned addresses are not aged out or relearned on other port for as long as the port is locked.  
- **DeleteOnReset** – Deletes the current dynamic MAC addresses associated with the port. Learn up to the maximum addresses allowed on the port (this number is also configurable). Aging is disabled; the addresses are deleted on reset  
- **DeleteOnTimeout** – Deletes the current dynamic MAC addresses associated with the port. The port learns up to the maximum addresses allowed on the port. Re-learned MAC addresses and address aging out are also enabled. The MAC addresses are deleted when the device is reset and on when the address is aged out.  
**trap <interval 1-1000000>** - Sends SNMP traps and defines the minimum amount of time in seconds between consecutive traps. |
| Restrictions | Only administrator or operator-level users can issue this command |

### Example usage:

To configure port security:

```
DGS3100# config port_security 1-5 admin_state enable max_learning_addr 5 lock_address_mode deleteontimeout trap 50
Success.
DGS3100#
```
show port_security

Purpose: To display the current port security configuration.

Syntax: `show port_security {<portlist>}`

Description: The `show port_security` command displays port security information for the Switch’s ports. The information displayed includes port security, admin state, maximum number of learning address and lock mode and trap interval.

Parameters: `<portlist>` – A port or range of ports whose settings are to be displayed.

Restrictions: None.

Example usage:
To display the port security configuration:

```
DGS3100# show port_security ports 1:1-5

<table>
<thead>
<tr>
<th>Port</th>
<th>Admin state</th>
<th>Max.Learning Addr.</th>
<th>Lock Address Mode</th>
<th>Trap interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>1:1</td>
<td>Disabled</td>
<td>1</td>
<td>DeleteOnReset</td>
<td>10</td>
</tr>
<tr>
<td>1:2</td>
<td>Disabled</td>
<td>1</td>
<td>DeleteOnReset</td>
<td>10</td>
</tr>
<tr>
<td>1:3</td>
<td>Disabled</td>
<td>1</td>
<td>DeleteOnReset</td>
<td>10</td>
</tr>
<tr>
<td>1:4</td>
<td>Disabled</td>
<td>1</td>
<td>DeleteOnReset</td>
<td>10</td>
</tr>
<tr>
<td>1:5</td>
<td>Disabled</td>
<td>1</td>
<td>DeleteOnReset</td>
<td>10</td>
</tr>
</tbody>
</table>

DGS3100#
```
The Time and SNTP commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

<table>
<thead>
<tr>
<th>Command</th>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>config sntp</td>
<td>{primary &lt;ipaddr&gt;</td>
</tr>
<tr>
<td>show sntp</td>
<td></td>
</tr>
<tr>
<td>enable sntp</td>
<td></td>
</tr>
<tr>
<td>disable sntp</td>
<td></td>
</tr>
<tr>
<td>config time date</td>
<td>&lt;date ddmmyyyy&gt; &lt;time hh:mm:ss&gt;</td>
</tr>
<tr>
<td>config time_zone</td>
<td>{operator [+ hour &lt;gmt_hour 0-13&gt; minute &lt;minute 0-59&gt;</td>
</tr>
<tr>
<td>config dst</td>
<td>[disable</td>
</tr>
<tr>
<td>show time</td>
<td></td>
</tr>
</tbody>
</table>

Each command is listed in detail, as follows:

**config sntp**

**Purpose**
To setup SNTP service.

**Syntax**
cfg snntp (primary <ipaddr> | secondary <ipaddr> | poll-interval <int 60-86400>)

**Description**
The config sntp command configures SNTP service from an SNTP server. SNTP must be enabled for this command to function (See enable snntp).

**Parameters**
- primary <ipaddr> – Specifies the IP address of the primary SNTP server.
- secondary <ipaddr> – Specifies the IP address of the secondary SNTP server.
- poll-interval <int 60-86400> – The interval between requests for updated SNTP information. The polling interval ranges from 60 seconds (1 minute) to 86,400 seconds (1 day).

**Restrictions**
Only administrator or operate-level users can issue this command. SNTP service must be enabled for this command to function (enable sntp).

**Example usage:**
To configure SNTP settings:
DGS3100# config sntp primary 10.1.1.1 secondary 10.1.1.2 poll-interval 60
Success.
DGS3100#

**show sntp**

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To display the SNTP information.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>show sntp</td>
</tr>
<tr>
<td>Description</td>
<td>The <code>show sntp</code> command displays SNTP settings information, including the source IP address, time source and poll interval.</td>
</tr>
<tr>
<td>Parameters</td>
<td>None.</td>
</tr>
<tr>
<td>Restrictions</td>
<td>None.</td>
</tr>
</tbody>
</table>

**Example usage:**

To display SNTP configuration information:

```
DGS3100# show sntp
Current Time Source : System Clock
SNTP Primary Server : 10.1.1.1
SNTP Secondary Server : 10.1.1.2
SNTP Poll Interval : 30 sec
DGS3100#
```

**enable sntp**

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To enable SNTP server support.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>enable sntp</td>
</tr>
<tr>
<td>Description</td>
<td>The <code>enable sntp</code> command enables SNTP server support. SNTP service must be separately configured (see <code>config sntp</code>). Enabling and configuring SNTP support override any manually configured system time settings.</td>
</tr>
<tr>
<td>Parameters</td>
<td>None.</td>
</tr>
<tr>
<td>Restrictions</td>
<td>Only administrator and Operator-level users can issue this command. SNTP settings must be configured for SNTP to function (<code>config sntp</code>).</td>
</tr>
</tbody>
</table>

**Example usage:**

To enable the SNTP function:

```
DGS3100# enable sntp
Success.
DGS3100#
```
**disable sntp**

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To disable SNTP server support.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>disable sntp</code></td>
</tr>
<tr>
<td>Description</td>
<td>The <code>disable sntp</code> command disables SNTP support.</td>
</tr>
<tr>
<td>Parameters</td>
<td>None.</td>
</tr>
<tr>
<td>Restrictions</td>
<td>Only administrator or operator level users can issue this command.</td>
</tr>
</tbody>
</table>

**Example usage:**

To disable SNTP support:

```
DGS3100# disable sntp
Success.
DGS3100#
```

**config time date**

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To manually configure system time and date settings.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>config time date &lt;date ddmmyyyy&gt; &lt;time hh:mm:ss&gt;</code></td>
</tr>
<tr>
<td>Description</td>
<td>The <code>config time date</code> command configures the system time and date settings. These will be overridden if SNTP is configured and enabled.</td>
</tr>
</tbody>
</table>
| Parameters       | `date <ddmmyyyy>` – Specifies the date, using two numerical characters for the day of the month, two numerical characters for the name of the month, and four numerical characters for the year. For example: 03072008.  
`Time <hh:mm:ss>` – Specifies the system time, using the format hh:mm:ss; that is, two numerical characters each for the hour using a 24-hour clock, the minute and second. For example: 19:42:30. |
| Restrictions     | Only administrator or operate-level users can issue this command. Manually configured system time and date settings are overridden if SNTP support is enabled. |

**Example usage:**

To manually set system time and date settings:

```
DGS3100# config time 30072008 16:30:30
Success.
DGS3100#
```
config time_zone

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To determine the time zone used in order to adjust the system clock.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>\texttt{config time_zone {operator [+ hour &lt;gmt_hour 0-13&gt;] minute &lt;minute 0-59&gt; [- hour &lt;gmt_hour 0-12&gt;] minute &lt;minute 0-59&gt;}}</td>
</tr>
<tr>
<td>Description</td>
<td>The <code>config time_zone</code> command adjusts the system clock settings according to the time zone. Time zone settings adjust SNTP information accordingly.</td>
</tr>
<tr>
<td>Parameters</td>
<td>\begin{itemize} \item \texttt{operator} – May be (+) to add or (-) to subtract time to adjust for time zone relative to GMT. \item \texttt{hour &lt;gmt_hour 0-13&gt;} – Specifies the number of hours difference from GMT. \item \texttt{Minute &lt;minute 0-59&gt;} – Specifies the number of minutes added or subtracted to adjust the time zone. \end{itemize}</td>
</tr>
<tr>
<td>Restrictions</td>
<td>Only administrator or operator level users can issue this command.</td>
</tr>
</tbody>
</table>

Example usage:

To configure time zone settings:

```
DGS3100# config time_zone operator + hour 2 min 30
Success.
DGS3100#
```

config dst

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To configure time adjustments to allow for the use of Daylight Saving Time (DST).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>\texttt{config dst {disable</td>
</tr>
<tr>
<td>Description</td>
<td>The <code>config dst</code> command disables or configures Daylight Saving Time (DST). When enabled, this adjusts the system clock to comply with any DST requirement. DST adjustment affects system time for both manually configured time and time set using SNTP service.</td>
</tr>
<tr>
<td>Parameters</td>
<td>\begin{itemize} \item \texttt{disable} - Disables the DST seasonal time adjustment for the Switch. \item \texttt{repeating} - Enables DST seasonal time adjustment on a repeating basis. Repeating mode requires that the DST beginning and ending date be specified using a formula. For example, specify to begin DST on Saturday during the second week of April and end DST on Sunday during the last week of October. The format for repeating mode is as follows, and in the order listed: \begin{itemize} \item \texttt{&lt;week 1-4,last&gt;} - The week of the month in which DST begins, where 1 is the first week, 2 is the second week and so on, and last is the last week of the month. \item \texttt{&lt;day sun-sat&gt;} - The weekday on which DST begins, expressed using a three character abbreviation (sun, mon, tue, wed, thu, fri, sat) \item \texttt{&lt;month 1-12&gt;} - The month of the year to begin DST, \end{itemize} \end{itemize} \end{itemize}</td>
</tr>
</tbody>
</table>

Example usage:

To configure DST settings:

```
DGS3100# config dst repeating {week sun sat month 4 week sun sat month 10 offset 60}
Success.
DGS3100#
```
expressed numerically.
- `<hh:mm>` - The time of day to begin DST in hours and minutes, expressed using a 24-hour clock.
- `<week 1-4,last>` - The week of the month in which DST ends, where 1 is the first week, 2 is the second week and so on, and last is the last week of the month.
- `<day sun-sat>` - The weekday on which DST ends, expressed using a three character abbreviation (sun, mon, tue, wed, thu, fri, sat)
- `<month 1-12>` - The month of the year to end DST, expressed numerically.
- `<hh:mm>` - The time of day to end DST, in hours and minutes, expressed using a 24-hour clock.

**annual** - Enables DST seasonal time adjustment on an annual basis. Annual mode requires that the DST beginning and ending date be specified concisely. For example, specify to begin DST on April 3 and end DST on October 14. The format for annual mode is as follows, and in the order listed:
- `<date 1-31>` - The day of the month to begin DST, expressed numerically.
- `<month 1-12>` - The month of the year to begin DST, expressed numerically.
- `<hh:mm>` - The time of day to begin DST in hours and minutes, expressed using a 24-hour clock.
- `<date 1-31>` - The day of the month to end DST, expressed numerically.
- `<month 1-12>` - The month of the year to end DST, expressed numerically.
- `<hh:mm>` - The time of day to end DST, in hours and minutes, expressed using a 24-hour clock.

**offset [30 | 60 | 90 | 120]** - Indicates the number of minutes to add during the summertime. The possible offset times are 30, 60, 90, and 120. The default value is 60.

Restrictions
Only Administrator or operator-level users can issue this command.

**Example usage:**
To configure daylight savings time on the Switch to run from the 2nd Tuesday in April at 3 PM until the 2nd Wednesday in October at 3:30 PM and add 30 minutes at the onset of DST:

```
DGS3100# config dst repeating 2 tue 4 15:00 2 wed 10 15:30 offset 30
Success.
DGS3100#
```
### show time

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To display the current time settings and status.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>show time</code></td>
</tr>
<tr>
<td>Description</td>
<td>The <code>show time</code> command displays the system time and date configuration, as well as displays the current system time.</td>
</tr>
<tr>
<td>Parameters</td>
<td>None.</td>
</tr>
<tr>
<td>Restrictions</td>
<td>None.</td>
</tr>
</tbody>
</table>

**Example usage:**

To show the time currently set on the Switch’s System clock:

```
DGS3100# show time

Current Time Source : System Clock
Current Time : 4 May 2006 15:01:32
Time Zone : GMT +02:30
Daylight Saving Time : Repeating
Offset in Minutes : 30
Repeating From : Apr 2nd Tue 15:00
To : Oct 2nd Wed 15:30
Annual From : 29 Apr 00:00
To : 12 Oct 00:00

DGS3100#
```
The Routing Table commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

<table>
<thead>
<tr>
<th>Command</th>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>create iproute</td>
<td>[default] &lt;ipaddr&gt; {&lt;metric 1-65535&gt;}</td>
</tr>
<tr>
<td>delete iproute</td>
<td>[default]</td>
</tr>
<tr>
<td>show iproute</td>
<td></td>
</tr>
</tbody>
</table>

Each command is listed in detail, as follows:

**create iproute**

- **Purpose**: To create IP route entries in the Switch’s IP routing table.
- **Syntax**: `create iproute [default] <ipaddr> {<metric 1-65535>}`
- **Description**: The `create iproute` command creates a static IP route entry in the Switch’s IP routing table.
- **Parameters**:
  - `default` – The entry is the default IP route entry in the Switch’s routing table.
  - `<ipaddr>` – The gateway IP address for the next hop router.
  - `<metric 1-65535>` – The routing protocol metric entry representing the number of routers between the Switch and the IP address above. The default setting is 1.
- **Restrictions**: Only Administrator or operator-level users can issue this command.

**Example usage**:

To add the default static address 10.48.74.121, with a metric setting of 1, to the routing table as the default route:

```
DGS3100# create iproute default 10.48.74.121 1
Success.
DGS3100#
```

**delete iproute**

- **Purpose**: To delete a default IP route entry from the Switch’s IP routing table.
- **Syntax**: `delete iproute [default]`
- **Description**: The `delete iproute` command deletes an existing default entry from the Switch’s IP routing table.
- **Parameters**: None.
- **Restrictions**: Only Administrator or operator-level users can issue this command.
Example usage:
To delete the default IP route:

```
DGS3100# delete iproute default
Success.
DGS3100#
```

**show iproute**

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To display the Switch’s current IP routing table.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>show iproute</code></td>
</tr>
<tr>
<td>Description</td>
<td>The <code>show iproute</code> command displays the Switch’s current IP routing table.</td>
</tr>
<tr>
<td>Parameters</td>
<td>None</td>
</tr>
<tr>
<td>Restrictions</td>
<td>None</td>
</tr>
</tbody>
</table>

Example usage:
To display the contents of the IP routing table:

```
DGS3100# show iproute
Routing Table
IP Address/Netmask        Gateway     Interface Hops Protocol
-------------------------------------        --------   -----      -------
10.0.0.0/8                 0.0.0.0      System    1        Local
Total Entries : 1
DGS3100#
```
The ARP commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

<table>
<thead>
<tr>
<th>Command</th>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>create arpentry</td>
<td>&lt;ipaddr&gt; &lt;macaddr&gt;</td>
</tr>
<tr>
<td>config arpentry</td>
<td>&lt;ipaddr&gt; &lt;macaddr&gt;</td>
</tr>
<tr>
<td>delete arpentry</td>
<td>[&lt;ipaddr&gt;</td>
</tr>
<tr>
<td>show arpentry</td>
<td>{ipif system</td>
</tr>
<tr>
<td>config arp_aging time</td>
<td>&lt;value 1-65535 &gt;</td>
</tr>
<tr>
<td>clear arptable</td>
<td></td>
</tr>
<tr>
<td>config arpSpoofing prevention</td>
<td>add gateway_ip &lt;ipaddr&gt; mac gateway_mac &lt;macaddr&gt; ports [&lt;portlist&gt;</td>
</tr>
<tr>
<td>config arpSpoofing prevention</td>
<td>delete gateway_ip &lt;ipaddr&gt;</td>
</tr>
<tr>
<td>show arpSpoofing prevention</td>
<td></td>
</tr>
</tbody>
</table>

Each command is listed in detail, as follows:

**create arpentry**

**Purpose:** To insert a static entry into the ARP table.

**Syntax:**

create arpentry <ipaddr> <macaddr>

**Description:**

The `create arpentry` command enters an IP address and the corresponding MAC address into the Switch's ARP table.

**Parameters:**

- `<ipaddr>` – The IP address of the end node or station.
- `<macaddr>` – The MAC address corresponding to the IP address above.

**Restrictions:**

Only Administrator or operator-level users can issue this command.

**Example usage:**

To create a static ARP entry for the IP address 10.48.74.121 and MAC address 00:50:BA:00:07:36:

DGS3100# create arpentry 10.48.74.121 00-50-BA-00-07-36

Success.

DGS3100#
### config arpentry

**Purpose:** To configure a static entry in the ARP table.

**Syntax:**

```
config arpentry <ipaddr> <macaddr>
```

**Description:** The `config arpentry` command configures a static entry in the ARP Table. The user may specify the IP address and the corresponding MAC address of an entry in the Switch’s ARP table.

**Parameters:**

- `<ipaddr>` – The IP address of the end node or station.
- `<macaddr>` – The MAC address corresponding to the IP address above.

**Restrictions:** Only Administrator or operator-level users can issue this command.

**Example usage:**

To configure a static ARP entry for the IP address 10.48.74.12 and MAC address 00:50:BA:00:07:36:

```
DGS3100# config arpentry 10.48.74.12 00-50-BA-00-07-36
Success.
DGS3100#
```

### delete arpentry

**Purpose:** To delete a static entry from the ARP table.

**Syntax:**

```
delete arpentry [<ipaddr> | all]
```

**Description:** The `delete arpentry` command deletes a static ARP entry, made using the `create arpentry` command above, by specifying either the IP address of the entry or all. Specifying `all` clears the Switch’s ARP table.

**Parameters:**

- `<ipaddr>` – The IP address of the end node or station to be deleted from the ARP table.
- `all` – Deletes all ARP entries.

**Restrictions:** Only Administrator or operator-level users can issue this command.

**Example usage:**

To delete an entry of IP address 10.48.74.121 from the ARP table:

```
DGS3100# delete arpentry 10.48.74.121
Success.
DGS3100#
```
### show arpentry

**Purpose**
To display the ARP table.

**Syntax**
```
show arpentry {ipif system | ipaddress <ipaddr> | static }
```

**Description**
The `show arpentry` command displays the current contents of the Switch's ARP table.

**Parameters**
- `ipif system <ipif_name 12>` – The name of the IP interface, the end node or station for which the ARP table entry was made, resides on.
- `ipaddress <ipaddr>` – The network address corresponding to the IP interface name above.
- `static` – Displays the static entries to the ARP table.

**Restrictions**
None.

**Example usage:**
To display the ARP table:

```
DGS3100# show arpentry
ARP timeout : 150 Seconds

<table>
<thead>
<tr>
<th>Interface</th>
<th>IP Address</th>
<th>MAC Address</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>System</td>
<td>10.6.41.33</td>
<td>00:00:b0:07:07:49</td>
<td>dynamic</td>
</tr>
<tr>
<td>System</td>
<td>10.6.41.49</td>
<td>00:20:18:2a:56:18</td>
<td>dynamic</td>
</tr>
</tbody>
</table>

Total Entries = 2
```

### config arp_aging time

**Purpose**
To configure the age-out timer for ARP table entries on the Switch.

**Syntax**
```
config arp_aging time <value 1-65535 >
```

**Description**
The `config arp_aging time` command sets the maximum amount of time, in minutes, that an ARP entry can remain in the Switch's ARP table, without being accessed, before it is dropped from the table.

**Parameters**
- `time <value 1-65535>` – The ARP age-out time, in minutes. The value may be in the range of 1-65535 minutes, with a default setting of 20 minutes.

**Restrictions**
Only Administrator or operator-level users can issue this command.

**Example usage:**
To configure ARP aging time:

```
DGS3100# config arp_aging time 30
Success.
```

DGS3100#
### clear arptable

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To remove all dynamic ARP table entries.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>clear arptable</code></td>
</tr>
<tr>
<td>Description</td>
<td>The <code>clear arptable</code> command is used to remove dynamic ARP table entries from the Switch’s ARP table. Static ARP table entries are not affected.</td>
</tr>
<tr>
<td>Parameters</td>
<td>None.</td>
</tr>
<tr>
<td>Restrictions</td>
<td>Only Administrator or operator-level users can issue this command.</td>
</tr>
</tbody>
</table>

**Example usage:**

To remove dynamic entries in the ARP table:

```
DGS3100# clear arptable
Success.
DGS3100#
```

### config arp_spoofing_prevention

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To insert an ARP spoofing prevention entry into the Switch.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>`config arp_spoofing_prevention add gateway_ip &lt;ipaddr&gt; mac gateway_mac &lt;macaddr&gt; ports [&lt;portlist&gt;</td>
</tr>
<tr>
<td>Description</td>
<td>The <code>config arp_spoofing_prevention add</code> command enters an IP address and the corresponding MAC address and ports into the Switch’s ARP spoofing prevention table that validates ARP packets in a network. It intercepts, logs, and discards ARP packets with invalid IP-to-MAC address bindings. This capability protects the network from certain man-in-the-middle attacks.</td>
</tr>
<tr>
<td>Parameters</td>
<td><code>&lt;ipaddr&gt;</code> – The IP address of the end node or station. <code>&lt;macaddr&gt;</code> – The MAC address corresponding to the IP address above. <code>&lt;portlist&gt;</code> – A port or range of ports whose settings are to be displayed. <code>all</code> – Configures all ports on the Switch.</td>
</tr>
<tr>
<td>Restrictions</td>
<td>Only Administrator or operator-level users can issue this command.</td>
</tr>
</tbody>
</table>

**Example usage:**

To create an ARP spoofing prevention entry for the IP address `1.1.1.1` and MAC address `00:50:BA:00:07:36` and port 1:

```
DGS3100# config arp_spoofing_prevention add gateway_ip 1.1.1.1 gateway_mac 00:50:BA:00:07:36 ports 1
Success.
DGS3100#
```
**config arp_spoofing_prevention**

**Purpose:** To delete an ARP spoofing prevention entry from the Switch.

**Syntax:**
```
config arp_spoofing_prevention delete gateway_ip <ipaddr>
```

**Description:** The `config arp_spoofing_prevention delete` command deletes an ARP spoofing prevention entry which existed in the Switch.

**Parameters:**
- `<ipaddr>` - The IP address of the end node or station.

**Restrictions:** Only Administrator or operator-level users can issue this command.

**Example usage:**
To delete an ARP spoofing prevention entry for the IP address 1.1.1.1:

```
DGS3100# config arp_spoofing_prevention delete gateway_ip 1.1.1.1
Success.
DGS3100#
```

**show arp_spoofing_prevention**

**Purpose:** To display all ARP spoofing prevention table entries on the Switch.

**Syntax:**
```
show arp_spoofing_prevention
```

**Description:** The `show arp_spoofing_prevention` command displays current contents of the ARP spoofing prevention table in the Switch.

**Parameters:** None.

**Restrictions:** None.

**Example usage:**
To display the ARP spoofing prevention table:

```
DGS-3100# show arp_spoofing_prevention
IP : 1.1.1.1
MAC : 00:50:ba:00:07:37
Ports : 1:1
DGS-3100#
```
The Banner commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

<table>
<thead>
<tr>
<th>Command</th>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>config login_banner</td>
<td>&lt;text 0-159&gt;</td>
</tr>
<tr>
<td>show login_banner</td>
<td></td>
</tr>
</tbody>
</table>

Each command is listed in detail, as follows:

**config login_banner**
- **Purpose**: Used to define telnet login banner.
- **Syntax**: `config login_banner <text 0-159>`
- **Description**: This command allows definition of the login banner text.
- **Parameters**: <text 0 – 159> - up to 160 characters
- **Restrictions**: Only Administrator or operator-level users can issue this command.

**Example usage:**
To define telnet login banner to show ‘D-Link’:

```
DGS3100# config login_banner D-Link
Success.
DGS3100#
```

**show login_banner**
- **Purpose**: Used to show the login banner.
- **Syntax**: `show login_banner`
- **Description**: This command allows display of the telnet login banner.
- **Parameters**: None
- **Restrictions**: None

**Usage Example:**
To show the login banner:

```
DGS3100# show login_banner
Login banner is : D-Link
DGS3100#
```
The Command History List commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

<table>
<thead>
<tr>
<th>Command</th>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>?</td>
<td></td>
</tr>
<tr>
<td>show command_history</td>
<td></td>
</tr>
<tr>
<td>dir</td>
<td></td>
</tr>
<tr>
<td>config command_history</td>
<td>&lt;value 10-237&gt;</td>
</tr>
</tbody>
</table>

Each command is listed in detail, as follows:

<table>
<thead>
<tr>
<th>?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
</tr>
<tr>
<td>Syntax</td>
</tr>
<tr>
<td>Description</td>
</tr>
<tr>
<td>Parameters</td>
</tr>
<tr>
<td>Restrictions</td>
</tr>
</tbody>
</table>

Example usage:

To display all of the commands in the CLI:

```
DGS3100# ?
...
? clear clear arptable clear counters clear fdb clear log clear port_security_entry_port config 802.1p default_priority config 802.1p user_priority config 802.1x auth_mode config 802.1x auth_parameter ports config 802.1x auth_protocol config 802.1x capability ports config 802.1x init config 802.1x reauth config access_profile profile_id
```
show command_history

Purpose: To display the command history.
Syntax: `show command_history`
Description: The `show command_history` command displays the command history.
Parameters: None.
Restrictions: None.

Example usage:
To display the command history:

```
DGS3100# show command_history

? 
? show 
show vlan 
show command history

DGS3100#
```

dir

Purpose: To display all commands.
Syntax: `dir`
Description: The `dir` command displays all commands.
Parameters: None.
Restrictions: None.

Example usage:
To display all of the commands:

```
DGS3100# dir 
.. 
? 
clear 
clear arptable 
clear counters 
clear fdb 
clear log 
config 802.1p default_priority
```
config 802.1p user_priority
config 802.1x auth_parameter ports
config 802.1x auth_protocol
config 802.1x capability ports
config 802.1x init
config 802.1x reauth
config account
config admin local_enable
config arp_aging time
config arpentry
config authen application
config authen parameter attempt
config authen parameter response_timeout
config authen server group

More: <space>, Quit: q, One line: <return>

---

**config command_history**

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To configure the command history.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><strong>config command_history</strong> <code>&lt;value 10-237&gt;</code></td>
</tr>
<tr>
<td>Description</td>
<td>The <code>config command_history</code> command configures the command history.</td>
</tr>
<tr>
<td>Parameters</td>
<td><code>&lt;value 10-237&gt;</code> – The number of previously executed commands maintained in the buffer. Up to 40 of the latest executed commands may be viewed.</td>
</tr>
<tr>
<td>Restrictions</td>
<td>Only Administrator or operator-level users can issue this command.</td>
</tr>
</tbody>
</table>

---

**Example usage:**

To configure the command history:

```
DGS3100# config command_history 20
Success.
DGS3100#
```
## SSH COMMANDS

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable ssh</td>
<td></td>
</tr>
<tr>
<td>disable ssh</td>
<td></td>
</tr>
<tr>
<td>config ssh authmode</td>
<td>publickey [enable</td>
</tr>
<tr>
<td>show ssh authmode</td>
<td></td>
</tr>
<tr>
<td>config ssh server</td>
<td>{ timeout &lt;sec 120-600&gt;</td>
</tr>
<tr>
<td>show ssh server</td>
<td></td>
</tr>
<tr>
<td>show ssh algorithm</td>
<td></td>
</tr>
<tr>
<td>config ssh crypto</td>
<td>&lt;username 1-48&gt; [ rsa</td>
</tr>
<tr>
<td>show ssh crypto</td>
<td></td>
</tr>
<tr>
<td>delete ssh crypto</td>
<td>&lt;username 1-48&gt;</td>
</tr>
</tbody>
</table>

Each command is listed in detail, as follows:

**enable ssh**

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To enable SSH.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><strong>enable ssh</strong></td>
</tr>
<tr>
<td>Description</td>
<td>The <strong>enable ssh</strong> command enables SSH on the Switch.</td>
</tr>
<tr>
<td>Parameters</td>
<td>None</td>
</tr>
<tr>
<td>Restrictions</td>
<td>Only administrator or operator-level users can issue this command.</td>
</tr>
</tbody>
</table>

**Example usage:**

To enable SSH:

```
DGS3100# enable ssh
TELNET will be disabled when enable SSH.
Success.
DGS3100#
```
### disable ssh

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To disable SSH.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>disable ssh</td>
</tr>
<tr>
<td>Description</td>
<td>The disable ssh command disables SSH on the Switch.</td>
</tr>
<tr>
<td>Parameters</td>
<td>None</td>
</tr>
<tr>
<td>Restrictions</td>
<td>Only administrator or operator-level users can issue this command.</td>
</tr>
</tbody>
</table>

**Example usage:**

To disable SSH:

```
DGS3100# disable ssh
Success.
DGS3100#
```

### config ssh authmode

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To configure the SSH authentication mode setting.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>config ssh authmode publickey [enable</td>
</tr>
<tr>
<td>Description</td>
<td>The config ssh authmode command configures the SSH authentication mode for users attempting to access the Switch.</td>
</tr>
<tr>
<td>Parameters</td>
<td>publickey [enable</td>
</tr>
<tr>
<td>Restrictions</td>
<td>Only administrator or operator-level users can issue this command.</td>
</tr>
</tbody>
</table>

**Example usage:**

To enable the SSH authentication mode:

```
DGS3100# config ssh authmode publickey enable
Success.
DGS3100#
```

### show ssh authmode

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To display the SSH authentication mode setting.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>show ssh authmode</td>
</tr>
<tr>
<td>Description</td>
<td>The show ssh authmode command displays the current SSH authentication set on the Switch.</td>
</tr>
<tr>
<td>Parameters</td>
<td>None</td>
</tr>
<tr>
<td>Restrictions</td>
<td>None</td>
</tr>
</tbody>
</table>
Example usage:

To view the current authentication mode set on the Switch:

```
DGS3100# show ssh authmode
The SSH User Authentication Support
-------------------------------
Publickey : Enabled
DGS3100#
```

### config ssh server

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To configure the SSH server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>`config ssh server { timeout &lt;sec 120-600&gt;</td>
</tr>
<tr>
<td>Description</td>
<td>The <code>config ssh server</code> command configures the SSH server.</td>
</tr>
<tr>
<td>Parameters</td>
<td><code>timeout &lt;sec 120-600&gt;</code> - Specifies the connection timeout. The value may be between 120 and 600 seconds. The default is 600 seconds.</td>
</tr>
<tr>
<td></td>
<td><code>port &lt;tcp_port_number 1-65535&gt;</code> - The TCP port number of the server. TCP ports are numbered between 1 and 65535. The ‘well-known’ port for the SSH management software is 22.</td>
</tr>
<tr>
<td>Restrictions</td>
<td>Only administrator or operator-level users can issue this command.</td>
</tr>
</tbody>
</table>

Example usage:

To configure the SSH server:

```
DGS3100# config ssh server timeout 300 port 1000
Success.
DGS3100#
```

### show ssh server

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To display the SSH server setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>show ssh server</code></td>
</tr>
<tr>
<td>Description</td>
<td>The <code>show ssh server</code> command displays the current SSH server settings.</td>
</tr>
<tr>
<td>Parameters</td>
<td>None</td>
</tr>
<tr>
<td>Restrictions</td>
<td>None</td>
</tr>
</tbody>
</table>

Example usage:

To display the SSH server:

```
DGS3100# show ssh server
SSH Server Status : disabled
SSH Max Session   : 5
Connection timeout: 600
```
Authenticate failed attempts : 3
Listened Port Number : 22
DGS3100#

show ssh algorithm

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To display the SSH algorithm setting.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>show ssh algorithm</td>
</tr>
<tr>
<td>Description</td>
<td>The show ssh algorithm command displays the current SSH algorithm setting status.</td>
</tr>
<tr>
<td>Parameters</td>
<td>None</td>
</tr>
<tr>
<td>Restrictions</td>
<td>None</td>
</tr>
</tbody>
</table>

Example usage:
To display SSH algorithms currently set on the Switch:

```
DGS3100# show ssh algorithm

Encryption Algorithm
---------------------
3des-cbc
AES128
AES192
AES256
RC4

Data Integrity Algorithm
------------------------
MD5
SHA1

Public Key Algorithm
---------------------
RSA
DSA
```

DGS3100#

config ssh crypto

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To specify which SSH public key is manually configured.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>config ssh crypto &lt;username 1-48&gt; [ rsa</td>
</tr>
<tr>
<td>Description</td>
<td>The config ssh crypto command specifies which SSH public key is manually configured. The key string needs to be in UU-encoded DER format. UU-encoded format is the same format in the authorized_keys file used by OpenSSH.</td>
</tr>
</tbody>
</table>
**Parameters**

- `<username 1-48>` – The username of the remote SSH client.
- `rsa` – Indicates the RSA key pair is manually configured.
- `dsa` – Indicates the DSA key pair is manually configured.
- `<sequences>` – Specifies User’s public key that identifies the user upon login.

**Restrictions**

Only administrator or operator-level users can issue this command.

**Example usage:**

To specify the SSH public key for the remote SSH client bob:

```
DGS3100# config ssh crypto bob rsa
Please input the public key:
AAAAB3NzaC1yc2EAAAABJQAAAEEAhtXYN0V9WMF4972irwSdLFbz6Inm+
GdpMScn
+PXv1JrRPJk4k9svJRm5mbIYEfuM9NMVZ7fvgVQyQwTuAlQ==
DGS3100#
DGS3100#
```

**show ssh crypto**

**Purpose**

To display the SSH public key stored on the device.

**Syntax**

```
show ssh crypto
```

**Description**

The `show ssh crypto` command displays the SSH public key stored on the device.

**Parameters**

None

**Restrictions**

Only Administrator or operator-level users can issue this command.

**Example usage:**

To display the SSH public key on the device:

```
DGS3100# show ssh crypto

<table>
<thead>
<tr>
<th>Username</th>
<th>Fingerprint</th>
</tr>
</thead>
</table>

DGS3100#```
**delete ssh crypto**

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To remove a specified user’s SSH public key from the device.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>delete ssh crypto &lt;username 1-48&gt;</td>
</tr>
<tr>
<td>Description</td>
<td>The delete ssh crypto command deletes the specified user’s SSH public key from the device.</td>
</tr>
<tr>
<td>Parameters</td>
<td>&lt;username 1-48&gt; - The username of the remote SSH client.</td>
</tr>
<tr>
<td>Restrictions</td>
<td>Only administrator or operator-level users can issue this command.</td>
</tr>
</tbody>
</table>

**Example usage:**
To delete the SSH public key of the remote SSH client bob:

```
DGS3100# Delete ssh crypto bob
Success.
DGS3100#
```
SSL COMMANDS

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable ssl</td>
<td></td>
</tr>
<tr>
<td>disable ssl</td>
<td></td>
</tr>
<tr>
<td>show ssl</td>
<td></td>
</tr>
<tr>
<td>show ssl cachetimeout</td>
<td></td>
</tr>
<tr>
<td>crypto certificate</td>
<td>&lt;number 1-2&gt; generate {key-generate &lt;length 512 - 1024&gt;</td>
</tr>
<tr>
<td>crypto certificate</td>
<td>&lt;number 1-2&gt; request {cn &lt;common-name 1 - 64&gt;</td>
</tr>
<tr>
<td>crypto certificate</td>
<td>&lt;number 1-2&gt; import</td>
</tr>
<tr>
<td>config ssl certificate</td>
<td>&lt;number 1-2&gt;</td>
</tr>
<tr>
<td>show crypto certificate</td>
<td>mycertificate {number 1-2}</td>
</tr>
</tbody>
</table>

Each command is listed in detail, as follows:

**enable ssl**

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To enable the SSL function on the Switch.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><strong>enable ssl</strong></td>
</tr>
<tr>
<td>Description</td>
<td>The <strong>enable ssl</strong> command enables SSL on the Switch by implementing every combination of listed ciphersuites on the Switch. Entering this command enables the SSL status on the Switch. Enabling SSL disables the web-manager on the Switch.</td>
</tr>
<tr>
<td>Parameters</td>
<td>None</td>
</tr>
<tr>
<td>Restrictions</td>
<td>Only administrator or operator-level users can issue this command.</td>
</tr>
</tbody>
</table>

**Example usage:**

To enable SSL on the Switch for all ciphersuites:

```
DGS3100# enable ssl

Note: Web will be disabled if SSL is enabled.
Success.
```
disable ssl

Purpose
To disable the SSL function on the Switch.

Syntax
`disable ssl`

Description
The `disable ssl` command disables SSL on the Switch and can be used to disable all combinations of listed ciphersuites on the Switch. Note that disabling SSL will not enable WEB access automatically (WEB access will stay disabled), and you'll need to enable it manually.

Parameters
None

Restrictions
Only administrator or operator-level users can issue this command.

Example usage:

To disable the SSL status on the Switch:

```
DGS3100# disable ssl
Success.
DGS3100#
```

show ssl

Purpose
To view the SSL status and the certificate file status on the Switch.

Syntax
`show ssl`

Description
The `show ssl` command displays the SSL status and the certificate file status on the Switch.

Parameters
None.

Restrictions
None.

Example usage:

To view the SSL status on the Switch:

```
DGS3100# show ssl

SSL status                        Enabled
RSA_WITH_RC4_128_MD5               Enabled
RSA_WITH_3DES_EDE_CBC_SHA         Enabled
RSA_EXPORT_WITH_RC4_40_MD5        Enabled

DGS3100#
```
show ssl cachetimeout

**Purpose**
To show the SSL cache timeout.

**Syntax**
show ssl cachetimeout

**Description**
The `show ssl cachetimeout` command displays the SSL cache timeout currently implemented on the Switch.

**Parameters**
None.

**Restrictions**
None.

**Example usage:**
To view the SSL cache timeout on the Switch:

```
DGS3100# show ssl cachetimeout
Cache timeout is 600 seconds.
DGS3100#
```

crypto certificate (generate)

**Purpose**
To generate a self-signed HTTPS certificate

**Syntax**
crypto certificate <number 1-2> generate {key-generate <length 512-1024>| cn <common-name 1-64>| ou <organization-unit 1-64>| or <organization 1-64>| loc <location 1-64>| st <state 1-64>| cu <country 1-2>| duration <days 30-3650>

**Description**
The `crypto certificate (generate)` command generates a self-signed HTTPS certificate for the device.
Default Certificate 1 generated at very first start up.
Note that for first time certificate 2 generates, there is a need in key generate.

**Parameters**
- `number` — Specifies the certificate number (Range: 1 - 2).
- `key-generate` — Regenerates the SSL RSA key.
- `length` — Specifies the SSL RSA key length (Range: 512 - 1024).
- `common-name` — Specifies the fully qualified URL or IP address of the device (Range: 1 - 64).
- `organization` — Specifies the organization name (Range: 1 - 64).
- `organization-unit` — Specifies the organization-unit or department name (Range: 1 - 64).
- `location` — Specifies the location or city name (Range: 1 - 64).
- `state` — Specifies the state or province name (Range: 1 - 64).
- `country` — Specifies the country name (Range: 1 - 2).
- `days` — Specifies number of days certification is valid (Range: 30 - 3650).

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

**Example usage:**
To generate a self-signed HTTPS certificate:

```
DGS3100# crypto certificate 1 generate
```
**crypto certificate (request)**

**Purpose**
To generate and display certificate requests for HTTPS.

**Syntax**
```
crypto certificate <number 1-2> request {cn <common-name 1-64> | ou <organization-unit 1-64> | or <organization 1-64> | loc <location 1-64> | st <state 1-64> | cu <country 1-2>
```

**Description**
The **crypto certificate (request)** command exports a certificate request to a Certification Authority. The certificate request is generated in Base64-encoded X.509 format. Before generating a certificate request, a self-signed certificate must first be generated using the crypto certificate generate command. Be aware that you have to reenter the certificate fields. After receiving the certificate from the Certification Authority, use the crypto certificate import to import the certificate into the device. This certificate replaces the self-signed certificate.

**Parameters**
- **number** — Specifies the certificate number (Range: 1 - 2).
- **common-name** — Specifies the fully qualified URL or IP address of the device (Range: 1- 64).
- **organization-unit** — Specifies the organization-unit or department name (Range: 1- 64).
- **organization** — Specifies the organization name (Range: 1- 64).
- **location** — Specifies the location or city name (Range: 1- 64).
- **state** — Specifies the state or province name (Range: 1- 64).
- **country** — Specifies the country name (Range: 1- 2).

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

**Example usage:**
To generate and display certificate requests for HTTPS:

```
DGS3100# crypto certificate 1 request
-----BEGIN CERTIFICATE REQUEST-----
MIIBDTCBuAIBADBTMqswCQYDVQQGEwIgIDEKMAgGA1UECBMBIDEKMAgGA1UEBxMB
IDEUMBIGA1UEAxMlMTAuNi4yMi4xMTQxCjAIBgNVBAoTASAxCjAIBgNVBAsTASA
XDNBgkqhkiG9w0BAQEFAANLADBIAkEaw3odbbo5S4JPRz2QJKoEpTmve8Wddsm4
0nvmOpxqUDORi7TigrZfs3vGxz2Nar1RfiQwKQxb7VetgxF8VeKmDQIDAQABoAw
DQYJKoZlhwvNAQEEBQADQQB1owjB2ifZvYydBS1zJIl/Hd6F2MhrzF35ULNgNHP0Z
pbtU7Y4HkyqsQzkCwDazGD+y4YB/mu4jNxeq+lk2UEYD
-----END CERTIFICATE REQUEST-----
```

Success.
DGS3100#
**crypto certificate (import)**

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To import a certificate signed by the Certification Authority for HTTPS.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>crypto certificate &lt;number 1-2&gt; import</code></td>
</tr>
<tr>
<td>Description</td>
<td>The <strong>crypto certificate (import)</strong> command imports an external certificate (signed by a Certification Authority) to the device. To end the session, add a period (.) on a separate line after the input. The imported certificate must be based on a certificate request created by the crypto certificate request. If the public key found in the certificate does not match the device's SSL RSA key, the command fails. This command is not saved in the device configuration; however, the certificate imported by this command is saved in the private configuration (which is never displayed to the user or backed up to another device).</td>
</tr>
<tr>
<td>Parameters</td>
<td><code>number</code> — Specifies the certificate number (Range: 1 - 2).</td>
</tr>
<tr>
<td>Restrictions</td>
<td>Only administrator or operator-level users can issue this command.</td>
</tr>
</tbody>
</table>

**Example usage:**
To import a certificate signed by the Certification Authority for HTTPS:

```
DGS3100# crypto certificate 1 import
Please paste the input now, add a period (.) on a separate line after the input, and press Enter.
-----BEGIN CERTIFICATE-----
MIIFXTCCBEWgAwIBAgIKFWx9ZgACAAAAMDANBgkqhCZImiZPyLGQBGRYDTkVUMiEAYKCZImiZPyLGQBGRY
xicNoBiJIFr8H/nMiL/Aa86nhnevaq49df/cIt6XDHervIC
767yZ3iyB8U3hzUxVOjfACNcQR0GuwNt1i58qbCGuhE
eaft/2OmveJezNF5oDgYgblnlotykUgNXzFaTecebu161
scXi7iqyF1dMQKG0/LZ3nzSux2dyycg5lt9Lsi+b+Ej2j
UKOlzyLRkan3m1WGGJEmcv4JK0WaJLzyfW4iyYtrryN
-----END CERTIFICATE-----
.
Certificate imported successfully
Issued by : DC=, DC=, CN=
Valid From: Jan 24 14:42:10 2008 GMT
Valid to: Jan 24 14:52:10 2009 GMT
Subject: C= , ST= , L= , O= , OU= , CN=
SHA1 Fingerprint: E7495984 30BDFFA6 D133E7B6 4AA7A608 CE017347

Success.
DGS3100#
```

**config ssl certificate**

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To configure the active certificate for HTTPS.</th>
</tr>
</thead>
</table>

---

165
Syntax

```
config ssl certificate <number 1-2>
```

Description
The `config ssl certificate` command activates SSL certificate.

Parameters

- `number` — Specifies the certificate number (Range: 1 - 2).

Restrictions
Only administrator or operator-level users can issue this command.

Example usage:

To configure the active certificate for SSL:

```
DGS3100# config ssl certificate 1
Success.
DGS3100#
```

Syntax

```
show crypto certificate mycertificate {number 1-2}
```

Description
The `show crypto certificate mycertificate` command displays the SSL certificate of the device.

Parameters

- `number` — Specifies the certificate number (Range: 1 - 2).

Restrictions
Only administrator or operator-level users can issue this command.

Example usage:

To show crypto certificate mycertificate:

```
DGS3100# show crypto certificate mycertificate
-----BEGIN CERTIFICATE-----
MIIBkDCCAToCAQAwDQYJKoZIhvcNAQEEBQAwUzELMAkGA1UEBhMCICAxCjAIBgNV
BAgTASAxCjAIBgNVBAcTASAxFDASBgNVBAgTASAxCjAIBgNVBAcTASAxFDASBgNV
BAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNV
BAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNV
BAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNV
BAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNV
BAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNV
BAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNV
BAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNV
BAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNV
BAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNV
BAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNV
BAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNV
BAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNV
BAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNV
BAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNV
BAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNV
BAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNV
BAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNV
BAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNV
BAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNV
BAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNV
BAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNV
BAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNV
BAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNV
BAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNV
BAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNV
BAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNV
BAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNV
BAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNV
BAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNV
BAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNV
BAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNV
BAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNV
BAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNV
BAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNV
BAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNV
BAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNV
BAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNV
BAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNV
BAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNV
BAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNV
BAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNV
BAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNV
BAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNV
BAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNV
BAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNV
BAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNV
BAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNV
BAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNV
BAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNV
BAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNV
BAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNV
BAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNV
BAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNV
BAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNV
BAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNVBAgTASAxFDASBgNV
BAgTASAxFBvDkKx3BkH7NPzBO6PHaQ==
-----END CERTIFICATE-----
Issued by : C= , ST= , L= , CN=10.6.22.111, O= , OU=
Valid From: Jan 3 02:33:54 2005 GMT
Valid to: Jan 3 02:33:54 2006 GMT
Subject: C= , ST= , L= , CN=10.6.22.111, O= , OU=
SHA1 Fingerprint: 99A1052E E4C9DA24 2F9E2BBB 0968364E 387C6628

DGS3100#
## ACCESS AUTHENTICATION CONTROL COMMANDS

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>create authen_login</td>
<td>method_list_name &lt;string 12&gt;</td>
</tr>
<tr>
<td>config authen_login</td>
<td>{ [default</td>
</tr>
<tr>
<td>delete authen_login</td>
<td>method_list_name &lt;string 12&gt;</td>
</tr>
<tr>
<td>show authen_login</td>
<td>{all</td>
</tr>
<tr>
<td>create authen_enable</td>
<td>method_list_name &lt;string 12&gt;</td>
</tr>
<tr>
<td>config authen_enable</td>
<td>[default</td>
</tr>
<tr>
<td>delete authen_enable</td>
<td>method_list_name &lt;string 12&gt;</td>
</tr>
<tr>
<td>show authen_enable</td>
<td>[all</td>
</tr>
<tr>
<td>config authen application</td>
<td>{console</td>
</tr>
<tr>
<td>show authen application</td>
<td></td>
</tr>
<tr>
<td>create authen server_host</td>
<td>&lt;ipaddr&gt; protocol [tacacs+</td>
</tr>
<tr>
<td>config authen server_host</td>
<td>&lt;ipaddr&gt; protocol tacacs+ {port &lt;int 1-65535&gt;</td>
</tr>
<tr>
<td>delete authen server_host</td>
<td>&lt;ipaddr&gt; protocol [tacacs+</td>
</tr>
<tr>
<td>show authen server_host</td>
<td></td>
</tr>
<tr>
<td>local_enable admin</td>
<td></td>
</tr>
<tr>
<td>config admin local_enable</td>
<td></td>
</tr>
</tbody>
</table>

Each command is listed in detail, as follows:
### create authen_login method_list_name

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To create a user-defined list of authentication methods for users logging on to the Switch.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>create authen_login method_list_name &lt;string 12&gt;</code></td>
</tr>
<tr>
<td>Description</td>
<td>The <code>create authen_login method_list_name</code> command creates a list of authentication techniques for user login. The Switch can support up to eight method lists, but one is reserved as a default and cannot be deleted. Multiple method lists must be created and configured separately.</td>
</tr>
<tr>
<td>Parameters</td>
<td><code>&lt;string 12&gt;</code> - Defines the <code>method_list_name</code> to be created as a string of up to 12 alphanumeric characters.</td>
</tr>
<tr>
<td>Restrictions</td>
<td>Only Administrator or operator-level users can issue this command.</td>
</tr>
</tbody>
</table>

**Example usage:**

To create the method list ‘Trinity’:

```
DGS3100# create authen_login method_list_name Trinity
Success.
DGS3100#
```

### config authen_login

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To configure a user-defined or default method list of authentication methods for user login.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>`config authen_login { [default</td>
</tr>
<tr>
<td>Description</td>
<td>The <code>config authen_login</code> command configures a user-defined or default method list of authentication methods for users logging on to the Switch. The sequence of methods implemented in this command affects the authentication result. For example, if a user enters a sequence of methods like <code>tacacs – local</code>, the Switch sends an authentication request to the first <code>tacacs</code> host in the server group. If no response comes from the server host, the Switch sends an authentication request to the second <code>tacacs</code> host in the server group and so on, until the list is exhausted. When the local method is used, the privilege level is dependant on the local account privilege configured on the Switch. Successful login using any of these methods gives the user a ‘user’ privilege only. If the user wishes to upgrade his or her status to the administrator level, the user must implement the <code>enable admin</code> command, followed by a previously configured password. (See the <code>enable admin</code> part of this section for more detailed information, concerning the <code>enable admin</code> command.)</td>
</tr>
</tbody>
</table>
| Parameters | `default` – The default method list for access authentication, as defined by the user. The user may choose one or more of the following authentication methods:  
  - `tacacs+` – Specifies that the user is to be authenticated using the TACACS+ protocol from the remote TACACS+ server hosts of the TACACS+ server group list. |
**radius** - Specifies that the user is to be authenticated using the RADIUS protocol from the remote RADIUS server hosts of the RADIUS server group list.

**local** - Specifies that the user is to be authenticated using the local user account database on the Switch.

**none** – Specifies that no authentication is required to access the Switch.

- **http_method_list** – Specifies the https method list for access authentication.
- **https_method_list** – Specifies the https method list for access authentication.
- **method_list_name <string 12>** – Specifies a previously created method list name defined by the user. One or more of the following authentication methods may be added to this method list:
  - **tacacs+** – Specifies that the user is to be authenticated using the TACACS+ protocol from a remote TACACS+ server.
  - **radius** - Specifies that the user is to be authenticated using the RADIUS protocol from a remote RADIUS server.
  - **local** - Specifies that the user is to be authenticated using the local user account database on the Switch.
  - **none** – Specifies that no authentication is required to access the Switch.

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

**Restrictions**

Only Administrator or operator-level users can issue this command.

**Example usage:**

To configure the user defined method list ‘Trinity’ with authentication methods TACACS+, RADIUS and local, in that order.

```
DGS3100# config authen_login method_list_name Trinity method tacacs+ radius local
Success.
DGS3100#
```

**delete authen_login method_list_name**

**Purpose**

To delete a previously configured user defined list of authentication methods for users logging on to the Switch.

**Syntax**

```
delete authen_login method_list_name <string 12>
```

**Description**

The `delete authen_login method_list_name` command deletes a list of authentication methods for user login.

**Parameters**

- `<string 12>` - The previously created `method_list_name` to delete.

**Restrictions**

Only Administrator or operator-level users can issue this command.

**Example usage:**

To delete the method list name ‘Trinity’:

```
DGS3100# delete authen_login method_list_name Trinity
Success.
DGS3100#
```
DGS3100# delete authen_login method_list_name Trinity
Success.
DGS3100#

**show authen_login**

**Purpose**
To display a previously configured user defined method list of authentication methods for users logging on to the Switch.

**Syntax**
```
show authen_login {all | default | method_list_name <string 12>}
```

**Description**
The `show authen_login` command displays a list of authentication methods for user login.

**Parameters**
- `default` – Displays the default method list for users logging on to the Switch.
- `method_list_name <string 12>` - Specifies the `method_list_name` to display.
- `all` – Displays all the authentication login methods currently configured on the Switch.

The command displays the following parameters:
- Method List Name – The name of a previously configured method list name.
- Method Name – Defines which security protocols are implemented, per method list name.

**Restrictions**
None

**Example usage:**

To view all authentication login method list names:

DGS3100# show authen_login all

<table>
<thead>
<tr>
<th>Method List Name</th>
<th>Method Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Local</td>
</tr>
</tbody>
</table>

DGS3100#

**create authen_enable method_list_name**

**Purpose**
To create a user-defined method list of authentication methods for promoting normal user level privileges to Administrator level privileges on the Switch.

**Syntax**
```
create authen_enable method_list_name <string 12>
```

**Description**
The `create authen_enable method_list_name` command creates a list of authentication methods for promoting users with normal level privileges to Administrator level privileges using authentication methods on the Switch. Once a user acquires normal user level privileges on the Switch, he or she must be authenticated by a method on the Switch to gain administrator privileges on the Switch.
which is defined by the Administrator. A maximum of eight (8) enable method lists can be implemented on the Switch.

Parameters

- `<string 12>` - Defines the `authen_enable method_list_name` to be created as a string of up to 12 alphanumeric characters.

Restrictions

Only Administrator or operator-level users can issue this command.

Example usage:

To create a user-defined method list, named ‘Permit’ for promoting user privileges to Administrator privileges:

```
DGS3100# create authen_enable method_list_name Permit
Success.
DGS3100#
```

`config authen_enable`

Purpose

To configure a user-defined method list of authentication methods for promoting normal user level privileges to Administrator level privileges on the Switch.

Syntax

```
config authen_enable [default | method_list_name <string 12>] method {tacacs+ | radius | local_enable | none}
```

Description

The `config authen_enable` command configures a user-defined list of authentication methods for promoting normal user level privileges to Administrator level privileges using authentication methods on the Switch. Once a user acquires normal user level privileges on the Switch, he or she must be authenticated by a method on the Switch to gain administrator privileges on the Switch, which is defined by the Administrator. A maximum of eight (8) enable method lists can be implemented simultaneously on the Switch.

The sequence of methods implemented in this command affects the authentication result. For example, if a user enters a sequence of methods like `tacacs+ – radius – local_enable`, the Switch sends an authentication request to the first TACACS+ host in the server group. If no verification is found, the Switch sends an authentication request to the second TACACS+ host in the server group and so on, until the list is exhausted. At that point, the Switch restarts the same sequence with the following protocol listed, `radius`. If no authentication takes place using the `radius` list, the `local_enable` password set in the Switch is used to authenticate the user.

Successful authentication using any of these methods gives the user an ‘Admin’ level privilege.

Parameters

- `default` – The default method list for administration rights authentication, as defined by the user. The user may choose one or more of the following authentication methods:
  - `tacacs+` – Specifies that the user is to be authenticated using the TACACS+ protocol from the remote TACACS+ server hosts of the TACACS+ server group list.
  - `radius` – Specifies that the user is to be authenticated using the RADIUS protocol from the remote RADIUS server hosts of the RADIUS server group list.
  - `local_enable` - Specifies that the user is to be authenticated
using the local user account database on the Switch.

- none – Specifies that no authentication is required to access the Switch.

method_list_name <string 12> – Specifies a previously created authen_enable method_list_name. The user may add one or more of the following authentication methods to this method list:

- tacacs+ – Specifies that the user is to be authenticated using the TACACS+ protocol from a remote TACACS+ server.
- radius - Specifies that the user is to be authenticated using the RADIUS protocol from a remote RADIUS server.
- local_enable - Specifies that the user is to be authenticated using the local user account database on the Switch. The local enable password of the device can be configured using the 'config admin local_password' command.
- none – Specifies that no authentication is required to access the Switch.

Restrictions Only Administrator or operator-level users can issue this command.

Example usage:
To configure the user defined method list ‘Permit’ with authentication methods TACACS+, RADIUS and local_enable, in that order.

DGS3100# config authen_enable method_list_name Trinity method tacacs+ radius local_enable
Success.
DGS3100#

delete authen_enable method_list_name

Purpose To delete a user-defined list of authentication methods for promoting normal user level privileges to Administrator level privileges on the Switch.

Syntax delete authen_enable method_list_name <string 12>

Description The delete authen_enable method_list_name command deletes a user-defined list of authentication methods for promoting user level privileges to Administrator level privileges.

Parameters <string 12> - The previously created authen_enable method_list_name to be deleted.

Restrictions Only Administrator or operator-level users can issue this command.

Example usage:
To delete the user-defined method list ‘Permit’

DGS3100# delete authen_enable method_list_name Permit
Success.
DGS3100#
**show authen_enable**

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To display the list of authentication methods for promoting normal user level privileges to Administrator level privileges on the Switch.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>`show authen_enable [all</td>
</tr>
<tr>
<td>Description</td>
<td>The <code>show authen_enable</code> command deletes a user-defined list of authentication methods for promoting user level privileges to Administrator level privileges.</td>
</tr>
<tr>
<td>Parameters</td>
<td><code>default</code> – Displays the default method list for users attempting to gain access to Administrator level privileges on the Switch.</td>
</tr>
<tr>
<td></td>
<td><code>method_list_name &lt;string 12&gt;</code> – The <code>method_list_name</code> to be displayed.</td>
</tr>
<tr>
<td></td>
<td><code>all</code> – Displays all the authentication login methods currently configured on the Switch.</td>
</tr>
<tr>
<td>Restrictions</td>
<td>None</td>
</tr>
</tbody>
</table>

**Example usage:**

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

```
DGS3100# show authen_enable all
Method List Name       Method Name
----------------------------------------------
Permit                 tacacs+
default               tacacs+
Total Entries : 2
DGS3100#
```

**config authen application**

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To configure various applications on the Switch for authentication using a previously configured method list.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>`config authen application {console</td>
</tr>
<tr>
<td>Description</td>
<td>The <code>config authen application</code> command configures Switch applications (console, Telnet, SSH) for login at the user level and at the administration level (<code>authen_enable</code>), utilizing a previously configured method list.</td>
</tr>
<tr>
<td>Parameters</td>
<td><code>application</code> – Specifies the application to configure. One of the following four options may be selected:</td>
</tr>
</tbody>
</table>

```
• **console** – Configures the command line interface login method.
• **telnet** – Configures the Telnet login method.
• **ssh** – Configures the Secure Shell login method.
• **all** – Configures all applications as (console, Telnet, SSH) login methods.

**login** – Configures an application for normal login on the user level, using a previously configured method list.

**enable** – Configures an application for upgrading a normal user level to administrator privileges, using a previously configured method list.

**default** – Configures an application for user authentication using the default method list.

**method_list_name <string 12>** – Configures an application for user authentication using a previously configured method_list_name.

**Restrictions** Only Administrator or operator-level users can issue this command.

**Example usage:**

To configure the default method list for the command line interface:

```
DGS3100# config authen application console login default
Success.
DGS3100#
```

### show authen application

**Purpose** To display authentication methods for the various applications on the Switch.

**Syntax** `show authen application`

**Description** The `show authen application` command displays all of the authentication method lists (login, enable administrator privileges) for Switch configuration applications (console, Telnet, SSH) currently configured on the Switch.

**Parameters** None.

**Restrictions** None.

**Example usage:**

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

```
DGS3100# show authen application

<table>
<thead>
<tr>
<th>Application</th>
<th>Login Method List</th>
<th>Enable Method List</th>
</tr>
</thead>
<tbody>
<tr>
<td>Console</td>
<td>default</td>
<td>default</td>
</tr>
<tr>
<td>Telnet</td>
<td>Trinity</td>
<td>default</td>
</tr>
<tr>
<td>SSH</td>
<td>default</td>
<td>default</td>
</tr>
</tbody>
</table>

DGS3100#
```
**create authen server_host**

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To create an authentication server host.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>`create authen server_host &lt;ipaddr&gt; protocol tacacs+ {port &lt;int 1-65535&gt;</td>
</tr>
<tr>
<td>Description</td>
<td>The <code>create authen server_host</code> command creates an authentication server host for the TACACS+/RADIUS security protocols on the Switch. When a user attempts to access the Switch with authentication protocol enabled, the Switch sends authentication packets to a remote TACACS+/RADIUS server host on a remote host. The TACACS+/RADIUS server host then verifies or denies the request and returns the appropriate message to the Switch. More than one authentication protocol can be run on the same physical server host but, remember that TACACS+/RADIUS are separate entities and are not compatible with each other. The maximum supported number of server hosts is 16.</td>
</tr>
</tbody>
</table>
| Parameters | `server_host <ipaddr>` – The IP address of the remote server host to add.  
 `protocol` – The protocol used by the server host. The options are:  
  - `tacacs+` – Specifies that the server host utilizes the TACACS+ protocol.  
  - `radius` – Specifies that the server host utilizes the RADIUS protocol.  
 `port <int 1-65535>` – The virtual port number of the authentication protocol on a server host. The value must be between 1 and 65535. The default port number is 49 for TACACS/TACACS+ servers and 1812 and 1813 for RADIUS servers but the user may set a unique port number for higher security.  
 `key [<key_string 128> | none]` – The authentication key to be shared with a configured TACACS+ or RADIUS server only. The value is a string of up to 128 alphanumeric characters, or `none`.  
 `timeout <int 1-30>` – The time in seconds the Switch waits for the server host to reply to an authentication request. The default value is 5 seconds.  
 `retransmit <int 1-10>` – The number of times the device resends an authentication request when the server does not respond. The value is between 1 and 10. This field is inoperable for the TACACS+ protocol. |
| Restrictions | Only Administrator or operator-level users can issue this command. |

**Example usage:**

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

```
DGS3100# create authen server_host 10.1.1.121 protocol tacacs+ port 1234 timeout 10 retransmit 5
Success.
DGS3100#
```
### config authen server_host

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To configure a user-defined authentication server host.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>config authen server_host &lt;ipaddr&gt; protocol [tacacs+</td>
</tr>
<tr>
<td>Description</td>
<td>The config authen server_host command configures a user- defined authentication server host for the TACACS+/RADIUS security protocols on the Switch. When a user attempts to access the Switch with the authentication protocol enabled, the Switch sends authentication packets to a remote TACACS+/RADIUS server host on a remote host. The TACACS+/RADIUS server host then verifies or denies the request and returns the appropriate message to the Switch. More than one authentication protocol can be run on the same physical server host but, remember that TACACS+/RADIUS are separate entities and are not compatible with each other. The maximum supported number of server hosts is 16.</td>
</tr>
<tr>
<td>Parameters</td>
<td>server_host &lt;ipaddr&gt; – The IP address of the remote server host the user wishes to alter.</td>
</tr>
<tr>
<td></td>
<td>protocol – The protocol used by the server host. The options are:</td>
</tr>
<tr>
<td></td>
<td>• tacacs+ – Specifies that the server host utilizes the TACACS+ protocol.</td>
</tr>
<tr>
<td></td>
<td>• radius – Specifies that the server host utilizes the RADIUS protocol.</td>
</tr>
<tr>
<td></td>
<td>port &lt;int 1-65535&gt; – The virtual port number of the authentication protocol on a server host. The value must be between 1 and 65535. The default port number is 49 for TACACS/TACACS+ servers and 1812 and 1813 for RADIUS servers but the user may set a unique port number for higher security.</td>
</tr>
<tr>
<td></td>
<td>key [&lt;key_string 128&gt;</td>
</tr>
<tr>
<td></td>
<td>timeout &lt;int 1-30&gt; – The time in seconds the Switch waits for the server host to reply to an authentication request. The default value is 5 seconds.</td>
</tr>
<tr>
<td></td>
<td>retransmit &lt;int 1-10&gt; – The number of times the device resends an authentication request when the server does not respond. The value is between 1 and 10. This field is inoperable for the TACACS+ protocol.</td>
</tr>
<tr>
<td>Restrictions</td>
<td>Only Administrator or operator-level users can issue this command.</td>
</tr>
</tbody>
</table>

#### Example usage:

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

```
DGS3100# config authen server_host 10.1.1.121 protocol tacacs+ port 4321 timeout 12 retransmit 4
Success.
DGS3100#
```
### delete authen server_host

**Purpose**
To delete a user-defined authentication server host.

**Syntax**
```bash
delete authen server_host <ipaddr> protocol [tacacs+ | radius]
```

**Description**
The `delete authen server_host` command deletes a user-defined authentication server host previously created on the Switch.

**Parameters**
- `server_host <ipaddr>` - The IP address of the remote server host to be deleted.
- `protocol` – The protocol used by the server host the user wishes to delete. The options are:
  - `tacacs+` – Specifies that the server host utilizes the TACACS+ protocol.
  - `radius` – Specifies that the server host utilizes the RADIUS protocol.

**Restrictions**
Only Administrator or operator-level users can issue this command.

**Example usage:**

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

```
DGS3100# delete authen server_host 10.1.1.121 protocol tacacs+
Success.
DGS3100#
```

### show authen server_host

**Purpose**
To view a user-defined authentication server host.

**Syntax**
```
show authen server_host
```

**Description**
The `show authen server_host` command displays user-defined authentication server hosts previously created on the Switch.

The following parameters are displayed:
- **IP Address** – The IP address of the authentication server host.
- **Protocol** – The protocol used by the server host. Possible results include TACACS+ or RADIUS.
- **Port** – The virtual port number on the server host. The default value is 49.
- **Timeout** - The time in seconds the Switch waits for the server host to reply to an authentication request.
- **Retransmit** - The value in the retransmit field denotes how many times the device resends an authentication request when the TACACS server does not respond. This field is inoperable for the tacacs+ protocol.
- **Key** - Authentication key to be shared with a configured TACACS+ server only.

**Parameters**
None.

**Restrictions**
None.
Example usage:
To view authentication server hosts currently set on the Switch:

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Protocol</th>
<th>Port</th>
<th>Timeout</th>
<th>Retransmit</th>
<th>Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.53.13.94</td>
<td>TACACS</td>
<td>49</td>
<td>5</td>
<td>2</td>
<td></td>
</tr>
</tbody>
</table>

Total Entries: 1

local_enable admin

Purpose: To promote user level privileges to administrator level privileges.

Syntax: `local_enable admin`

Description: The `local_enable admin` command enables a user to be granted administrative privileges on to the Switch. After logging on to the Switch, users have only 'user' level privileges. To gain access to administrator level privileges, the user may enter this command. The system then prompts for an authentication password. Possible authentication methods for this function include TACACS, TACACS+, RADIUS, user defined server groups, local enable (local account on the Switch), or no authentication (none). Because TACACS does not support the enable function, the user must create a special account on the server host which has the username 'enable', and a password configured by the administrator that will support the 'enable' function. This function becomes inoperable when the authentication policy is disabled.

Parameters: None.

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

Example usage:
To enable administrator privileges on the Switch:

```
DGS3100# local_enable admin
Password: *****
DGS3100#
```

config admin local_enable

Purpose: To configure the local_enable password for administrator level privileges.

Syntax: `config admin local_enable`

Description: The `config admin local_enable` command changes the locally enabled password for the `local_enable admin` command. When a user chooses the `local_enable` method to promote user level privileges to administrator privileges, the user is prompted to enter the password configured here.

After entering the `config admin local_enable` command, the user is prompted to enter the old password, then a new password in a string
of no more than 15 alphanumeric characters, and finally prompted to enter the new password again for confirmation. See the example below.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>None.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restrictions</td>
<td>Only administrator-level users can issue this command.</td>
</tr>
</tbody>
</table>

**Example usage:**

To configure the password for the ‘local_enable’ authentication method.

```
DGS3100# config admin local_enable

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

DGS3100#
```
LACP COMMANDS

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>config lacp port_priority</td>
<td>&lt;portlist&gt; [priority 1-65535] [timeout &lt;90sec</td>
</tr>
<tr>
<td>show lacp</td>
<td>{&lt;portlist&gt;}</td>
</tr>
</tbody>
</table>

Each command is listed in detail, as follows:

**config lacp port_priority**

**Purpose**
To set the priority value of a physical port in an LACP group.

**Syntax**
config lacp port_priority <portlist> [priority 1-65535] [timeout <90sec | 3sec>]

**Description**
The `config lacp port_priority` command sets the LACP priority value and administrative timeout of a physical port or range of ports in an LACP group.

**Parameters**
- `<portlist>` - A port or range of ports to be configured.
- `<priority 1-65535>` - Specifies the LACP priority value for a port or range of ports to be configured. The default is 1.
- `<timeout>` - Specifies the administrative LACP timeout.
  - `90sec` – Specifies the LACP timeout to be 90 seconds. This is the default.
  - `3sec` – Specifies the LACP timeout to be 3 seconds.

**Restrictions**
Only Administrator or operator-level users can issue this command.

**Example usage:**
To configure the LACP priority of a port:

```
DGS3100# config lacp port_priority 1 priority 2
Success.
DGS3100#
```

**show lacp**

**Purpose**
To display current LACP port mode settings.

**Syntax**
show lacp {<portlist>}

**Description**
The `show lacp` command displays the current LACP mode settings.

**Parameters**
- `<portlist>` - A port or range of ports whose LACP settings are to be displayed.

If no parameter is specified, the system displays the current LACP
Example usage:

To display LACP port mode settings:

```
DGS3100# show lacp

<table>
<thead>
<tr>
<th>Port</th>
<th>Priority</th>
<th>Timeout</th>
</tr>
</thead>
<tbody>
<tr>
<td>1:1</td>
<td>1</td>
<td>90 sec</td>
</tr>
<tr>
<td>1:2</td>
<td>1</td>
<td>90 sec</td>
</tr>
<tr>
<td>1:3</td>
<td>1</td>
<td>90 sec</td>
</tr>
<tr>
<td>1:4</td>
<td>1</td>
<td>90 sec</td>
</tr>
<tr>
<td>1:5</td>
<td>1</td>
<td>90 sec</td>
</tr>
<tr>
<td>1:6</td>
<td>1</td>
<td>90 sec</td>
</tr>
<tr>
<td>1:7</td>
<td>1</td>
<td>90 sec</td>
</tr>
<tr>
<td>1:8</td>
<td>1</td>
<td>90 sec</td>
</tr>
<tr>
<td>1:9</td>
<td>1</td>
<td>90 sec</td>
</tr>
<tr>
<td>1:10</td>
<td>1</td>
<td>90 sec</td>
</tr>
</tbody>
</table>

DGS3100#
```
LLDP COMMANDS

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable lldp (global)</td>
<td></td>
</tr>
<tr>
<td>disable lldp</td>
<td></td>
</tr>
<tr>
<td>enable lldp forward_message</td>
<td></td>
</tr>
<tr>
<td>disable lldp forward_message</td>
<td></td>
</tr>
<tr>
<td>config lldp message_tx_interval</td>
<td>&lt;sec 5 - 32768 &gt;</td>
</tr>
<tr>
<td>config lldp message_tx_hold_multiplier</td>
<td>&lt; 2 - 10 &gt;</td>
</tr>
<tr>
<td>config lldp reinit_delay</td>
<td>&lt; sec 1 - 10 &gt;</td>
</tr>
<tr>
<td>config lldp tx_delay</td>
<td>&lt; sec 1 - 8192 &gt;</td>
</tr>
<tr>
<td>show lldp</td>
<td></td>
</tr>
<tr>
<td>show lldp local_ports</td>
<td>&lt;portlist&gt; [mode{brief</td>
</tr>
<tr>
<td>show lldp remote_ports</td>
<td>&lt;portlist&gt; [mode{brief</td>
</tr>
<tr>
<td>config lldp message_tx_hold_multiplier notification_interval ports reinit_delay tx_delay</td>
<td></td>
</tr>
<tr>
<td>config lldp ports</td>
<td>[&lt;portlist&gt;</td>
</tr>
<tr>
<td>config lldp ports</td>
<td>[&lt;portlist&gt;</td>
</tr>
<tr>
<td>config lldp ports</td>
<td>[&lt;portlist&gt;</td>
</tr>
<tr>
<td>config lldp ports</td>
<td>[&lt;portlist&gt;</td>
</tr>
<tr>
<td>config lldp ports</td>
<td>[&lt;portlist&gt;</td>
</tr>
</tbody>
</table>

Each command is listed in detail, as follows:

**enable lldp (global)**

**Purpose**
To enable LLDP on the switch.

**Syntax**
```
enable lldp
```

**Description**
The *enable lldp* command enables the *Link Layer Discovery Protocol* (LLDP) on the switch.

**Parameters**
None

**Restrictions**
Only Administrator or operator–level users can issue this command.
**Example usage:**

To enable LLDP on the switch:

```plaintext
DGS3100# enable lldp
Success.
DGS3100#
```

### disable lldp (global)

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To disable LLDP on the switch.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>disable lldp</code></td>
</tr>
<tr>
<td>Description</td>
<td>The <code>disable lldp</code> command disables the <strong>Link Discovery Protocol</strong> (LLDP) on the switch.</td>
</tr>
<tr>
<td>Parameters</td>
<td>None</td>
</tr>
<tr>
<td>Restrictions</td>
<td>Only Administrator or operator–level users can issue this command.</td>
</tr>
</tbody>
</table>

**Example usage:**

To disable LLDP on the switch:

```plaintext
DGS3100# disable lldp
Success.
DGS3100#
```

### enable lldp forward_message

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To enable forwarding of LLDP message on the switch. When LLDP is disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>enable lldp forward_message</code></td>
</tr>
<tr>
<td>Description</td>
<td>The <code>enable lldp forward_message</code> command enables lldp forward messaging on the switch.</td>
</tr>
<tr>
<td>Parameters</td>
<td>None</td>
</tr>
<tr>
<td>Restrictions</td>
<td>Only Administrator or operator-level users can issue this command.</td>
</tr>
</tbody>
</table>

**Example usage:**

To enable LLDP forward message on the switch:

```plaintext
DGS3100# enable lldp forward_message
Success.
DGS3100#
```

### disable lldp forward_message

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To disable forwarding of LLDP message on the switch. When LLDP is disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>disable lldp forward_message</code></td>
</tr>
<tr>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>Parameters</td>
<td></td>
</tr>
<tr>
<td>Restrictions</td>
<td></td>
</tr>
</tbody>
</table>
### disable lldp forward_message

**Syntax**

disable lldp forward_message

**Description**
The `disable lldp forward_message` command disables lldp forward messaging on the switch.

**Parameters**
None

**Restrictions**
Only Administrator or operator-level users can issue this command.

**Example usage:**
To disable LLDP forward message on the switch:

```
DGS3100# disable lldp forward_message
Success.
DGS3100#
```

### config lldp message_tx_interval

**Purpose**
To define the lldp message tx interval

**Syntax**
cfg lldp message_tx_interval <5-32768>

**Description**
The `config lldp message_tx_interval` command defines the lldp message interval of the incoming messages.

**Parameters**
message_tx_interval – Defines the message interval time. The range is between 5 and 32768.

**Restrictions**
Only Administrator or operator-level users can issue this command.

**Example usage:**
To configure LLDP message tx interval on the switch:

```
DGS3100# config lldp message_tx_interval 5
Success.
DGS3100#
```

### config lldp message_tx_hold_multiplier

**Purpose**
To define the lldp hold-multiplier on the switch.

**Syntax**
cfg lldp message_tx_hold_multiplier <2-10>

**Description**
The `config lldp message_tx_hold_multiplier <2-10>` command specifies the amount of time the receiving device should hold a Link Layer Discovery Protocol (LLDP) packet before discarding it.

**Parameters**
Message_tx_hold_multiplier (2-10) – Specifies the hold time to be sent in the LLDP update packets as a multiple of the timer value. (Range: 2-10). The default configuration is 4.

**Restrictions**
Only Administrator or operator-level users can issue this command.

**Example usage:**
To configure LLDP Message tx hold multiplier settings:

```
DGS3100# config lldp message_tx_hold_multiplier 2
Success.
```

### config lldp reinit_delay

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To define the lldp reinit–delay on the switch.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>config lldp reinit_delay &lt; sec 1 - 10 &gt;</code></td>
</tr>
<tr>
<td>Description</td>
<td>The <code>lldp reinit_delay</code> seconds command specifies the minimum time an LLDP port will wait before reinitializing LLDP transmission.</td>
</tr>
<tr>
<td>Parameters</td>
<td><code>sec</code> – Specifies the minimum time in seconds an LLDP port will wait before reinitializing LLDP transmission. The range is 1 – 10 seconds. The default configuration is 2 seconds.</td>
</tr>
<tr>
<td>Restrictions</td>
<td>Only Administrator or operator–level users can issue this command.</td>
</tr>
</tbody>
</table>

**Example usage:**

To configure LLDP reinit delay:

```
DGS3100# config lldp reinit_delay 1
Success.
DGS3100#
```

### config lldp tx_delay

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To configure the lldp tx_delay on the switch.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>config lldp tx_delay &lt; sec 1 - 8192 &gt;</code></td>
</tr>
<tr>
<td>Description</td>
<td>The <code>lldp tx_delay</code> command specifies the delay between successive LLDP frame transmissions initiated by value/status changes in the LLDP local systems MIB, use the <code>lldp tx_delay</code> command in global configuration mode.</td>
</tr>
<tr>
<td>Parameters</td>
<td><code>sec</code> – Specifies the minimum time in seconds an LLDP port will wait before reinitializing LLDP transmission. The range is 1 – 10 seconds. The default configuration is 2 seconds.</td>
</tr>
<tr>
<td>Restrictions</td>
<td>Only Administrator or operator-level users can issue this command.</td>
</tr>
</tbody>
</table>

**Example usage:**

To configure LLDP tx delay:

```
DGS3100# config lldp tx_delay 1
Success.
DGS3100#
```
**show lldp**

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To display the <em>Link Layer Discovery Protocol</em> (LLDP) on the switch.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>show lldp configuration [ethernet interface]</code></td>
</tr>
<tr>
<td>Description</td>
<td>The <code>show lldp configuration [ethernet interface]</code> displays the LLDP configuration on the switch.</td>
</tr>
<tr>
<td>Parameters</td>
<td><em>Interface</em> – Ethernet port.</td>
</tr>
<tr>
<td>Restrictions</td>
<td>Only Administrator or operator-level users can issue this command.</td>
</tr>
</tbody>
</table>

**Example usage:**

To show LLDP settings:

```
DGS3100# show lldp
LLDP System Information
Chassis ID Subtype          : MAC Address
Chassis ID                  : 00:00:22:aa:bb:33
System Name                 : DGS-3100
System Description          : DGS-3100-48P Gigabit stackable PoE L2 Managed Switch
System Capabilities         : Bridge

LLDP Configurations
LLDP Status                 : Enabled
LLDP Forward Status         : Disabled
Message Tx Interval         : 5
Message Tx Hold Multiplier  : 2
Tx Delay                    : 1
Reinit Delay                : 1
Notification Interval       : 5

DGS3100#
```

**show lldp ports**

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To display the <em>Link Layer Discovery Protocol</em> (LLDP) ports configuration on the switch.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>show lldp ports &lt;portlist&gt;</code></td>
</tr>
<tr>
<td>Description</td>
<td>The <code>show lldp ports</code> command displays the information regarding the ports.</td>
</tr>
<tr>
<td>Parameters</td>
<td><code>&lt;portlist&gt;</code> – A port or range of ports to be displayed.</td>
</tr>
<tr>
<td>Restrictions</td>
<td>Only Administrator or operator-level users can issue this command.</td>
</tr>
</tbody>
</table>

**Example usage:**

To show the information for port 2:9:

```
DGS3100# show lldp ports 2:9
```
show lldp local_ports

Purpose To display the Link Layer Discovery Protocol (LLDP) configuration that is advertised from a specific port.

Syntax show lldp local_ports <portlist> [mode{brief | normal | detailed}]

Description The show lldp local_ports command displays the configuration that is advertised from a specific port.

Parameters <portlist> – A port or range of ports to be displayed.

Restrictions Only Administrator or operator-level users can issue this command.

Example usage:

To show the local port information for port 2:9 with mode detailed:

DGS3100# show lldp local_ports 2:9 mode detailed

Port ID                      : 2:9
---------------------------------
Port ID Subtype               : Interface Name
Port ID                      : 2:9
Port Description             : Ethernet Interface
Auto-negotiation support     : Supported
Auto-negotiation status      : Disabled
Auto-negotiation Advertised Capabilities : other or unknown
Operational MAU type         : Unknown
DGS-3100#

show lldp remote_ports

Purpose To display information regarding the neighboring devices discovered using LLDP.

Syntax show lldp remote_ports <portlist> [mode{brief | normal | detailed}]

Description The show lldp remote_ports command displays the information regarding neighboring devices.

Parameters <portlist> – A port or range of ports to be displayed.

Restrictions Only Administrator or operator-level users can issue this command.
Restrictions

Only Administrator or operator-level users can issue this command.

Example usage:

To show the information for remote ports:

DGS3100# show lldp remote_ports
DGS3100#

config lldp ports

Purpose
To enable LLDP notification on a port or ports.

Syntax
config lldp ports [<portlist> | all] notification [enable | disable]

Description
The config lldp ports notification command defines lldp notification per port on the switch.

Parameters

ports – ports.
notification[enable | disable] – defines is notification is enabled or disabled.

Restrictions
Only Administrator or operator-level users can issue this command.

Example usage:

To configure LLDP notification:

DGS3100# config lldp ports 1 notification enable
Success.
DGS3100#

config lldp ports

Purpose
To define LLDP admin status on a port or ports.

Syntax
config lldp ports [<portlist> | all] admin_status [tx | rx | both | disable]

Description
The config lldp ports admin status command defines lldp admin status per port on the switch.

Parameters

ports – ports.
Admin status – defines admin status of ports on the switch
Tx- Tx only
Rx – Rx only
Both – Tx and RX
Disable – admin status disabled..

Restrictions
Only Administrator or operator-level users can issue this command.

Example usage:

To configure LLDP admin status

DGS3100# config lldp ports 1 admin_status both
Success.
DGS3100#
**config lldp ports**

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To define LLDP management address advertisement on a port or ports.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>`config lldp ports [&lt;portlist&gt;</td>
</tr>
<tr>
<td>Description</td>
<td>The <code>config lldp mgt_addr</code> command defines if lldp will advertise the switch’s IP address the command is per port on the switch.</td>
</tr>
<tr>
<td>Parameters</td>
<td><code>ports</code> – ports.</td>
</tr>
<tr>
<td>Mgt_addr</td>
<td><code>Mgt_addr</code> – defines whether the management address (IP address) advertisement will be enabled or disabled</td>
</tr>
<tr>
<td>Restrictions</td>
<td>Only Administrator or operator-level users can issue this command.</td>
</tr>
</tbody>
</table>

**Example usage:**

To configure LLDP management address advertisement

```
DGS3100# config lldp ports 1 mgt_addr enable
Success.
DGS3100#
```

**config lldp ports**

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To define LLDP management basic TLVs advertisement on a port or ports.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>`config lldp ports [&lt;portlist&gt;</td>
</tr>
<tr>
<td>Description</td>
<td>The <code>config lldp basic_tlvs</code> command defines if lldp will advertise the switch’s basic TLVs the command is per port on the switch.</td>
</tr>
<tr>
<td>Parameters</td>
<td><code>ports</code> – ports.</td>
</tr>
<tr>
<td>Basic TLVs</td>
<td><code>All</code> – Advertisement of all the basic TLVs</td>
</tr>
<tr>
<td>Port description</td>
<td>Advertisement of Port description</td>
</tr>
<tr>
<td>System name</td>
<td>Advertisement of system name</td>
</tr>
<tr>
<td>System description</td>
<td>Advertisement of System description</td>
</tr>
<tr>
<td>System capabilities</td>
<td>Advertisement of system capabilities</td>
</tr>
<tr>
<td>Restrictions</td>
<td>Only Administrator or operator-level users can issue this command.</td>
</tr>
</tbody>
</table>

**Example usage:**

To configure LLDP Basis TLVs

```
DGS3100# config lldp ports 1 basic_tlvs all enable
Success.
DGS3100#
```
<table>
<thead>
<tr>
<th>Purpose</th>
<th>To define LLDP management basic TLVs advertisement on a port or ports.</th>
</tr>
</thead>
</table>
| Syntax       | `config lldp ports ports [<portlist>][all] dot3_tlvs`  
                | `maciphyconfigurationstatus [enable | disable]`                           |
| Description  | The `config lldp` dot3 TLVs command defines if LLDP will advertise the  
                | `mac_phy_configuration_status` the command is per port on the switch. |
| Parameters   | `ports` – ports.  
                | `dot3_tlvs mac_phy_configuration_status` – defines if the advertisement is  
                | `enabled` or `disabled` |
| Restrictions | Only Administrator or operator-level users can issue this command. |

**Example usage:**

To configure LLDP `mac_phy_configuration` status:

```
DGS3100# config lldp ports 1 dot3_tlvs mac_phy_configuration_status enable
Success.
DGS3100#
```
The Stacking commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

<table>
<thead>
<tr>
<th>Command</th>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>config box_id</td>
<td>current_box_id &lt;value 1-6&gt; new_box_id [auto</td>
</tr>
<tr>
<td>show stack_information</td>
<td></td>
</tr>
</tbody>
</table>

**config box_id**

- **Purpose**: To change the unit ID (stack membership number).
- **Syntax**: `config box_id current_box_id <value 1-6> new_box_id [auto | 1 | 2 | 3 | 4 | 5 | 6]`
- **Description**: The `config box_id` command changes the unit ID (stack membership number). The command takes effect only after rebooting the device.
- **Parameters**:
  - `current_box_id <value 1-6>` - Specifies the unit’s current stack membership number.
  - `new_box_id <auto | 1 | 2 | 3 | 4 | 5 | 6>` - Specifies the unit’s new stack membership number. If `auto` is specified, the system automatically defines the unit’s new ID.
- **Restrictions**: Only Administrator or operator-level users can issue this command.

**Example usage:**

To change the unit ID from 1 to 2:

```
DGS3100# config box_id 1 new_box_id 2
DGS3100#
```

**show stack_information**

- **Purpose**: To display information about the units in the stack.
- **Syntax**: `show stack_information`
- **Description**: The `show stack_information` command displays information about the units in the stack, including the unit numbers, firmware version, hardware version, Master ID and Backup ID.
- **Parameters**: None.
- **Restrictions**: None.

**Example usage:**

191
To display information about units in the stack:

```
DGS3100# show stack_information

Master ID : 1
Backup ID : 2

<table>
<thead>
<tr>
<th>Box ID</th>
<th>User Set</th>
<th>Boot version</th>
<th>Firmware version</th>
<th>H/W version</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Auto</td>
<td>1.0.0.03</td>
<td>1.0.0.28</td>
<td>00.00.01</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>1.0.0.03</td>
<td>1.0.0.28</td>
<td>00.00.01</td>
</tr>
</tbody>
</table>

DGS3100#
```
The PoE commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table. These commands are available only on DGS-3100-24P and DGS-3100-48P.

<table>
<thead>
<tr>
<th>Command</th>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>config poe</td>
<td>`box_id &lt;value 1-6&gt; system_power_limit [ps1</td>
</tr>
<tr>
<td>config poe ports</td>
<td>`&lt;portlist&gt; { state [enable</td>
</tr>
<tr>
<td>show poe</td>
<td></td>
</tr>
</tbody>
</table>

Each command is listed in detail, as follows:

**config poe**

**Purpose**
To configure the parameters for the whole PoE system.

**Syntax**
```plaintext
config poe box_id <value 1-6> system_power_limit [ps1 | ps2 | ps3] disconnect_method [deny_next_port | deny_low_priority_port]
```

**Description**
The `config poe` command configures the parameters for the PoE system on a unit member of the stack.

**Parameters**
- `box_id <value 1-6>` – The unit’s current stack membership number.
- `system_power_limit [ps1 | ps2 | ps3]` – Specifies the power budget of the whole PoE system, according to the type of power supply used (`ps1, ps2, ps3`).
- `disconnect_method` – Configures the power management disconnection method. When the total consumed power exceeds the power budget, the PoE controller initiates a port disconnection to prevent overloading the power supply. The controller uses one of the following two ways to implement the disconnection:
  - `deny_next_port` – After the power budget has been exceeded, the next port attempting to power up is denied, regardless of its priority. This is the default setting.
  - `deny_low_priority_port` – After the power budget has been exceeded, the next port attempting to power up, causes the port with the lowest priority to shut down (to allow high-priority ports to power up).

**Restrictions**
Only Administrator or operator-level users can issue this command.

**Example usage:**
To config the PoE System on the Switch:

```
DGS3100# config poe system_power_limit 300 disconnect_method deny_next_port
```
### config poe ports

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To configure the PoE port settings.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>`config poe ports &lt;portlist&gt; { state [enable</td>
</tr>
<tr>
<td>Description</td>
<td>The <code>config poe ports</code> command configures PoE settings for a port or range of ports.</td>
</tr>
<tr>
<td>Parameters</td>
<td><code>&lt;portlist&gt;</code> – A port or range of ports to be configured or all the ports. <code>&lt;state&gt;</code> – Enables or disables the PoE function on the Switch. <code>&lt;priority&gt;</code> – Setting the port priority affects power-up order and shutdown order. <strong>Power-up order</strong>: When the Switch powers-up or reboots, the ports are powered up according to their priority (<code>critical</code> first, then <code>high</code> and finally <code>low</code>). <strong>Shutdown order</strong>: When the power limit has been exceeded, the ports will shut down according to their priority if the power disconnect method is set to <code>deny_low_priority_port</code>. The possible options are:</td>
</tr>
<tr>
<td></td>
<td>• <code>critical</code> – Specifies that these ports have the highest priority for all configured PoE ports. These ports will be the first ports to receive power and the last to disconnect power.</td>
</tr>
<tr>
<td></td>
<td>• <code>high</code> – Specifies that these ports have the second highest priority for receiving power and shutting down power.</td>
</tr>
<tr>
<td></td>
<td>• <code>low</code> – Specifies that these ports have the lowest priority for receiving and shutting down power. These ports will be the first ports to have their power disconnected if the <code>power_disconnect_method</code> chosen in the <code>config poe</code> command is <code>deny_low_priority_port</code>.</td>
</tr>
<tr>
<td></td>
<td><code>power_limit &lt;value 1-15400&gt;</code> – Specifies the per-port power limit. If a port exceeds 10% of its power limit, the PoE system will shut down that port. The minimum user-defined setting is 1 mW and the maximum is 15400 mW. The default setting is 15400 mW.</td>
</tr>
<tr>
<td>Restrictions</td>
<td>Only Administrator or operator-level users can issue this command.</td>
</tr>
</tbody>
</table>

#### Example usage:

To config the Switch’s ports for PoE:

DGS3100# `config poe ports 1-3 state enable priority critical power_limit 12000`

Success.

DGS3100#

### show poe

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To display the setting and actual values of the whole PoE system.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>show poe</code></td>
</tr>
<tr>
<td>Description</td>
<td>The <code>show poe</code> command displays the settings, actual values and port configuration of the whole PoE system.</td>
</tr>
</tbody>
</table>
Parameters None.
Restrictions None.

**Example usage:**

To display the power settings for the Switch:

```
DGS3100# show poe

<table>
<thead>
<tr>
<th>Port</th>
<th>State</th>
<th>Priority</th>
<th>Power Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

DGS3100#
```
## ACCESS CONTROL LIST COMMANDS

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>create access_profile</strong></td>
<td>profile_id &lt;value 1-15&gt; [ethernet {vlan</td>
</tr>
<tr>
<td><strong>create access_profile</strong></td>
<td>profile_id &lt;value 1-15&gt; [ip</td>
</tr>
<tr>
<td><strong>config access_profile</strong></td>
<td>profile_id &lt;value 1-15&gt; [add access_id [auto assign</td>
</tr>
<tr>
<td><strong>config access_profile</strong></td>
<td>profile_id &lt;value 1-15&gt; [add access_id [auto assign</td>
</tr>
<tr>
<td><strong>config access_profile</strong></td>
<td>profile_id &lt;value 1-15&gt; delete access_id &lt;value 1-240&gt;</td>
</tr>
<tr>
<td><strong>delete access_profile</strong></td>
<td>profile_id &lt;value 1-15&gt;</td>
</tr>
<tr>
<td><strong>show access_profile</strong></td>
<td>{profile_id &lt;value 1-15&gt;}</td>
</tr>
<tr>
<td><strong>config time-range</strong></td>
<td>&lt;range_name 32&gt; [hours start_time &lt;time hh:mm&gt; end_time &lt;time hh:mm&gt;</td>
</tr>
<tr>
<td><strong>show time-range</strong></td>
<td></td>
</tr>
</tbody>
</table>

Each command is listed in detail, as follows:

### create access_profile (for Ethernet)

**Purpose**

To create an access profile on the Switch by examining the Ethernet part of the packet header. Masks entered are 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**

```plaintext
create access_profile profile_id <value 1-15> [ethernet {vlan | source_mac <macmask 00000000000-ffffffffffff> | destination_mac <macmask 00000000000-ffffffffffff> | 802.1p | ethernet_type}]
```
The **create access_profile** command creates a profile for packets that may be accepted or denied by the Switch by examining the Ethernet part of the packet header. Specific values for rules pertaining to the Ethernet part of the packet header may be defined by configuring the **config access_profile** command for Ethernet, as stated below.

**Parameters**

- **profile_id <value 1-15>** – Specifies an index number between 1 and 15 that identifies the access profile being created with this command.
- **ethernet** - Specifies that the Switch examines the layer 2 part of each packet header with emphasis on one or more of the following:
  - **vlan** – Specifies that the Switch examine the VLAN part of each packet header.
  - **source_mac <macmask>** – Specifies a MAC address mask for the source MAC address. This mask is entered in the following hexadecimal format: 00:00:00:00:00:00-FF:FF:FF:FF:FF:FF
  - **destination_mac <macmask>** – Specifies a MAC address mask for the destination MAC address in the following format: 00:00:00:00:00:00-FF:FF:FF:FF:FF:FF
  - **802.1p** – Specifies that the Switch examine the 802.1p priority value in the frame’s header.
- **ethernet_type** – Specifies that the Switch examine the Ethernet type value in each frame’s header.

**Restrictions**

Only administrator or operate-level users can issue this command.

**Example usage:**

To create an Ethernet access profile:

```bash
DGS3100# create access_profile profile_id 1 ethernet vlan 802.1p
Success.
DGS3100#
```

### create access_profile (for IP)

**Purpose**

To create an access profile on the Switch by examining the IP part of the packet header. Masks entered are 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**

```
profile_id <value 1-15> ip [ icmp { type | code } | igmp { type } | tcp { src_port_mask < hex 0x0-0xffff > | dst_port_msk <hex 0x0-0xffff> | flag_mask }{+ | –} {urg | ack | psh | rst | syn | fin }} | udp { src_port_mask < hex 0x0-0xffff > | dst_port_msk <hex 0x0-0xffff> } ] { source_ip_mask <netmask> | destination_ip_mask <netmask> | dscp }
```

**Description**

The **create access_profile** command creates a profile for packets that may be accepted or denied by the Switch by examining the IP part of the packet header. Specific values for rules pertaining to the IP part of the packet header may be defined by configuring the
**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>config access_profile</td>
<td>command for IP, as stated below.</td>
</tr>
<tr>
<td>profile_id &lt;value 1-15&gt;</td>
<td>Specifies an index number between 1 and 15 that identifies the access profile being created with this command.</td>
</tr>
<tr>
<td>ip</td>
<td>Specifies that the Switch examines the IP fields in each packet with special emphasis on one or more of the following:</td>
</tr>
<tr>
<td>source_ip_mask &lt;netmask&gt;</td>
<td>Specifies an IP address mask for the source IP address.</td>
</tr>
<tr>
<td>destination_ip_mask &lt;netmask&gt;</td>
<td>Specifies an IP address mask for the destination IP address.</td>
</tr>
<tr>
<td>dscp</td>
<td>Specifies that the Switch examines the DiffServ Code Point (DSCP) field in each frame’s header.</td>
</tr>
<tr>
<td>icmp</td>
<td>Specifies that the Switch examines the Protocol field in each frame’s IP header, and that the value must be 1 (Internet Control Message Protocol-ICMP) for the action to take place.</td>
</tr>
<tr>
<td>type</td>
<td>Specifies that the Switch examines each frame’s ICMP Type field.</td>
</tr>
<tr>
<td>code</td>
<td>Specifies that the Switch examines each frame’s ICMP Code field.</td>
</tr>
<tr>
<td>igmp</td>
<td>Specifies that the Switch examine each frame’s protocol field and it must be 2 (Internet Group Management Protocol-IGMP) for the action to take place.</td>
</tr>
<tr>
<td>igmp_type</td>
<td>Specifies that the Switch examine each frame’s IGMP Type field.</td>
</tr>
<tr>
<td>tcp</td>
<td>Specifies that the Switch examines each frames protocol field and its value must be 6 (Transmission Control Protocol-TCP) for the action to take place.</td>
</tr>
<tr>
<td>src_port_mask &lt;hex 0x0-0xffff&gt;</td>
<td>Specifies a TCP port mask for the source port.</td>
</tr>
<tr>
<td>dst_port_mask &lt;hex 0x0-0xffff&gt;</td>
<td>Specifies a TCP port mask for the destination port.</td>
</tr>
<tr>
<td>flag_mask {+</td>
<td>-} {urg</td>
</tr>
<tr>
<td>udp</td>
<td>Specifies that the Switch examines each frame’s protocol field and it’s value must be 17 (User Datagram Protocol-UDP) in order for the action to take place.</td>
</tr>
<tr>
<td>src_port_mask &lt;hex 0x0-0xffff&gt;</td>
<td>Specifies a UDP port mask for the source port.</td>
</tr>
<tr>
<td>dst_port_mask &lt;hex 0x0-0xffff&gt;</td>
<td>Specifies a UDP port mask for the destination port.</td>
</tr>
</tbody>
</table>

**Restrictions**

Only administrator or operate-level users can issue this command.

**Example usage:**

To create an IP access profile:

```
DGS3100# create access_profile profile_id 2 ip source_ip_mask 20.0.0.0
```
destination_ip_mask 10.0.0.0 dscp icmp type
Success.
DGS3100#

**config access_profile (for Ethernet)**

**Purpose**
To configure the Ethernet access profile on the Switch and to define specific values for the rules that to 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 operational method, with the values the Switch finds in the specified frame header fields.

**Syntax**

```
config access_profile profile_id <value 1-15> [add access_id [auto assign | <value 1-240>] [ethernet {vlan <vlan_name 32> | source_mac <macaddr 00:00:00:00:00-ff:ff:ff:ff:ff:ff> | destination_mac <macaddr 00:00:00:00:00-ff:ff:ff:ff:ff:ff> | 802.1p <value 0-7> | ethernet_type <hex 0x05dd-0xffff>} ports <portlist> [permit {replace_priority <value 0-7> | replace_dscp <value 0-63> | rate_limit <value 64-1000000>} | deny] {time_range <range_name 32>}
```

**Description**
The `config access_profile` command defines the rules used by the Switch to either filter or forward packets based on the Ethernet part of each packet header.

**Parameters**

- `profile_id <value 1-15>` – Specifies the access profile id to be configured with this command. This value is assigned to the access profile when it is created with the `create access_profile` command. The lower the profile ID, the higher the priority the rule will be given.
- `add access_id <value 1-240>` – Adds an additional rule to the above specified access profile. The value specifies the relative priority of the additional rule. Up to 240 different rules may be configured for the Ethernet access profile.
  - `auto_assign` – Configures the Switch to automatically assign a numerical value (between 1 and 240) for the rule being configured.
  - `ethernet` – Specifies that the Switch examine only the layer 2 part of each packet to determine if it is to be filtered or forwarded based on one or more of the following:
    - `vlan <vlan_name 32>` – Specifies that the access profile applies only to this previously created VLAN.
    - `source_mac <macaddr>` – Specifies that the access profile applies only to packets with this source MAC address. MAC address entries may be made in the following format: 00:00:00:00:00-FF:FF:FF:FF:FF
    - `destination_mac <macaddr>` – Specifies that the access profile applies only to packets with this destination MAC address. MAC address entries may be made in the following format: 00:00:00:00:00-FF:FF:FF:FF:FF
    - `802.1p <value 0-7>` – Specifies that the access profile applies only to packets with this 802.1p priority value.
    - `ethernet_type <hex 0x05dd-0xffff>` – Specifies that the access profile applies only to packets with this hexadecimal
802.1Q Ethernet type value in the packet header.

ports <portlist> - The access profile for Ethernet may be defined for each port on the Switch.

permit - Specifies that packets that match the access profile are permitted to be forwarded by the Switch.

- replace_priority - Specifies the value to replace the 802.1p default priority of a packet, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being forwarded by the Switch.

- replace_dscp <value 0-63> - Specifies 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.

- rate_limit <value 64-1000000> - Specifies the rate limit to limit Rx bandwidth for the profile being configured. This rate is implemented using the following equation – 1 value = 64kbit/sec. (ex. If the user selects a rx rate limit of 10 then the ingress rate is 640kbit/sec.) The user may select a value between 64-1000000 or no limit. The default setting is no limit.

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

- time_range <range_name 32> - Defines a time range name.

Restrictions: Only Administrator or operator-level users can issue this command.

Example usage:

To configure a rule for the Ethernet access profile:

DGS3100# config access profile profile_id 1 add access_id 1 ethernet vlan Trinity 802.1p 1 port 1 permit priority 1 replace priority 1

Success.

DGS3100#
The **config access_profile** command defines the rules used by the Switch to either filter or forward packets based on the IP part of each packet header.

### Parameters

- **profile_id <value 1-15>** – Specifies the access profile id to be configured with this command. This value is assigned to the access profile when it is created with the **create access_profile** command. The lower the profile ID, the higher the priority the rule will be given.

- **add access_id <value 1-240>** – Adds an additional rule to the above specified access profile. The value specifies the relative priority of the additional rule. Up to 240 different rules may be configured for the IP access profile.
  - **auto_assign** – Configures the Switch to automatically assign a numerical value (between 1 and 240) for the rule being configured.

- **ip** – Specifies that the Switch examine the IP fields in each packet to determine if it will be either forwarded or filtered based on one or more of the following:
  - **source_ip <ipaddr>** – Specifies that the access profile applies only to packets with this source IP address.
  - **destination_ip <ipaddr>** – Specifies that the access profile applies only to packets with this destination IP address.
  - **dscp <value 0-63>** – Specifies that the access profile applies 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 examine the protocol field in each frame’s header and it should match Internet Control Message Protocol (ICMP).
    - **type** – Specifies that the Switch examine each frame’s ICMP Type field.
    - **code** – Specifies that the Switch examine each frame’s ICMP Code field.
    - **igmp** – Specifies that the Switch examine each frame’s protocol and it should match Internet Group Management Protocol (IGMP) field.
      - **type** – Specifies that the Switch examine each frame’s IGMP Type field.
  - **tcp** – Specifies that the Switch examine each frame’s protocol and it should match Transport Control Protocol (TCP) field.
    - **src_port <value 0-65535>** – Specifies that the access profile applies only to packets that have this TCP source port in their TCP header.
    - **dst_port <value 0-65535>** – Specifies that the access profile applies only to packets that have this TCP destination port in their TCP header.

- **flag (+ | –) {urg | ack | psh | rst | syn | fin}** – Specifies the appropriate flag parameter. All incoming packets have TCP flag bits associated with them which are parts of a packet that determine what to do with the packet. The user may deny packets by denying certain flag bits within the packets.

To specify flag bits that should be “1” type + and the flag bit
name, to specify bits that should be "0" type – and the flag bit name.

- **udp** – Specifies that the Switch examine the protocol field in each packet and it should match User Datagram Protocol (UDP).
- **src_port <value 0-65535>** – Specifies that the access profile applies only to packets that have this UDP source port in their header.
- **dst_port <value 0-65535>** – Specifies that the access profile applies only to packets that have this UDP destination port in their header.
- **protocol_id <value 0-255>** – Specifies that the Switch examine the Protocol field in each packet and if this field contains the value entered here, apply the appropriate rules.
- **user_define <hex 0x0-0xffffffff>** – Specifies a hexadecimal value to identify the protocol to be discovered in the packet header.

ports [<portlist> | <ch1-32>] | - The access profile for IP may be defined for each port on the Switch.

- **permit** – Specifies that packets that match the access profile are permitted to be forwarded by the Switch special actions may be added to the rule such as:
  - **replace_priority** – Specifies the value to replace the 802.1p default priority of a packet, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being forwarded by the Switch.
  - **replace_dscp <value 0-63>** – Specifies 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.
  - **rate_limit <value 64-1000000>** – Specifies the kbps rate limit to limit Rx bandwidth for for the profile being configured. The user may select a value between 64- 1000000 or no limit. The default setting is no limit.

- **deny** – Specifies that packets that do not match the access profile are not permitted to be forwarded by the Switch and will be filtered.
  - **time_range <range_name 32>** – Defines a time range name.

Restrictions

Only administrator or operate-level users can issue this command.

Example usage:

To configure a rule for the IP access profile:

```
DGS3100# config access_profile profile_id 2 add access_id 2 ip protocol_id 2 port 2 deny
Success.
DGS3100#
```
### config access_profile

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To delete a specific rule from the access profile on the Switch.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>config access_profile profile_id &lt;value 1-15&gt; delete access_id &lt;value 1-240&gt;</code></td>
</tr>
<tr>
<td>Description</td>
<td>The <code>config access_profile</code> command deletes a specific rule from the access profile on the Switch.</td>
</tr>
</tbody>
</table>
| Parameters | `profile_id <value 1-15>` - Specifies the access profile id that is used to identify the access profile to be configured with this command.  
`delete access_id <value 1-240>` – Specifies the specific rule to be deleted from the profile. |
| Restrictions | Only administrator or operate-level users can issue this command. |

**Example usage:**

To delete a rule from the access profile:

```
DGS3100# config access_profile profile_id 2 delete access_id 2
Success.
DGS3100#
```

### delete access_profile

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To delete a previously created access profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>delete access_profile profile_id &lt;value 1-15&gt;</code></td>
</tr>
<tr>
<td>Description</td>
<td>The <code>delete access_profile</code> command deletes a previously created access profile on the Switch.</td>
</tr>
<tr>
<td>Parameters</td>
<td><code>profile_id &lt;value 1-15&gt;</code> – Specifies the access profile to be deleted.</td>
</tr>
<tr>
<td>Restrictions</td>
<td>Only administrator or operate-level users can issue this command.</td>
</tr>
</tbody>
</table>

**Example usage:**

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

```
DGS3100# delete access_profile profile_id 1
Success.
DGS3100#
```

### show access_profile

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To display the currently configured access profiles on the Switch.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>show access_profile (profile_id &lt;value 1-15&gt;)</code></td>
</tr>
<tr>
<td>Description</td>
<td>The <code>show access_profile</code> command displays the currently configured access profiles.</td>
</tr>
<tr>
<td>Parameters</td>
<td><code>profile_id &lt;value 1-15&gt;</code> – Specifies the access profile to be displayed. This value is assigned to the access profile when it is created with the <code>create access_profile</code> command. If the <code>profile_id</code> is not specified, all access profiles are displayed.</td>
</tr>
</tbody>
</table>

parameter is omitted, all access profile entries are displayed.

Restrictions Only Administrator or operator-level users can issue this command.

Example usage:

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

```
DGS3100# show access_profile

Access Profile Table

Access Profile ID: 1          TYPE : Ethernet
======================================================================
MASK Option :
VLAN      802.1p
-----------      ------
Access ID : 3              Mode: Permit(replaced) priority: 1
Ports: 1
-----------  ------
Trinity      1
======================================================================

Access Profile ID: 2          TYPE : IP
======================================================================
MASK Option :
Protocol ID
--------------------
Access ID : 2              Mode: Deny
Ports: 2
--------------------
2
======================================================================

Total Entries: 2

DGS3100#
```

```
config time_range

Purpose To configure the time range on the Switch.

Syntax `config time_range <range_name 32> [hours start_time <time hh:mm> end_time <time hh:mm> weekdays <daylist> | delete]`

Description The `config time_range` command defines time ranges for access lists.

Parameters
- `range-name` – Specifies the time range name. The range of characters is 1 - 32.
- `start_time <time hh:mm>` - defines the time on which the time range will start to be active.
- `end_time <time hh:mm>` - defines the time on which the time range will stop to be active.
- `weekdays <daylist>` - defines the days of the week on which the time range will be active.
- `comment`: - If the end time is earlier than the start time, the end time will move to the following day.

Restrictions Only Administrator or operator-level users can issue this command.
```
Example usage:
To configure the time range on the Switch:

```
DGS3100# DGS-3100# config time_range xxx hours start_time 10:00 end_time 11:00 weekdays wed sun
Success.
DGS3100#
```

**show time_range**

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To display the currently configured access profiles on the Switch.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>show time_range</code></td>
</tr>
<tr>
<td>Description</td>
<td>The <code>show time_range</code> command displays the time range configuration.</td>
</tr>
<tr>
<td>Parameters</td>
<td>None</td>
</tr>
<tr>
<td>Restrictions</td>
<td>None</td>
</tr>
</tbody>
</table>

Example usage:
To display time range settings on the Switch:

```
DGS3100# show time_range
Range name : xxx
Start time : 10:00
End time   : 11:00
Days       : wed sun
Total Entries : 1
DGS3100#
```
TRAFFIC SEGMENTATION COMMANDS

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>config traffic_segmentation</td>
<td>[&lt;portlist&gt;</td>
</tr>
<tr>
<td>show traffic_segmentation</td>
<td>{&lt;portlist&gt;}</td>
</tr>
</tbody>
</table>

Each command is listed in detail, as follows:

**config traffic_segmentation**

- **Purpose**: To configure traffic segmentation on the Switch.
- **Syntax**: `config traffic_segmentation [<portlist> | <ch1-32> | all] forward_list [<portlist> | <ch1-32> | all]`
- **Description**: The `config traffic_segmentation` command configures traffic segmentation on the Switch.
- **Parameters**:
  - `<portlist>`: A port or a port channel for which the current traffic segmentation configuration on the Switch is to be displayed.
  - `<ch1-32>`: A port-channel.
  - `all`: Configures all ports on the Switch.
  - `forward_list`: Specifies a port or a port channel to receive forwarded frames from the source ports specified in the portlist, above.
- **Restrictions**: Only administrator or operator-level users can issue this command.

**Example usage:**

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

```
DGS3100# config traffic_segmentation 1 forward_list 11
Success.
DGS3100#
```

**show traffic_segmentation**

- **Purpose**: To display the current traffic segmentation configuration on the Switch.
- **Syntax**: `show traffic_segmentation {<portlist>}`
- **Description**: The `show traffic_segmentation` command displays the current traffic segmentation configuration on the Switch.
- **Parameters**:
  - `<portlist>`: A port or a port channel for which the current traffic segmentation configuration on the Switch is to be displayed.
Restrictions: The port lists for segmentation and the forward list must be on the same Switch.

**Example usage:**

To display the current traffic segmentation configuration on the Switch.

```
DGS3100# show traffic_segmentation
Traffic Segmentation Table

<table>
<thead>
<tr>
<th>Port</th>
<th>Forward Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>7</td>
<td>1</td>
</tr>
<tr>
<td>8</td>
<td>1</td>
</tr>
<tr>
<td>9</td>
<td>1</td>
</tr>
<tr>
<td>10</td>
<td>1</td>
</tr>
<tr>
<td>11</td>
<td>1</td>
</tr>
<tr>
<td>12</td>
<td>1</td>
</tr>
<tr>
<td>13</td>
<td>1</td>
</tr>
<tr>
<td>14</td>
<td>1</td>
</tr>
<tr>
<td>15</td>
<td>1</td>
</tr>
<tr>
<td>16</td>
<td>1</td>
</tr>
<tr>
<td>17</td>
<td>1</td>
</tr>
<tr>
<td>18</td>
<td>1</td>
</tr>
</tbody>
</table>
```

CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
The Traceroute commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

<table>
<thead>
<tr>
<th>Command</th>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>traceroute</td>
<td>{ipv4-address</td>
</tr>
</tbody>
</table>

Each command is listed in detail, as follows:

**traceroute**

**Purpose**
Used to discover the routes packets actually take when traveling to their destination.

**Syntax**
`traceroute {ipv4-address | hostname} [size 40-1472] [ttl 1-255] [count 1-10] [timeout 1-60] [source ip-address] [tos 0-255]`

**Description**
The `traceroute` command takes advantage of the error messages generated by the devices when a datagram exceeds its time-to-live (TTL) value.

The `traceroute` command starts by sending probe datagrams with a TTL value of one. This causes the first device to discard the probe datagram and send back an error message. The `traceroute` command sends several probes at each TTL level and displays the round-trip time for each.

The `traceroute` command sends out one probe at a time. Each outgoing packet may result in one or two error messages. A 'time exceeded' error message indicates that an intermediate device has seen and discarded the probe. A 'destination unreachable' error message indicates that the destination node has received the probe and discarded it because it could not deliver the packet. If the timer goes off before a response comes in, the `traceroute` command prints an asterisk (*).

The `traceroute` command terminates when the destination responds, when the maximum TTL is exceeded or when the user interrupts the trace by pressing Esc.

**Parameters**
- **ipv4-address** – Specifies the IP address of the destination host.
- **hostname** – Defines the host name of the destination host. (Range: 1-158 characters).
- **packet_size** - Defines the number of bytes in a packet. (Range: 40-1472).
- **max-ttl** - Defines the largest TTL value that can be used. The `traceroute` command terminates when the destination is reached or when this value is reached. (Range: 1-255)
- **packet_count** - The number of probes to be sent at each TTL level. (Range: 1-10)
- **time_out** - Specifies the number of seconds to wait for a response to a probe packet. (Range: 1-60)
- **source ip-address** - Specifies one of the device’s interface addresses to use as a source address for the probes. The device normally selects what it feels is the best source address to use.
\textit{Tos} - Specifies the Type-Of-Service byte in the IP Header of the packet. (Range: 0-255)

Restrictions Only Administrator or operator-level users can issue this command.

**Example usage:**

To discover the routes packets take when traveling to their destination:

```
DGS3100# traceroute umaxp1.physics.lsa.umich.edu
Type Esc to abort.

Tracing the route to umaxp1.physics.lsa.umich.edu (141.211.101.64)
1 i2-gateway.stanford.edu (192.68.191.83) 0 msec 0 msec 0 msec
2 STAN.POS.calren2.NET (171.64.1.213) 0 msec 0 msec 0 msec
3 SUNV--STAN.POS.calren2.net (198.32.249.73) 1 msec 1 msec 1 msec
4 Abilene--QSV.POS.calren2.net (198.32.249.162) 1 msec 1 msec 1 msec
5 kscyng-snvang.abilene.ucaid.edu (198.32.8.103) 33 msec 35 msec 35 msec
6 iplsng-kscyng.abilene.ucaid.edu (198.32.8.80) 47 msec 45 msec 45 msec
7 so-0-2-0x1.aa1.mich.net (192.122.183.9) 56 msec 53 msec 54 msec
8 atm1-0x24.michnet8.mich.net (198.108.23.82) 56 msec 56 msec 57 msec
9 * * *
10 A-ARB3-LSA-NG.c-SEB.umnet.umich.edu (141.211.5.22) 58 msec 58 msec 58 msec
11 umaxp1.physics.lsa.umich.edu (141.211.101.64) 62 msec 63 msec 63 msec

DGS3100#
```
SAFEGUARD COMMANDS

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>config safeguard_engine</td>
<td>state [enable</td>
</tr>
<tr>
<td>show safeguard_engine</td>
<td></td>
</tr>
</tbody>
</table>

Each command is listed in detail, as follows:

**config safeguard_engine**

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To define the safeguard engine on the switch.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>state [enable</td>
</tr>
<tr>
<td>Description</td>
<td>To define the safeguard_engine on the switch.</td>
</tr>
<tr>
<td>Parameters</td>
<td>state [enable</td>
</tr>
<tr>
<td></td>
<td>Indicates the CPU Utilization thresholds. The possible field values are:</td>
</tr>
<tr>
<td></td>
<td>• rising – Indicates the rising CPU Utilization thresholds. The possible field range is between 20%-100%. The default value is 70%.</td>
</tr>
<tr>
<td></td>
<td>• falling – Indicates the falling CPU Utilization thresholds. The possible field range is between 20%-100%. The default value is 20%.</td>
</tr>
<tr>
<td>Restrictions</td>
<td>Only Administrator or operator-level users can issue this command.</td>
</tr>
</tbody>
</table>

Example usage:

To define safeguard engine on the switch:

```
DGS-3100# config safeguard_engine state enable rising 70 falling 20
Success.
DGS-3100#
```
### show safeguard_engine

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To show the safeguard engine status on the switch.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><strong>show safeguard_engine</strong></td>
</tr>
<tr>
<td>Description</td>
<td>To show the safeguard engine on the switch.</td>
</tr>
<tr>
<td>Parameters</td>
<td>None.</td>
</tr>
<tr>
<td>Restrictions</td>
<td>Only Administrator or operator-level users can issue this command.</td>
</tr>
</tbody>
</table>

#### Example usage:

To show the safeguard engine status on the switch:

```
DGS-3100# show safeguard_engine

Safe Guard : Enable

Rising Threshold (20%-100%) : 70
Falling Threshold (20%-100%) : 20
Status : No attack
DGS-3100#
```
This appendix contains the device specifications, and contains the following topics:
- Technical Specifications
- Cable Lengths

## Technical Specifications

<table>
<thead>
<tr>
<th></th>
<th>Performance</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Transmission Method</strong></td>
<td>Store-and-forward</td>
</tr>
<tr>
<td><strong>RAM Buffer</strong></td>
<td>512Kbytes per device</td>
</tr>
<tr>
<td><strong>Packet Filtering/ Forwarding Rate</strong></td>
<td>Full-wire speed for all connections. 1,488,095 pps per port (for 1000Mbps)</td>
</tr>
<tr>
<td><strong>MAC Address Learning</strong></td>
<td>Automatic update. Supports 8K MAC address.</td>
</tr>
<tr>
<td><strong>Priority Queues</strong></td>
<td>4 Priority Queues per port.</td>
</tr>
<tr>
<td><strong>Forwarding Table Age Time</strong></td>
<td>Max age: 10–1000000 seconds. Default = 300.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Physical and Environmental</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AC Inputs</strong></td>
<td>100 – 240 VAC, 50/60 Hz (internal universal power supply)</td>
</tr>
<tr>
<td><strong>Power Consumption</strong></td>
<td>45 watts maximum for the DGS-3100-24 and DGS-3100-24P 82 watts maximum for the DGS-3100-48 and DGS-3100-48P</td>
</tr>
<tr>
<td><strong>DC Fans</strong></td>
<td>2 built-in 40 x 40 x 10 mm fans</td>
</tr>
<tr>
<td><strong>Operating Temperature</strong></td>
<td>0 to 40 degrees Celsius (32 to 104 degrees Fahrenheit)</td>
</tr>
<tr>
<td><strong>Storage Temperature</strong></td>
<td>-40 to 70 degrees Celsius (-40 to 158 degrees Fahrenheit)</td>
</tr>
<tr>
<td><strong>Humidity</strong></td>
<td>Storage: 5% to 95% non-condensing</td>
</tr>
<tr>
<td><strong>Dimensions</strong></td>
<td>441mm (W) x 309mm (D) x 44mm (H), 19-inch rack-mount width 1U height</td>
</tr>
<tr>
<td><strong>Weight</strong></td>
<td>3.8 kg (8.38 lb)</td>
</tr>
<tr>
<td><strong>EMI</strong></td>
<td>FCC, CE Mark</td>
</tr>
<tr>
<td><strong>Safety</strong></td>
<td>CSA International</td>
</tr>
</tbody>
</table>
### General

<table>
<thead>
<tr>
<th>Standards</th>
<th>IEEE 802.3 10BASE-T Ethernet</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>IEEE 802.3u 100BASE-TX Fast Ethernet</td>
</tr>
<tr>
<td></td>
<td>IEEE 802.3z Gigabit Ethernet</td>
</tr>
<tr>
<td></td>
<td>IEEE 802.1Q Tagged VLAN</td>
</tr>
<tr>
<td></td>
<td>IEEE 802.1P Tagged Packets</td>
</tr>
<tr>
<td></td>
<td>IEEE 802.3ab 1000BASE-T</td>
</tr>
<tr>
<td></td>
<td>IEEE 802.3x Full-duplex Flow Control</td>
</tr>
<tr>
<td></td>
<td>ANSI/IEEE 802.3 NWay auto-negotiation</td>
</tr>
</tbody>
</table>

| Protocols                  | CSMA/CD  |

### Data Transfer Rates

- **Ethernet**: Half-duplex, Full-duplex
  - 10 Mbps
  - 20 Mbps

- **Fast Ethernet**: 100 Mbps, 200 Mbps
  - 2000 Mbps (Full duplex only)

### Topology

- Star

### Network Cables

<table>
<thead>
<tr>
<th>10BASE-T:</th>
<th>UTP Category 3, 4, 5 (100 meters max.)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>EIA/TIA-568 150-ohm STP (100 meters max.)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>100BASE-TX:</th>
<th>UTP Cat. 5 (100 meters max.)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>EIA/TIA-568 150-ohm STP (100 meters max.)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>1000BASE-T:</th>
<th>UTP Cat. 5e (100 meters max.)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>UTP Cat. 5 (100 meters max.)</td>
</tr>
<tr>
<td></td>
<td>EIA/TIA-568B 150-ohm STP (100 meters max.)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>1000BASE-LX:</th>
<th>Single-mode fiber module (10km)</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>1000BASE-SX:</th>
<th>Multi-mode fiber module (550m)</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>1000BASE-LHX:</th>
<th>Single-mode fiber module (40km)</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>1000BASE-ZX:</th>
<th>Single-mode fiber module (80km)</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Mini-GBIC:</th>
<th>SFP Transceiver for 1000BASE-LX</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Single-mode fiber module (10km)</td>
</tr>
<tr>
<td></td>
<td>SFP Transceiver for 1000BASE-SX</td>
</tr>
<tr>
<td></td>
<td>Multi-mode fiber module (550m)</td>
</tr>
<tr>
<td></td>
<td>SFP Transceiver for 1000BASE-LHX</td>
</tr>
<tr>
<td></td>
<td>Single-mode fiber module (40km)</td>
</tr>
<tr>
<td></td>
<td>SFP Transceiver for 1000BASE-ZX</td>
</tr>
<tr>
<td></td>
<td>Single-mode fiber module (80km)</td>
</tr>
</tbody>
</table>

### Number of Ports:

- 48 x 10/100/1000 Mbps ports
- 4 x GBIC combo ports
## Cable Lengths

Use the following table to as a guide for the maximum cable lengths:

<table>
<thead>
<tr>
<th>Standard</th>
<th>Media Type</th>
<th>Maximum Distance</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Mini GBIC</strong></td>
<td>DEM-310GT: SFP Transceiver for 1000BASE-LX, Single-mode fiber module</td>
<td>10km</td>
</tr>
<tr>
<td></td>
<td>DEM-311GT: SFP Transceiver for 1000BASE-SX, Multi-mode fiber module</td>
<td>550m</td>
</tr>
<tr>
<td></td>
<td>DEM-314GT: SFP Transceiver for 1000BASE-LHX, Single-mode fiber module</td>
<td>40km</td>
</tr>
<tr>
<td></td>
<td>DEM-315GT: SFP Transceiver for 1000BASE-ZX, Single-mode fiber module</td>
<td>80km</td>
</tr>
<tr>
<td><strong>1000BASE-T</strong></td>
<td>Category 5e UTP Cable</td>
<td>100m</td>
</tr>
<tr>
<td></td>
<td>Category 5 UTP Cable (1000 Mbps)</td>
<td></td>
</tr>
<tr>
<td><strong>100BASE-TX</strong></td>
<td>Category 5 UTP Cable (100 Mbps)</td>
<td>100m</td>
</tr>
<tr>
<td><strong>10BASE-T</strong></td>
<td>Category 3 UTP Cable (10 Mbps)</td>
<td>100m</td>
</tr>
</tbody>
</table>