



X S T A C K[®]

CLI Reference Guide

Product Model: xStack[®] DGS-3400 Series

Layer 2 Managed Gigabit Ethernet Switch

Release 2.7



TABLE OF CONTENTS

INTRODUCTION	1
USING THE CONSOLE CLI.....	3
COMMAND SYNTAX	7
BASIC SWITCH COMMANDS.....	9
802.1X COMMANDS.....	23
ACCESS AUTHENTICATION CONTROL COMMANDS	45
ACCESS CONTROL LIST (ACL) COMMANDS.....	66
ACL FLOW METERING COMMANDS	77
ADDRESS RESOLUTION PROTOCOL (ARP) COMMANDS	82
BPDU ATTACK PROTECTION COMMANDS	86
COMMAND HISTORY LIST.....	91
COMMAND LOGGING COMMANDS	94
COMPOUND AUTHENTICATION COMMANDS.....	96
CONFIGURATION COMMANDS.....	103
COUNTER COMMANDS	108
DEBUG COMMANDS	112
DHCP LOCAL RELAY COMMANDS	118
DHCP RELAY COMMANDS.....	120
DHCP SERVER SCREENING COMMANDS.....	130
DHCP SERVER COMMANDS	134
DHCPV6 CLIENT COMMANDS.....	149
DHCPV6 RELAY COMMANDS	152
DHCPV6 SERVER COMMANDS.....	158
DIGITAL DIAGNOSTIC MONITORING (DDM) COMMANDS.....	170
D-LINK SINGLE IP MANAGEMENT COMMANDS.....	177
D-LINK UNIDIRECTIONAL LINK DETECTION (DULD) COMMANDS	188
DOMAIN NAME SERVER (DNS) RESOLVER COMMANDS	190
DOMAIN NAME SERVER (DNS) RELAY COMMANDS.....	195
ETHERNET RING PROTECTION SWITCHING (ERPS) COMMANDS.....	199
FILTER DATABASE (FDB) COMMANDS.....	209
GRATUITOUS ARP COMMANDS.....	216
IEEE 802.1Q VLAN COMMANDS	220
IEEE 802.1QINQ COMMANDS.....	230
IGMP AND MLD SNOOPING COMMANDS.....	235
IP DIRECTED BROADCAST COMMANDS	256
IP-MAC-PORT BINDING (IMPB) COMMANDS	259
IP MULTICAST VLAN REPLICATION COMMANDS.....	275
IPV6 NEIGHBOR DISCOVER COMMANDS	281
IPV6 ROUTE COMMANDS.....	287
IPV6 TUNNEL COMMANDS.....	290
JAPANESE WEB-BASED ACCESS CONTROL (JWAC) COMMANDS	296

JUMBO FRAME COMMANDS	315
LIMITED IP MULTICAST ADDRESS.....	317
LINK AGGREGATION COMMANDS.....	320
LINK LAYER DISCOVERY PROTOCOL (LLDP) COMMANDS.....	325
MAC NOTIFICATION COMMANDS	340
MAC-BASED ACCESS CONTROL COMMANDS	344
MIRROR COMMANDS.....	356
MSTP DEBUG ENHANCEMENT COMMANDS	360
IGMP SNOOPING MULTICAST (ISM) VLAN COMMANDS.....	367
MULTIPLE SPANNING TREE PROTOCOL (MSTP) COMMANDS	372
NETWORK LOAD BALANCING (NLB) COMMANDS.....	382
PASSWORD ENCRYPTION COMMANDS	385
PASSWORD RECOVERY COMMANDS.....	389
PING COMMANDS	392
PORT SECURITY COMMANDS	396
POWER OVER ETHERNET (POE) COMMANDS.....	399
PROTOCOL VLAN GROUP COMMANDS.....	403
QUALITY OF SERVICE (QOS) COMMANDS	408
REMOTE COPY PROTOCOL (RCP) COMMANDS.....	419
REMOTE SWITCHED PORT ANALYZER (RSPAN) COMMANDS.....	428
ROUTING INFORMATION PROTOCOL (RIP) COMMANDS.....	434
SAFEGUARD ENGINE COMMANDS	437
SECURE SHELL (SSH) COMMANDS	440
SECURE SOCKETS LAYER (SSL) COMMANDS	446
SFLOW COMMANDS	451
STACKING COMMANDS	459
STATIC MAC-BASED VLAN COMMANDS	463
SUBNET VLAN COMMANDS.....	465
SWITCH PORT COMMANDS	469
SYSLOG OR TRAP SOURCE-INTERFACE COMMANDS	475
SYSTEM LOG COMMANDS.....	478
TECHNICAL SUPPORT COMMANDS.....	488
TELNET CLIENT COMMANDS	491
TFTP CLIENT COMMANDS	492
TIME AND SNTP COMMANDS	496
TIME RANGE COMMANDS.....	502
TRACE ROUTE COMMANDS	504
TRAFFIC CONTROL COMMANDS.....	507
TRAFFIC SEGMENTATION COMMANDS.....	511
TRUSTED HOST COMMANDS	513
UNICAST ROUTE COMMANDS.....	515
UTILIZATION COMMANDS.....	521

WEB-BASED ACCESS CONTROL (WAC) COMMANDS.....	524
TECHNICAL SPECIFICATIONS.....	534
PASSWORD RECOVERY PROCEDURE	536

INTRODUCTION

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

The DGS-3400 Layer 2 stackable Gigabit Ethernet switch series are members of the D-Link xStack® family. Ranging from 10/100Mbps edge switches to core gigabit switches, the xStack® switch family has been future-proof designed to provide a stacking architecture with fault tolerance, flexibility, port density, robust security and maximum throughput with a user-friendly management interface for the networking professional.

This manual provides a reference for all of the commands contained in the CLI for the xStack® DGS-3426, DGS-3427, DGS-3450 and DGS-3426P series of switches. Configuration and management of the Switch via the Web-based management agent is discussed in the User's Guide.



NOTE: For the remainder of this manual, all versions of the DGS-3426, DGS-3427, DGS-3450, and DGS-3426P switches will be referred to as simply the Switch or the DGS-3450.

Accessing the Switch via the Serial Port

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

- **115200 baud**
- **no parity**
- **8 data bits**
- **1 stop bit**

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 or refresh the console screen.

```
DGS-3450 Gigabit Ethernet Switch
Command Line Interface

Firmware: Build 2.70.B56
Copyright(C) 2010 D-Link Corporation. All rights reserved.

UserName:
```

Figure 1-1. Initial CLI screen

There is no initial username or password. Just press the Enter key twice to display the CLI input cursor –DGS-3450:admin# . This is the command line where all commands are input.

Setting the Switch's IP Address

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

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

```

Boot Procedure 1.00-B13
-----
Power On Self Test ..... 100 %

MAC Address   : 00-19-5B-F5-26-C0
H/W Version   : 1A1G

Please wait, loading V2.70.B56 Runtime image ..... 100 %
UART init     ..... 100 %
Device Discovery ..... -
    
```

Figure 1-2. Boot screen

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

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

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

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

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

```

DGS-3450:admin# config ipif System ipaddress 10.24.22.200/255.0.0.0
Command: config ipif System ipaddress 10.24.22.200/8

Success.

DGS-3450:admin#
    
```

Figure 1-3. Assigning an IP Address

In the above example, the Switch was assigned an IP address of 10.24.22.200 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.

USING THE CONSOLE CLI

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 SNMP-based network management software over the network.

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



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

Connecting to the Switch

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

- **VT-100 compatible**
- **115200 baud**
- **8 data bits**
- **No parity**
- **One stop bit**

No flow control

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

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

```
DGS-3450 Gigabit Ethernet Switch
Command Line Interface

Firmware: Build 2.70.B56
Copyright(C) 2010 D-Link Corporation. All rights reserved.

UserName:
Password:

DGS-3450:admin# _
```

Figure 2- 1. Initial Console Screen after logging in

Commands are entered at the command prompt, **DGS-3450:admin#** .

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

```

DGS-3450:admin# ?
Command: ?

..
?
cable_diag ports
clear
clear address_binding dhcp_snoop binding_entry ports
clear address_binding nd_snoop binding_entry ports
clear arptable
clear attack_log
clear counters
clear dhcp_binding
clear dhcpv6 binding
clear fdb
clear igmp_snooping date_driven_group
clear jwac auth_state
clear log
clear mac_based_access_control auth_state
clear mld_snooping data_driven_group
clear port_security_entry port
clear wac auth_state
config 802.1p default_priority
config 802.1p user_priority
config 802.1x auth_failoverCTRL+C ESC q Quit SPACE n Next Page Enter Next Entry a All

```

Figure 2- 2. The ? Command

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

```

DGS-3450:admin# config account
Command: config account
Next possible completions:
<username>

DGS-3450:admin#

```

Figure 2- 3. Example Command Parameter Help

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

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

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


```
DGS-3450:admin# config account
Command: config account
Next possible completions:
<username>

DGS-3450:admin# config account
```

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

In the above example, the command **config account** was entered without the required parameter **<username>**, the CLI returned the **Next possible completions: <username>** prompt. The up arrow cursor control key was pressed to re-enter the previous command (**config account**) at the command prompt. Now the appropriate 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, braces { } indicate optional parameters or a choice of parameters, and brackets [] indicate required parameters.

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

```
DGS-3450:admin# the
Available commands:
..                ?                cable_diag        clear
config            create                debug              delete
disable           download              enable              login
logout            no                    ping                ping6
reboot            reconfig              reset                save
show              telnet                traceroute          traceroute6
upload

DGS-3450:admin#
```

Figure 2- 5. Available Commands

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

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

```
DGS-3450:admin# create
Command: create
Next possible completions:
802.1x          access_profile    account           address_binding
arprentry      authen            authen_enable    authen_login
authentication  cpu              dhcp             dhcpv6
dot1v_protocol_group  double_vlan      erps
fdb            host_name        igmp_snooping   ip_tunnel
ipif          ipmc_vlan_replication_entry  iproute
ipv6          ipv6route        jwac            link_aggregation
mac_based_access_control  mac_based_access_control_local
mac_based_vlan  mirror          multicast_fdb    nlb
route         rspan          sflow           snmp
stp          subnet_vlan    syslog          trusted_host
vlan         vlan_translation  wac
```

DGS-3450:admin#

Figure 2- 6. Next possible completions: Create command

In the above example, all of the possible next parameters for the **create** command are displayed.

COMMAND SYNTAX

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



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

<angle brackets>

Purpose	Encloses a variable or value that must be specified.
Syntax	create ipif <ipif_name 12> <network_address> (<ip_addr/netmask>) <vlan_name 32> {secondary state [enable disable]}
Description	In the above syntax example, users must supply an IP interface name in the <ipif_name> space, a VLAN name in the <vlan_name 32> space, and the network address, including the netmask, in the <network_address> (<ip_addr/netmask>) space. Do not type the angle brackets.
Example Command	create ipif Engineering 10.24.22.5/255.0.0.0 Design

[square brackets]

Purpose	Encloses a required value or set of required arguments. One value or argument can be specified.
Syntax	create account [admin operator user] <username 15>
Description	In the above syntax example, users must specify the admin , operator , or user level account to be created. Do not type the square brackets.
Example Command	create account admin ctsnow

| vertical bar

Purpose	Separates two or more mutually exclusive items in a list, one of which must be entered.
Syntax	create account [admin operator user] <username 15>
Description	In the above syntax example, you must specify the admin , operator , or user level account to be created. Do not type the backslash.
Example Command	create account admin ctsnow

{braces}

Purpose	Encloses an optional value or set of optional arguments.
Syntax	reset {[config system]}
Description	In the above syntax example, users have the option to specify config or system . It is not

{braces}

	necessary to specify either optional value, however the effect of the system reset is dependent on which, if any, value is specified. Therefore, with this example there are three possible outcomes of performing a system reset. See the following chapter, Basic Commands for more details about the reset command.
Example command	reset config

Line Editing Key Usage

Delete	Deletes the character under the cursor and then shifts the remaining characters in the line to the left.
Backspace	Deletes the character to the left of the cursor and then shifts the remaining characters in the line to the left.
Insert or Ctrl+R	Toggle on and off. When toggled on, inserts text and shifts previous text to the right.
Left Arrow	Moves the cursor to the left.
Right Arrow	Moves the cursor to the right.
Up Arrow	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.
Down Arrow	The down arrow will display the next command in the command history entered in the current session. This displays each command sequentially as it was entered. Use the up arrow to review previous commands.
Tab	Shifts the cursor to the next field to the left.

Multiple Page Display Control Keys

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

BASIC SWITCH COMMANDS

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

Command	Parameters
create account	[admin operator user] <username 15>
config account	<username> {encrypt [plain_text sha_1] <password>}
show account	
delete account	<username> {<string>}
show session	
show switch	
show serial_port	
config serial_port	{baud_rate [9600 19200 38400 115200] auto_logout [never 2_minutes 5_minutes 10_minutes 15_minutes]}
enable clipaging	
disable clipaging	
enable telnet	<tcp_port_number 1-65535>
disable telnet	
telnet	[<ipaddr> <domain_name 255>] {tcp_port <value 0-65535>}
enable web	<tcp_port_number 1-65535>
disable web	
Save	{[config <config_id 1-2> log all]}
reboot	{<string>}
reset	{[config system]} {<string>}
login	
logout	
show device_status	
config command_prompt	[<string 16> username default]
config greeting_message	{default}
show greeting_message	

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

create account

Purpose	Used to create user accounts.
Syntax	create account [admin operator user] <username 15>
Description	The create account command is used to create user accounts that consist of a username of 1 to 15 characters and a password of 0 to 15 characters. Up to eight user accounts can be created.
Parameters	<p><i>admin <username 15></i> – Enter a name between 1 and 15 alphanumeric characters to define the administrator account created here.</p> <p><i>operator <username 15></i> – Enter a name between 1 and 15 alphanumeric characters to define the operator account created here.</p> <p><i>user <username 15></i> – Enter a name between 1 and 15 alphanumeric characters to define the user account created here.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

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

```
DGS-3450:admin# create account admin dlink
Command: create account admin dlink

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

Success.

DGS-3450:admin#
```

To create an operator-level user account with the username “frazier”.

```
DGS-3450:admin# create account operator frazier
Command: create account operator frazier

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

Success.

DGS-3450:admin#
```

To create a user-level user account with the username “reed”.

```
DGS-3450:admin# create account user reed
Command: create account user reed

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

Success.

DGS-3450:admin#
```

config account

Purpose	Used to configure user accounts.
Syntax	config account <username> {encrypt [plain_text] sha_1} <password>
Description	The config account command configures a user account that has been created using the create account command.
Parameters	<p><i><username></i> – Enter a name between 1 and 15 alphanumeric characters to define the administrator account to configure here.</p> <p><i>encrypt</i> - Specifies that the account uses encryption.</p> <p><i>plain_text</i> - Specifies that the account uses the plain text encryption.</p> <p><i>sha_1</i> - Specifies that the account uses the SHA-1 encryption.</p> <p><i><password></i> - Enter the password here.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the user password of “dlink” account:

```
DGS-3450:admin# config account dlink
Command: config account dlink

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

Success.

DGS-3450:admin#
```

show account

Purpose	Used to display user accounts
Syntax	show account
Description	Displays all user accounts created on the Switch. Up to eight user accounts can exist at one time.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To display the accounts that have been created:

```
DGS-3450:admin# show account
Command: show account

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

DGS-3450:admin#
```

delete account

Purpose	Used to delete an existing user account.
Syntax	delete account <username> {<string>}
Description	The delete account command deletes a user account that has been created using the create account command.
Parameters	<username> <string> – Enter an alphanumeric string of up to 15 characters to define the username.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete the user account “System”:

```
DGS-3450:admin# delete account System
Command: delete account System

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

DGS-3450:admin#
```

show session

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

Example usage:

To display the way that the users logged in:

```
DGS-3450:admin# show session
Command: show session

ID      Live Time      From           Level  Name
--      -
8       03:36:27      Serial Port    5      Anonymous

Total Entries: 1

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


show switch

Purpose	Used to display general information about the Switch.
Syntax	show switch
Description	This command displays information about the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display the Switch's information:

```
DGS-3450:admin# show switch
Command: show switch

Device Type       : DGS-3612 Gigabit Ethernet Switch
MAC Address       : 00-1C-F0-B5-40-00
IP Address        : 10.24.73.21 (Manual)
VLAN Name         : default
Subnet Mask       : 255.0.0.0
Default Gateway   : 0.0.0.0
Boot PROM Version : Build 1.10-B13
Firmware Version  : Build 2.70.B56
Hardware Version  : A1
Serial Number     : P4F7191000001
System Name       :
System Location   :
System Contact    :
Spanning Tree     : Disabled
GVRP              : Disabled
IGMP Snooping     : Disabled
MLD Snooping      : Disabled
RIP               : Disabled
DVMRP            : Disabled
PIM               : Disabled
OSPF              : Disabled
TELNET           : Enabled (TCP 23)
CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

show serial_port

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

Example usage:

To display the serial port setting:

```
DGS-3450:admin# show serial_port
```

```
Command: show serial_port
```

```
Baud Rate      : 115200
Data Bits      : 8
Parity Bits    : None
Stop Bits     : 1
Auto-Logout   : 10 mins
```

```
DGS-3450:admin#
```

config serial_port

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

Example usage:

To configure baud rate:

```
DGS-3450:admin# config serial_port baud_rate 115200
```

```
Command: config serial_port baud_rate 115200
```

```
Success.
```

```
DGS-3450:admin#
```

enable clipaging

Purpose	Used to pause the scrolling of the console screen when the show command displays more than one page.
Syntax	enable clipaging
Description	This command is used when issuing the show command which causes the console screen to rapidly scroll through several pages. This command will cause the console to pause at the end of each page. The default setting is enabled.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

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

```
DGS-3450:admin# enable clipaging
Command: enable clipaging

Success.

DGS-3450:admin#
```

disable clipaging

Purpose	Used to disable the pausing of the console screen scrolling at the end of each page when the show command displays more than one screen of information.
Syntax	disable clipaging
Description	This command is used to disable the pausing of the console screen at the end of each page when the show command would display more than one screen of information.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

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

```
DGS-3450:admin# disable clipaging
Command: disable clipaging

Success.

DGS-3450:admin#
```

enable telnet

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

Example usage:

To enable Telnet and configure port number:

```
DGS-3450:admin# enable telnet 23
Command: enable telnet 23

Success.

DGS-3450:admin#
```

disable telnet

Purpose	Used to disable the Telnet protocol on the Switch.
Syntax	disable telnet
Description	This command is used to disable the Telnet protocol on the Switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable the Telnet protocol on the Switch:

```
DGS-3450:admin# disable telnet
Command: disable telnet

Success.

DGS-3450:admin#
```

telnet

Purpose	Used to login remote system with telnet protocol.
Syntax	telnet [<ipaddr> <domain_name 255>] {tcp_port <value 0-65535>}
Description	This command is used to login remote system with Telnet protocol on the Switch.
Parameters	<p><i><ipaddr></i> – Specify the IP address of telnet server system</p> <p><i><domain_name 255></i> - Specify the domain name used.</p> <p><i>tcp_port</i> – The TCP port number. TCP ports are numbered between 1 and 65535. The “well-known” TCP port for the Telnet protocol is 23.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To login to the remote system using telnet on the Switch:

```
DGS-3450:admin# telnet 10.0.0.8
Command: telnet 10.0.0.8

Success.

DGS-3450:admin#
```

enable web

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

Example usage:

To enable HTTP and configure port number:

```
DGS-3450:admin# enable web 80
Command: enable web 80

Note: SSL will be disabled if web is enabled.
Success.

DGS-3450:admin#
```

disable web

Purpose	Used to disable the HTTP-based management software on the Switch.
Syntax	disable web
Description	This command disables the Web-based management software on the Switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable HTTP:

```
DGS-3450:admin# disable web
Command: disable web

Success.

DGS-3450:admin#
```

save

Purpose	Used to save changes in the Switch's configuration to non-volatile RAM.
Syntax	save {[config <config_id 1-2> log all]}
Description	This command is used to enter the current switch configuration or log file into non-volatile RAM. The saved switch configuration will be loaded into the Switch's memory each time the Switch is restarted.
Parameters	<i>log</i> – Specify to save current Switch log to NV-RAM. <i>all</i> – Use to save the configuration and log file to NV-RAM.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

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

```
DGS-3450:admin# save
Command: save

Saving all configurations to NV-RAM... Done.

DGS-3450:admin#
```

reboot

Purpose	Used to restart the Switch.
Syntax	reboot {<string>}
Description	This command is used to restart the Switch.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To restart the Switch:

```
DGS-3450:admin# reboot
Command: reboot
Are you sure want to proceed with the system reboot? (y|n) y
Please wait, the switch is rebooting...
```

reset

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

Example usage:

To restore all of the Switch's parameters to its default values:

```
DGS-3450:admin# reset config
Command: reset config

Are you sure to proceed with system reset?(y/n) y

Success.

DGS-3450:admin#
```

login

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

Example usage:

To initiate the login procedure:

```
DGS-3450:admin# login
Command: login

UserName:
```

logout

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

Example usage:

To terminate the current user's console session:

```
DGS-3450:admin# logout
```

show device_status

Purpose	Used to display the current status of the hardware of the Switch.
Syntax	show device_status
Description	This command displays the current status of the power and fans on the system. In the fan status display there are fans on the left of the switch, on the right, at the back and a CPU fan, if the fans are working normally the display will read "OK" in the fan field. If any of the fans fail the corresponding field will read 'Fail'.
Parameters	None.
Restrictions	None.

Example usage:

To show the device status of the Switch:

```
DGS-3450:admin# show device_status
```

```
Command: show device_status
```

```
Unit 1:
```

```
Internal Power: Active
```

```
External Power: Fail
```

```
Left Fan      : OK
```

```
Right Fan     : OK
```

```
Back Fan      : OK
```

```
CPU Fan       : OK
```

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


config command_prompt

Purpose	Used to configure the command prompt for the Command Line Interface.
Syntax	config command_prompt [<string 16> username default]
Description	This command is used to configure the command prompt for the CLI interface of the Switch. The current command prompt consists of “product name + : + user level + product name” (ex. DGS-3450:admin#). The user may replace all parts of the command prompt, except the # by entering a string of 16 alphanumeric characters with no spaces, or the user may enter the current login username configured on the Switch.
Parameters	<p><i><string 16></i> – Enter an alphanumeric string of no more than 16 characters to define the command prompt for the CLI interface.</p> <p><i>username</i> – Entering this parameter will replace the current CLI command prompt with the login username configured on the Switch.</p> <p><i>default</i> – Entering this parameter will return the command prompt to its original factory default setting.</p>
Restrictions	The reset command will not alter the configured command prompt, yet the reset system command will return the command prompt to its original factory default setting. Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the command prompt:

```
DGS-3450:admin# config command_prompt Tiberius
Command: config command_prompt Tiberius

Success.

Tiberius:admin#
```

config greeting_message

Purpose	Used to configure the greeting message or banner for the opening screen of the Command Line Interface.
Syntax	config greeting_message {default}
Description	This command is used to configure the greeting message or login banner for the opening screen of the CLI.
Parameters	<i>default</i> – Adding this parameter will return the greeting command to its original factory default configuration.
Restrictions	The reset command will not alter the configured greeting message, yet the reset system command will return the greeting message to its original factory default setting. The maximum character capacity for the greeting banner is 6 lines and 80 characters per line. Entering Ctrl+W will save the current configured banner to the DRAM only. To save it into the FLASH memory, the user must enter the save command. Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the greeting message:

```
DGS-3450:admin# config greeting_message
```

```
Command: config greeting_message
```

```
Greeting Messages Editor
```

```
=====
                        DGS-3450 Gigabit Ethernet Switch
                        Command Line Interface

                        Firmware: Build 2.70.B56
                        Copyright(C) 2010 D-Link Corporation. All rights reserved.
=====
```

<Function Key>		<Control Key>	
Ctrl+C	Quit without save	left/right/	
Ctrl+W	Save and quit	up/down	Move cursor
		Ctrl+D	Delete line
		Ctrl+X	Erase all setting
		Ctrl+L	Reload original setting

show greeting_message

Purpose	Used to view the currently configured greeting message configured on the Switch.
Syntax	show greeting_message
Description	This command is used to view the currently configured greeting message on the Switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To view the currently configured greeting message:

```
DGS-3450:admin# show greeting_message
```

```
Command: show greeting_message
```

```
=====
                        DGS-3450 Gigabit Ethernet Switch
                        Command Line Interface

                        Firmware: Build 2.70.B56
                        Copyright(C) 2010 D-Link Corporation. All rights reserved.
=====
```

```
DGS-3450:admin#
```

802.1X COMMANDS

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

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

Command	Parameters
enable 802.1x	
disable 802.1x	
create 802.1x user	< username 15 >
delete 802.1x user	< username 15 >
show 802.1x user	
config 802.1x auth_protocol	[local radius_eap]
config 802.1x fwd_pdu system	[enable disable]
config 802.1x fwd_pdu ports	[< portlist > all] [enable disable]
config 802.1x authorization network radius	[enable disable]
show 802.1x	{ [auth_state auth_configuration] ports { < portlist > } }
config 802.1x capability ports	[< portlist > all] [authenticator none]
config 802.1x max_users	[<value 1 – 4000> no_limit]
config 802.1x auth_parameter ports	[<portlist> all][default [{ direction [both in]] port_control [force_unauth auto force_auth] quiet_period < sec 0-65535> tx_period < sec 1-65535> supp_timeout < sec 1-65535> server_timeout < sec 1-65535> max_req < value 1-10> reauth_period < sec 1-65535> enable_reauth [enable disable] max_users [< value 1 – 128 > no_limit]} (1)]
config 802.1x auth_mode	[port_based mac_based]
config 802.1x init	[port_based ports [< portlist all >] mac_based ports [< portlist > all] { mac_address < macaddr > }]
config 802.1x reauth	[port_based ports [< portlist all >] mac_based ports [< portlist > all] { mac_address < macaddr > }]
create 802.1x guest_vlan	{ < vlan_name 32 > }
delete 802.1x guest_vlan	{ < vlan_name 32 > }
config 802.1x guest_vlan ports	[< portlist > all] state [enable disable]
show 802.1x guest_vlan	
config radius add	< server_index 1-3 > [< server_ip > < ipv6addr >] key < passwd 32 > [default { auth_port < udp_port_number 1-65535 > acct_port < udp_port_number 1-65535 > timeout < int 1-255 > retransmit < int 1-20 > } (1)]
config radius delete	< server_index 1-3 >
config radius	<server_index 1-3> { ipaddress [<server_ip> <ipv6addr>] key <passwd 32> auth_port [<udp_port_number> default] acct_port [<udp_port_number> default] timeout [<int 1-255> default] retransmit [<int 1-20> default]} (1)
show radius	
show auth_statistics	{ports [<portlist> all]}
show auth_diagnostics	{ports [<portlist> all]}
show auth_session_statistics	{ports [<portlist> all]}
show auth_client	
show acct_client	
config accounting service	[network shell system] state [enable disable]
show accounting service	

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

enable 802.1x

Purpose	Used to enable the 802.1X function.
Syntax	enable 802.1x
Description	The enable 802.1x command enables 802.1X function.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

Used to enable the 802.1X function:

```
DGS-3450:admin#enable 802.1x
Command: enable 802.1x

Success.

DGS-3450:admin#
```

disable 802.1x

Purpose	Used to disable the 802.1X function.
Syntax	disable 802.1x
Description	The disable 802.1x command disable 802.1X function.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable the 802.1X function:

```
DGS-3450:admin# disable 802.1x
Command: disable 802.1x

Success.

DGS-3450:admin#
```

create 802.1x user

Purpose	Used to create an 802.1X user.
Syntax	create 802.1x user < username 15 >
Description	The create 802.1x user command create an 802.1X user.
Parameters	<i>username</i> - Specifies adding user name.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create an 802.1x user “test”:

```
DGS-3450:admin# create 802.1x user test
Command: create 802.1x user test

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

Success.

DGS-3450:admin#
```

delete 802.1x user

Purpose	Used to delete an 802.1X user.
Syntax	delete 802.1x user < username 15 >
Description	The delete 802.1x user command delete an 802.1X user.
Parameters	<i>username</i> - Specifies the adding user name.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete user “test”:

```
DGS-3450:admin# delete 802.1x user test
Command: delete 802.1x user test

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

Success.

DGS-3450:admin#
```

show 802.1x user

Purpose	Used to display the 802.1X user.
Syntax	show 802.1x user
Description	The show 802.1x user command displays the 802.1X user account information.
Parameters	None.
Restrictions	None.

Example usage:

To display the 802.1X user information:

```
DGS-3450:admin# show 802.1x user
```

```
Command: show 802.1x user
```

```
Username      Password
-----
user1         abcds
```

```
Total Entries : 1
```

```
DGS-3450:admin#
```

config 802.1x auth_protocol

Purpose	Used to configure the 802.1X auth protocol.
Syntax	config 802.1x auth_protocol [local radius_eap]
Description	The config 802.1x auth_protocol command configures the 802.1X authentication protocol.
Parameters	<i>local</i> - Specifies the authentication protocol as local. <i>radius_eap</i> - Specifies the authentication protocol as RADIUS EAP.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the 802.1X authentication protocol to RADIUS EAP:

```
DGS-3450:admin# config 802.1x auth_protocol radius_eap
```

```
Command: config 802.1x auth_protocol radius_eap
```

```
Success.
```

```
DGS-3450:admin#
```

config 802.1x fwd_pdu system

Purpose	Used to configure forwarding of EAPOL PDU when 802.1X is disabled.
Syntax	config 802.1x fwd_pdu system [enable disable]
Description	This is a global setting to control the forwarding of EAPOL PDU. When 802.1X functionality is disabled globally or for a port, and if 802.1X fwd_pdu is enabled both globally and for the port, a received EAPOL packet on the port will be flooded in the same VLAN to those ports for which 802.1X fwd_pdu is enabled and 802.1X is disabled (globally or just for the port). The default state is disabled.
Parameters	<i>enable</i> - Enable the forwarding of EAPOL PDU. <i>disable</i> - Disable the forwarding of EAPOL PDU.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure forwarding of EAPOL PDU system state enable:

```
DGS-3450:admin# config 802.1x fwd_pdu system enable
Command: config 802.1x fwd_pdu system enable

Success.

DGS-3450:admin#
```

config 802.1x fwd_pdu ports

Purpose	Used to configure if the port will flood EAPOL PDU when 802.1X functionality is disabled.
Syntax	config 802.1x fwd_pdu ports [< portlist > all] [enable disable]
Description	This is a per port setting to control the forwarding of EAPOL PDU. When 802.1X functionality is disabled globally or for a port, and if 802.1X fwd_pdu is enabled both globally and for the port, a received EAPOL packet on the port will be flooded in the same VLAN to those ports for which 802.1X fwd_pdu is enabled and 802.1X is disabled (globally or just for the port). The default state is disabled.
Parameters	<i>ports</i> - Specifies a range of ports to be configured. <i>all</i> - All ports. <i>enable</i> - Enable forwarding EAPOL PDU receive on the ports. <i>disable</i> - Disable forwarding EAPOL PDU receive on the ports.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure 802.1X fwd_pdu for ports:

```
DGS-3450:admin# config 802.1x fwd_pdu ports 1,2 enable
Command: config 802.1x fwd_pdu ports 1,2 enable

Success.

DGS-3450:admin#
```

config 802.1x authorization network radius

Purpose	The enable or disable the acceptance of an authorized configuration.
Syntax	config 802.1x authorization network radius [enable disable]
Description	The command config 802.1x authorization attributes is used to enable or disable the acceptance of authorized configuration. When the authorization is enabled for 802.1X's RADIUS authentication, the authorized attributes (for example VLAN and 802.1p default priority) assigned by the RADIUS server will be accepted if the global authorization status is enabled.
Parameters	<i>radius</i> - If specified to enable, the authorization attributes (for example VLAN and 802.1p default priority) assigned by the RADIUS server will be accepted if the global authorization status is enabled. The default state is enabled.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

The following example will disable to accept the authorized data assigned from the RADIUS server:


```
DGS-3450:admin# config 802.1x authorization network radius disable
Command: config 802.1x authorization network radius disable

Success.

DGS-3450:admin#
```

show 802.1x

Purpose	Used to display the 802.1X state or configurations.
Syntax	show 802.1x { [auth_state auth_configuration] ports { < portlist > } }
Description	The show 802.1x command displays the 802.1X state or configurations.
Parameters	<p><i>auth_state</i> - Used to display 802.1X authentication state machine of some or all ports</p> <p><i>auth_configuration</i> - Used to display 802.1X configurations of some or all ports.</p> <p><i>portlist</i> - Specifies a range of ports to be displayed.</p> <p>If no port is specified, all ports will be displayed.</p> <p>If no parameter is specified, the 802.1X system configurations will be displayed.</p>
Restrictions	None.

Example usage:

To display the 802.1X states:

```
DGS-3450:admin# show 802.1x auth_state ports 1-4
Command: show 802.1x auth_state ports 1-4

Status:  A - Authorized; U - Unauthorized; (P): Port-Based 802.1X

Port  MAC Address          PAE State      Backend State  Status  VID  Priority
-----
1      00-00-00-00-00-01      Authenticated  Idle          A       4004  3
1      00-00-00-00-00-02      Authenticated  Idle          A       1234  -
1      00-00-00-00-00-04      Authenticating Response       U       -     -
2      - (P)                  Authenticating Request        U       -     -
3      - (P)                  Connecting     Idle          U       -     -
4      - (P)                  Held           Idle          U       -     -

Total Authenticating Hosts :2
Total Authenticated Hosts  :2

DGS-3450:admin#
```

To display the 802.1X system level configurations:

```
DGS-3450:admin# show 802.1x
Command: show 802.1x

802.1X                : Enabled
Authentication Mode   : Port_based
Authentication Protocol : Radius_Eap
Forward EAPOL PDU     : Enabled
Max Users              : no_limit
RADIUS Authorization  : Enabled

DGS-3450:admin#
```

To display the 802.1X port level configurations:

```
DGS-3450:admin# show 802.1x auth_configuration ports 1:1
Command: show 802.1x auth_configuration ports 1:1

Port number           : 1:1
Capability             : None
AdminCrlDir           : Both
OpenCrlDir            : Both
Port Control          : Auto
QuietPeriod           : 60 sec
TxPeriod              : 30 sec
SuppTimeout           : 30 sec
ServerTimeout         : 30 sec
MaxReq                : 2 times
ReAuthPeriod          : 3400 sec
ReAuthenticate        : Disabled
Forward EAPOL PDU On Port : Enabled
Max Users On Port     : 10

DGS-3450:admin#
```

config 802.1x capability

Purpose	Used to configure the port capability.
Syntax	config 802.1x capability ports [< portlist > all] [authenticator none]
Description	The config 802.1x capability command configures the port capability.
Parameters	<i>portlist</i> - Specifies a range of ports to be configured. <i>all</i> - Specifies all ports to be configured. <i>authenticator</i> - The port that wishes to enforce authentication before allowing access to services that are accessible via that port adopts the authenticator role. <i>none</i> - Disable authentication on the specified ports.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the port capability:

```
DGS-3450:admin# config 802.1x capability ports 1:1-1:10 authenticator
Command: config 802.1x capability ports 1:1-1:10 authenticator

Success.

DGS-3450:admin#
```

config 802.1x max_users

Purpose	Used to configure the maximum number of users that can be learned via 802.1X authentication.
Syntax	config 802.1x max_users [<value 1 – 4000> no_limit]
Description	The setting is a global limitation on the maximum number of users that can be learned via 802.1X authentication. In addition to the global limitation, maximum user for per port is also limited. It is specified by config 802.1x auth_parameter command.
Parameters	<i>max_users</i> - Specifies the maximum number of users. The range is 1 to 4000. By default, there is no limit on the maximum users.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure 802.1X number of users to be limited to 200:

```
DGS-3450:admin# config 802.1x max_users 200
Command: config 802.1x max_users 200

Success.

DGS-3450:admin#
```

config 802.1x auth_parameter

Purpose	Used to configure the parameters that control the operation of the authenticator associated with a port.
Syntax	config 802.1x auth_parameter ports [<portlist> all][default [{ direction [both in] port_control [force_unauth auto force_auth] quiet_period < sec 0-65535> tx_period < sec 1-65535> supp_timeout < sec 1-65535> server_timeout < sec 1-65535> max_req < value 1-10> reauth_period < sec 1-65535> enable_reauth [enable disable] max_users [<value 1 – 128> no_limit]} (1)]
Description	The config 802.1x auth_parameter command configures the parameters that control the operation of the authenticator associated with a port.
Parameters	<i>portlist</i> - Specifies a range of ports to be configured. <i>all</i> - All ports. <i>default</i> - Sets all parameter to be default value. <i>direction</i> - Sets the direction of access control. <i>both</i> - For bidirectional access control. <i>in</i> - For unidirectional access control. <i>port_control</i> - You can force a specific port to be unconditionally authorized or unauthorized by setting the parameter of port_control to be force_authorized or force_unauthorized. Besides, the controlled port will reflect the outcome of authentication if port_control is auto. <i>force_authorized</i> - Force a specific port to be unconditionally authorized. <i>auto</i> - The controlled port will reflect the outcome of authentication.

config 802.1x auth_parameter

force_unauthorized - Force a specific port to be unconditionally unauthorized.

quiet_period - It is the initialization value of the quietWhile timer. The default value is 60 seconds and can be any value among 0 to 65535.

tx_period - It is the initialization value of the txWhen timer. The default value is 30 seconds and can be any integer value among 1 to 65535.

supp_timeout - The initialization value of the aWhile timer when timing out the supplicant. Its default value is 30 seconds and can be any integer value among 1 to 65535.

server_timeout - The initialization value of the aWhile timer when timing out the authentication server. Its default value is 30 seconds and can be any integer value among 1 to 65535.

max_req - The maximum number of times that the authentication PAE state machine will retransmit an EAP Request packet to the supplicant. Its default value is 2 and can be any integer number among 1 to 10.

reauth_period - It's a nonzero number of seconds, which is used to be the re-authentication timer. The default value is 3400.

enable_reauth - You can enable or disable the re-authentication mechanism for a specific port.

max_users - Specifies per port maximum number of users.

The range is 1 to 128.

The default value is 16.

Restrictions

Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the parameters that control the operation of the authenticator associated with a port:

```
DGS-3450:admin# config 802.1x auth_parameter ports 1:1-1:20 direction both
Command: config 802.1x auth_parameter ports 1:1-1:20 direction both

Success.

DGS-3450:admin#
```

config 802.1x auth_mode

Purpose	Used to configure 802.1X authentication mode.
Syntax	config 802.1x auth_mode [port_based mac_based]
Description	The config 802.1x auth_mode command configures the authentication mode.
Parameters	<i>port_based</i> - Configure the authentication as port based mode. <i>mac_based</i> - Configure the authentication as MAC based mode.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the authentication mode:

```
DGS-3450:admin# config 802.1x auth_mode port_based
Command: config 802.1x auth_mode port_based

Success.

DGS-3450:admin#
```

config 802.1x init

Purpose	Used to initialize the authentication state machine of some or all ports.
Syntax	config 802.1x init [port_based ports [< portlist all >] mac_based ports [< portlist > all] { mac_address < macaddr > }]
Description	The config 802.1x init command used to initialize the authentication state machine of some or all.
Parameters	<i>port_based</i> - Configure the authentication as port based mode. <i>mac_based</i> - Configure the authentication as MAC based mode. <i>portlist</i> - Specifies a range of ports to be configured. <i>all</i> - All ports. <i>mac_address</i> - MAC address of client.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To initialize the authentication state machine of some or all:

```
DGS-3450:admin# config 802.1x init port_based ports all
Command: config 802.1x init port_based ports all

Success.

DGS-3450:admin#
```

config 802.1x reauth

Purpose	Used to re-authenticate the device connected to the port.
Syntax	config 802.1x reauth [port_based ports [< portlist all >] mac_based ports [< portlist > all] { mac_address < macaddr > }]
Description	The config 802.1x reauth command re-authenticates the device connected to the port. During the re-authentication period, the port status remains authorized until failed re-authentication.
Parameters	<i>port_based</i> - Configure the authentication as port based mode. <i>mac_based</i> - Configure the authentication as MAC based mode. <i>portlist</i> - Specifies a range of ports to be configured. <i>all</i> - All ports. <i>mac_address</i> - MAC address of client.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To re-authenticate the device connected to the port:

```
DGS-3450:admin# config 802.1x reauth port_based ports all
Command: config 802.1x reauth port_based ports all

Success.

DGS-3450:admin#
```

create 802.1x guest_vlan

Purpose	Used to assign a static VLAN to be guest VLAN.
Syntax	create 802.1x guest_vlan { < vlan_name 32 > }
Description	The create 802.1x guest_vlan command will assign a static VLAN to be guest VLAN. The specific VLAN which assigned to guest VLAN must be existed. The specific VLAN which assigned to guest VLAN can't be deleting.
Parameters	<vlan_name 32> - Specify the static VLAN to be guest VLAN.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create a VLAN named "guestVLAN" as 802.1X guest VLAN:

```
DGS-3450:admin# create 802.1x guest_vlan guestVLAN
Command: create 802.1x guest_vlan guestVLAN

Success.

DGS-3450:admin#
```

delete 802.1x guest_vlan

Purpose	Used to delete guest VLAN configuration.
Syntax	delete 802.1x guest_vlan { < vlan_name 32 > }
Description	The delete 802.1x guest_vlan command will delete guest VLAN setting, but not delete the static VLAN. All ports which enabled guest VLAN will remove to original VLAN after deleted guest VLAN.
Parameters	<vlan_name 32> - Specify the static VLAN to be guest VLAN.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete the guest VLAN named "guestVLAN":

```
DGS-3450:admin# delete 802.1x guest_vlan guestVLAN
Command: delete 802.1x guest_vlan guestVLAN

Success.

DGS-3450:admin#
```

config 802.1x guest_vlan

Purpose	Used to configure guest VLAN settings.
Syntax	config 802.1x guest_vlan ports [< portlist > all] state [enable disable]
Description	The config 802.1x guest_vlan command configures guest VLAN setting. If the specific port state is changed from enabled state to disable state, this port will move to its original VLAN.
Parameters	<i>ports</i> - A range of ports enable or disable guest VLAN function. <i>state</i> - Specify the guest VLAN port state of the configured ports. <i>enable</i> - join the guest VLAN. <i>disable</i> - remove from guest VLAN.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

Enable on port 1 – 8 to configure 802.1X guest VLAN:

```
DGS-3450:admin# config 802.1x guest_vlan ports 1-8 state enable
Command: config 802.1x guest_vlan ports 1-8 state enable

Warning! GVRP of the ports were disabled!

Success.

DGS-3450:admin#
```

show 802.1x guest_vlan

Purpose	Used to show guest VLAN setting.
Syntax	show 802.1x guest_vlan
Description	The show guest_vlan command allows you to show the information of guest VLANs.
Parameters	None.
Restrictions	None.

Example usage:

To show 802.1X guest VLAN on the switch:

```
DGS-3450:admin# show 802.1x guest_vlan
Command: show 802.1x guest_vlan

Guest VLAN Setting
-----
Guest VLAN   : guest
Enable Guest VLAN Ports      : 1-10

DGS-3450:admin#
```

config radius add

Purpose	Use to add a new RADIUS server. The server with lower index has higher authenticative priority.
---------	---

config radius add

Syntax	config radius add < server_index 1-3 > [< server_ip > < ipv6addr >] key < passwd 32 > [default { auth_port < udp_port_number 1-65535 > acct_port < udp_port_number 1-65535 > timeout < int 1-255 > retransmit < int 1-20 > } (1)]
Description	The “config radius add” command adds a new RADIUS server.
Parameters	<p><i>server_index</i> - RADIUS server index.</p> <p><i>server_ip</i> - The IP address of the RADIUS server.</p> <p><i>ipv6addr</i> - The IPv6 address of the RADIUS server.</p> <p><i>passwd</i> - The key pre-negotiated between switch and the RADIUS server. It is used to encrypt user’s authentication data before being transmitted over internet. The maximum length of the key is 32.</p> <p><i>default</i> - Sets the authentication UDP port number to 1812 accounting UDP port number to 1813, timeout to 5 seconds and retransmit to 2.</p> <p><i>auth_port</i> - Specifies the UDP port number which is used to transmit RADIUS authentication data between the switch and the RADIUS server. The range is 1 to 65535.</p> <p><i>acct_port</i> - Specifies the UDP port number which is used to transmit RADIUS accounting statistics between the switch and the RADIUS server. The range is 1 to 65535.</p> <p><i>timeout</i> - The time in second for waiting server reply. Default value is 5 seconds.</p> <p><i>retransmit</i> - The count for re-transmitting. Default value is 2.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To add a new RADIUS server:

```
DGS-3450:admin# config radius add 1 10.48.74.121 key dlink default
Command: config radius add 1 10.48.74.121 key dlink default

Success.

DGS-3450:admin#
```

config radius delete

Purpose	Used to delete a RADIUS server.
Syntax	config radius delete < server_index 1-3 >
Description	The config radius delete command delete a RADIUS server.
Parameters	<i>server_index</i> - RADIUS server index.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete a radius server:

```
DGS-3450:admin# config radius delete 1
Command: config radius delete 1

Success.

DGS-3450:admin#
```


config radius

Purpose	Used to configure a RADIUS server.
Syntax	config radius <server_index 1-3> { ipaddress [<server_ip> <ipv6addr>] key <passwd 32> auth_port [<udp_port_number> default] acct_port [<udp_port_number> default] timeout [<int 1-255> default] retransmit [<int 1-20> default] } (1)
Description	The config radius command configures a RADIUS server.
Parameters	<p><i>server_index</i> - RADIUS server index.</p> <p><i>server_ip</i> - The IP address of the RADIUS server.</p> <p><i>ipv6addr</i> - The IPv6 address of the RADIUS server</p> <p><i>passwd</i> - The key pre-negotiated between switch and RADIUS server. It is used to encrypt user's authentication data before being transmitted over internet. The maximum length of the key is 32.</p> <p><i>auth_port</i> - Specifies the UDP port number which is used to transmit RADIUS authentication data between the switch and the RADIUS server. The range is 1 to 65535. Default value is 1812.</p> <p><i>acct_port</i> - Specifies the UDP port number which is used to transmit RADIUS accounting statistics between the switch and the RADIUS server. The range is 1 to 65535. Default value is 1813.</p> <p><i>timeout</i> - The time in second for waiting server reply. Default value is 5 seconds.</p> <p><i>retransmit</i> - The count for re-transmitting. Default value is 2.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure a radius server:

```
DGS-3450:admin# config radius server 1 auth_port 60
Command: config radius server 1 auth_port 60

Success.

DGS-3450:admin#
```

show radius

Purpose	Used to display RADIUS server configurations.
Syntax	show radius
Description	The show radius command displays RADIUS server configurations.
Parameters	None.
Restrictions	None.

Example usage:

To display RADIUS server configurations:

```

DGS-3450:admin# show radius
Command: show radius

Index 1
IP Address       : fe80:fec0:56ab:34b0:20b2:6aff:fe6f:7ec6
Auth-Port       : 1812
Acct-Port       : 1513
Timeout         : 5
Retransmit      : 2
Key             : adfdslkfjefiefdkgjdassdwtgjk6y1w

Index 2
IP Address       : 172.18.211.71
Auth-Port       : 1812
Acct-Port       : 1813
Retransmit      : 2
Key             : 1234567

Index 3
IP Address       : 172.18.211.108
Auth-Port       : 1812
Acct-Port       : 1813
Retransmit      : 2
Key             : adfdslkfjefiefdkgjdassdwtgjk6y1w

Total Entries: 3

DGS-3450:admin#

```

show auth_statistics

Purpose	Use to display information of authenticator statistics.
Syntax	show auth_statistics {ports [<portlist> all]}
Description	The show auth_statistics command displays information of authenticator statistics.
Parameters	<i>portlist</i> - Specifies a range of ports to be displayed. <i>all</i> - Specifies that all the ports will be used for the configuration.
Restrictions	None.

Example usage:

To display authenticator statistics information for port 1:

```

DGS-3450:admin# show auth_statistics ports 1
Command: show auth_statistics ports 1

Port number : 1

EapolFramesRx                0
EapolFramesTx                6
EapolStartFramesRx          0
EapolReqIdFramesTx          6
EapolLogoffFramesRx         0
EapolReqFramesTx            0
EapolRespIdFramesRx         0
EapolRespFramesRx           0
InvalidEapolFramesRx        0
EapLengthErrorFramesRx      0
LastEapolFrameVersion        0
LastEapolFrameSource         00-00-00-00-00-00

DGS-3450:admin#

```

show auth_diagnostics

Purpose	Used to display information of authenticator diagnostics.
Syntax	show auth_diagnostics {ports [<portlist> all]}
Description	The show auth_diagnostics command displays information of authenticator diagnostics.
Parameters	<i>portlist</i> - Specifies a range of ports to be displayed. <i>all</i> - Specifies that all the ports will be used for the configuration.
Restrictions	None.

Example usage:

To display authenticator diagnostics information for port 1:

```

DGS-3450:admin# show auth_diagnostics ports 1
Command: show auth_diagnostics ports 1

Port number : 1

EntersConnecting                20
EapLogoffsWhileConnecting      0
EntersAuthenticating           0
SuccessWhileAuthenticating     0
TimeoutsWhileAuthenticating    0
FailWhileAuthenticating        0
ReauthsWhileAuthenticating     0
EapStartsWhileAuthenticating   0
EapLogoffWhileAuthenticating   0
ReauthsWhileAuthenticated      0
EapStartsWhileAuthenticated    0
EapLogoffWhileAuthenticated    0
BackendResponses               0
BackendAccessChallenges        0
BackendOtherRequestsToSupplicant 0
BackendNonNakResponsesFromSupplicant 0
BackendAuthSuccesses           0
BackendAuthFails               0

DGS-3450:admin#

```

show auth_session_statistics

Purpose	Use to display information of authenticator session statistics.
Syntax	show auth_session_statistics {ports [<portlist> all]}
Description	The show auth_session_statistics command displays information of authenticator session statistics.
Parameters	<i>portlist</i> - Specifies a range of ports to be displayed. <i>all</i> - Specifies that all the ports will be used for the configuration.
Restrictions	None.

Example usage:

To display authenticator session statistics information for port 1:

```
DGS-3450:admin# show auth_session_statistics ports 1
Command: show auth_session_statistics ports 1

Port number : 1

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

DGS-3450:admin#
```

show auth_client

Purpose	Use to display information of RADIUS authentication client.
Syntax	show auth_client
Description	The show auth_client command displays information of RADIUS authentication client.
Parameters	None.
Restrictions	None.

Example usage:

To display authentication client information:

```

DGS-3450:admin# show auth_client
Command: show auth_client

radiusAuthClient ==>
radiusAuthClientInvalidServerAddresses      0
radiusAuthClientIdentifier                   D-Link

radiusAuthServerEntry ==>
radiusAuthServerIndex :1

radiusAuthServerAddress                      0.0.0.0
radiusAuthClientServerPortNumber            0
radiusAuthClientRoundTripTime               0
radiusAuthClientAccessRequests              0
radiusAuthClientAccessRetransmissions       0
radiusAuthClientAccessAccepts               0
radiusAuthClientAccessRejects              0
radiusAuthClientAccessChallenges            0
radiusAuthClientMalformedAccessResponses    0
radiusAuthClientBadAuthenticators           0
radiusAuthClientPendingRequests             0
radiusAuthClientTimeouts                    0
radiusAuthClientUnknownTypes                0
radiusAuthClientPacketsDropped              0

DGS-3450:admin#

```

show acct_client

Purpose	Used to display information of RADIUS accounting client.
Syntax	show acct_client
Description	The show acct_client command displays information of RADIUS accounting client.
Parameters	None.
Restrictions	None.

Example usage:

To display information of RADIUS accounting client:

```

DGS-3450:admin# show acct_client
Command: show acct_client

radiusAcctClient ==>
radiusAcctClientInvalidServerAddresses      0
radiusAcctClientIdentifier                  D-Link

radiusAuthServerEntry ==>
radiusAccServerIndex : 1

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

DGS-3450:admin#
    
```

config accounting service

Purpose	Used to configure the state of the specified RADIUS accounting service.
Syntax	config accounting service [network shell system] state [enable disable]
Description	The config accounting service command is used to enable or disable the specified RADIUS accounting service.
Parameters	<p><i>network</i> - Accounting service for 802.1X port access control. By default, the service is disabled.</p> <p><i>shell</i> - Accounting service for shell events: When user logs on or out the switch (via the console, Telnet, or SSH) and timeout occurs, accounting information will be collected and sent to RADIUS server. By default, the service is disabled.</p> <p><i>system</i> - Accounting service for system events: reset, reboot. By default, the service is disabled.</p> <p><i>enable</i> - Enable the specified accounting service.</p> <p><i>disable</i> - Disable the specified accounting service.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

Enable it to configure accounting shell state:

```
DGS-3450:admin# config accounting service shell state enable
Command: config accounting service shell state enable

Success.

DGS-3450:admin#
```

show accounting service

Purpose	Used to show the status of RADIUS accounting services.
Syntax	show accounting service
Description	The show accounting service command displays the state for RADIUS accounting service.
Parameters	<i>portlist</i> - Specifies a range of ports to be configured.
Restrictions	None.

Example usage:

To show information of RADIUS accounting services:

```
DGS-3450:admin# show accounting service
Command: show accounting service

Accounting Service
-----
Network      : Enabled
Shell        : Enabled
System       : Enabled

DGS-3450:admin#
```


ACCESS AUTHENTICATION CONTROL COMMANDS

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

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

- TACACS (Terminal Access Controller Access Control System) —Provides password checking and authentication, and notification of user actions for security purposes utilizing via one or more centralized TACACS servers, utilizing the UDP protocol for packet transmission.
- Extended TACACS (XTACACS) — An extension of the TACACS protocol with the ability to provide more types of authentication requests and more types of response codes than TACACS. This protocol also uses UDP to transmit packets.
- TACACS+ (Terminal Access Controller Access Control System plus) — Provides detailed access control for authentication for network devices. TACACS+ is facilitated through Authentication commands via one or more centralized servers. The TACACS+ protocol encrypts all traffic between the Switch and the TACACS+ daemon, using the TCP protocol to ensure reliable delivery.

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

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

- a. The server verifies the username and password, and the user is granted normal user privileges on the Switch.
- b. The server will not accept the username and password and the user is denied access to the Switch.
- c. The server doesn't respond to the verification query. At this point, the Switch receives the timeout from the server and then moves to the next method of verification configured in the method list.

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

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

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



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

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

Command	Parameters
enable password encryption	
disable password encryption	
create account	[admin operator user] <username 15>
config account	<username> {encrypt [plain_text sha_1] <password>}
show account	
delete account	<username>
enable authen_policy	
disable authen_policy	
show authen_policy	
create authen_login method_list_name	<string 15>
config authen_login	[default method_list_name <string 15>] method {tacacs xtacacs tacacs+ radius server_group <string 15> local none}
delete authen_login method_list_name	<string 15>
show authen_login	[default method_list_name <string 15> all]
create authen_enable method_list_name	<string 15>
config authen_enable	[default method_list_name <string 15>] method {tacacs xtacacs tacacs+ radius server_group <string 15> local _enable none}
delete authen_enable method_list_name	<string 15>
show authen_enable	[default method_list_name <string 15> all]
config authen application	[console telnet ssh http all] [login enable] [default method_list_name <string 15>]
show authen application	
create authen server_group	<string 15>
config authen server_group	[tacacs xtacacs tacacs+ radius <string 15>] [add delete] server_host <ipaddr> protocol [tacacs xtacacs tacacs+ radius]
delete authen server_group	<string 15>
show authen server_group	{<string 15>}
create authen server_host	<ipaddr> protocol [tacacs xtacacs tacacs+ radius] { port <int 1-65535> key [<key_string 254> none] timeout <int 1-255> retransmit <int 1-20> }
config authen server_host	<ipaddr> protocol [tacacs xtacacs tacacs+ radius] { port <int 1-65535> key [<key_string 254> none] timeout <int 1-255> retransmit <int 1-20> }
delete authen server_host	<ipaddr> protocol [tacacs xtacacs tacacs+ radius]
show authen server_host	
config authen parameter response_timeout	<int 0-255>
config authen parameter attempt	<int 1-255>
show authen parameter	
enable admin	

Command	Parameters
config admin local_enable	

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

enable password encryption

Purpose	This command is used to enable password encryption.
Syntax	enable password encryption
Description	<p>The user account configuration information will be stored in the configuration file, and can be applied to the system later.</p> <p>If password encryption is enabled, the passwords will be in encrypted form.</p> <p>When password encryption is disabled, if the user specifies the password in plain text form, the password will be in plain text form. However, if the user specifies the password in encrypted form, or if the password has been converted to encrypted form by the last enable password encryption command, the password will always be in the encrypted form and can not be reverted back to plaintext.</p>
Parameters	None
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable password encryption:

```
DGS-3450:admin# enable password encryption
Command: enable password encryption

DGS-3450:admin#
```

disable password encryption

Purpose	This command is used to disable password encryption.
Syntax	disable password encryption
Description	<p>The user account configuration information will be stored in the configuration file, and can be applied to the system later.</p> <p>If password encryption is enabled, the passwords will be in encrypted form.</p> <p>When password encryption is disabled, if the user specifies the password in plain text form, the password will be in plain text form. However, if the user specifies the password in encrypted form, or if the password has been converted to encrypted form by the last enable password encryption command, the password will always be in the encrypted form and can not be reverted back to plaintext.</p>
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable password encryption:

```
DGS-3450:admin# disable password encryption
Command: disable password encryption

DGS-3450:admin#
```

create account

Purpose	This command is used to create user accounts.
Syntax	create account [admin operator user] <username 15>
Description	The create account command is used to create user accounts. A username can be between 1 and 15 characters. The password is between 0 and 15 characters and is case sensitive. The total number of accounts supported by the Switch (including admin and user level accounts) is 8.
Parameters	<p><i>admin</i> - Specify an administrator level account. The administrator is the highest privilege level in the Switch.</p> <p><i>operator</i> - Specify an operator level account.</p> <p><i>user</i> - Specify a user level account.</p> <p><i><username 15></i> - The user name, which must be a minimum of 1 character and a maximum of 15 characters.</p>
Restrictions	Only Administrator can issue this command.

Example usage:

To create the admin-level user "alpha":

```
DGS-3450:admin# create account admin alpha
Command: create account admin alpha

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

Success.

DGS-3450:admin#
```

config account

Purpose	This command is used to configure user accounts.
Syntax	config account <username> {encrypt [plain_text sha_1] <password>}
Description	<p>When the password information is not specified in the command, the system will prompt the user to input the password interactively. In this case, the user can only input a plain text password.</p> <p>If the user specifies a password in the command, the user can select to input the password in plain text form or in encrypted form. The encryption algorithm is based on SHA-1.</p>
Parameters	<p><i><username></i> - Specify the name of the account. The account must already be defined.</p> <p><i>plain_text</i> - Specify the password in plain text form.</p> <p><i>sha_1</i> - Specify the password in SHA-1 encrypted form.</p> <p><i>password</i> - The password for the user account. The length of a password in plain-text form and encrypted form are different. For a plain-text form password, the password must be a minimum of 0 characters and a maximum of 15 characters. For an encrypted form password, the length is fixed to 35 bytes long. The password is case-sensitive.</p>
Restrictions	Only Administrator can issue this command.

Example usage:

To configure the user password of the “alpha” account:

```
DGS-3450:admin# config account alpha
Command: config account alpha

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

Success.

DGS-3450:admin#
```

show account

Purpose	This command is used to display the user accounts that have been created on the Switch.
Syntax	show account
Description	The show account command displays the user accounts that have been created on the Switch.
Parameters	None
Restrictions	Only Administrator can issue this command.

Example usage:

To display the user accounts that have been created on the Switch:

```
DGS-3450:admin# show account
Command: show account

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

Total Entries : 2

DGS-3450:admin#
```

delete account

Purpose	This command is used to delete an existing account.
Syntax	delete account <username>
Description	The delete account command deletes an existing account.
Parameters	<username> - Specify the name of the user that will be deleted.
Restrictions	Only Administrator can issue this command.

Example usage:

To delete the user account “System”:

```
DGS-3450:admin# delete account System
Command: delete account System

Success.

DGS-3450:admin#
```

enable authen_policy

Purpose	This command is used to enable the system access authentication policy.
Syntax	enable authen_policy
Description	Enable system access authentication policy- When authentication is enabled, the device will adopt the login authentication method list to authenticate the user attempting to log in, and adopt the enable authentication method list to authenticate the enable password for promoting the user's privilege to Admin level.
Parameters	None.
Restrictions	Only Administrator can issue this command.

Example usage:

To enable the system access authentication policy:

```
DGS-3450:admin# enable authen_policy
Command: enable authen_policy

Success.

DGS-3450:admin#
```

disable authen_policy

Purpose	This command is used to disable the system access authentication policy.
Syntax	disable authen_policy
Description	Disable system access authentication policy- When authentication is disabled, the device will adopt the local user account database to authenticate the user attempting to log in, and adopt the local enable password to authenticate the enable password for promoting the user's privilege to Admin level.
Parameters	None.
Restrictions	Only Administrator can issue this command.

Example usage:

To disable the system access authentication policy:

```
DGS-3450:admin# disable authen_policy
Command: disable authen_policy

Success.

DGS-3450:admin#
```

show authen_policy

Purpose	This command is used to display if the system access authentication policy is enabled or disabled.
Syntax	show authen_policy
Description	Displays if the system access authentication policy is enabled or disabled.
Parameters	None.
Restrictions	Only Administrator can issue this command.

Example usage:

To display if the system access authentication policy is enabled or disabled:

```
DGS-3450:admin# show authen_policy
Command: show authen_policy

Authentication Policy : Enabled

DGS-3450:admin#
```

create authen_login method_list_name

Purpose	This command is used to create a user-defined method list of authentication methods for users attempting to log in to the Switch.
Syntax	create authen_login method_list_name <string 15>
Description	Creates a user-defined method list of authentication methods for users attempting to log into the Switch. The maximum number of supported login method lists is 8.
Parameters	<string 15> - The user-defined method list name
Restrictions	Only Administrator can issue this command.

Example usage:

To create a user-defined method list called "login_list_1" for users attempting to log in to the Switch:

```
DGS-3450:admin# create authen_login method_list_name login_list_1
Command: create authen_login method_list_name login_list_1

Success.

DGS-3450:admin#
```

config authen_login

Purpose	This command is used to configure a user-defined or default method list of authentication methods for users attempting to log in to the Switch.
Syntax	config authen_login [default method_list_name <string 15>] method {tacacs xtacacs tacacs+ radius server_group <string 15> local none}
Description	Configures a user-defined or default method list of authentication methods for users attempting to log in to the Switch. The method sequence will affect the authentication result. For example, if the user specifies tacacs+ first, then tacacs and local, when the user tries to log in, the authentication request will be sent to the first server host in the tacacs+ built-in server group. If the first server host in the tacacs+ group is missing, the authentication request will be sent to the second server host in the tacacs+ group, and so on. If all server

config authen_login

hosts in the tacacs+ group are missing, the authentication request will be sent to the first server host in the tacacs group. If all server hosts in the tacacs group are missing, the local account database in the device will be used to authenticate the user. When a user logs in to the device successfully, using either the tacacs/xtacacs/tacacs+/radius built-in, user-defined server groups methods, or none, only the “user” privilege level will be assigned. If the user wants to access admin privilege level, the user must use the “enable admin” command to promote the privilege level. However, when the local method is used, the privilege level will depend on the account privilege level stored in the local device.

Parameters

default - Specify the default method list of authentication methods.
method_list_name - Specify the user-defined method list of authentication methods.
tacacs - Specify authentication by the built-in server group “tacacs”.
xtacacs - Specify authentication by the built-in server group “xtacacs”.
tacacs+ - Specify authentication by the built-in server group “tacacs+”.
radius - Specify authentication by the built-in server group “radius”.
server_group - Specify authentication by the user-defined server group.
local - Specify authentication by the local user account database in the device.
none - Specify no authentication.

Restrictions

Only Administrator can issue this command.

Example usage:

To configure a user-defined method list called “login_list_1”, that specifies a sequence of the built-in “tacacs+” server group, followed by the “tacacs” server group, and finally the local account database for users attempting to log in to the Switch:

```
DGS-3450:admin# config authen_login method_list_name login_list_1 method tacacs+ tacacs local
Command: config authen_login method_list_name login_list_1 method tacacs+ tacacs local
Success.
DGS-3450:admin#
```

delete authen_login method_list_name

Purpose

This command is used to delete a user-defined method list of authentication methods for users logging into the Switch.

Syntax

delete authen_login method_list_name <string 15>

Description

Deletes a user-defined method list of authentication methods for users attempting to log in to the Switch.

Parameters

<string 15> - The user-defined method list name.

Restrictions

Only Administrator can issue this command.

Example usage:

To delete the user-defined method list called “login_list_1” for users attempting to log in to the Switch:

```
DGS-3450:admin# delete authen_login method_list_name login_list_1
Command: delete authen_login method_list_name login_list_1

Success.

DGS-3450:admin#
```

show authen_login

Purpose	This command is used to display the method list of authentication methods that will be used for users attempting to log in to the Switch.
Syntax	show authen_login [default method_list_name <string 15> all]
Description	Displays the method list of authentication methods that will be used for users attempting to log in to the Switch.
Parameters	<i>default</i> - Displays the default user-defined method list for users logging into the Switch. <i>method_list_name</i> - Displays the specific user-defined method list for users logging into the Switch. <i>all</i> - Displays all the method lists for users attempting to log in to the Switch.
Restrictions	Only Administrator can issue this command.

Example usage:

To display the user-defined method list called "login_list_1" for users attempting to log in to the Switch:

```
DGS-3450:admin# show authen_login method_list_name login_list_1
Command: show authen_login method_list_name login_list_1

Method List Name  Priority  Method Name      Comment
-----
login_list_1     1        tacacs+          Built-in Group
                  2        tacacs           Built-in Group
                  3        mix_1            User-defined Group
                  4        local            Keyword

DGS-3450:admin#
```

create authen_enable method_list_name

Purpose	This command is used to create a user-defined method list of authentication methods for promoting a user's privilege to Admin level.
Syntax	create authen_enable method_list_name <string 15>
Description	Creates a user-defined method list of authentication methods for promoting a user's privilege to Admin level. The maximum number of supported enable method lists is 8.
Parameters	<string 15> - The user-defined method list name
Restrictions	Only Administrator can issue this command.

Example usage:

To create a user-defined method list called "enable_list_1" for promoting a user's privilege to Admin level:

```
DGS-3450:admin# create authen_enable method_list_name enable_list_1
Command: create authen_enable method_list_name enable_list_1

Success.

DGS-3450:admin#
```

config authen_enable

Purpose	This command is used to configure a user-defined or default method list of authentication methods for promoting a user's privilege to Admin level.
Syntax	config authen_enable [default method_list_name <string 15>] method {tacacs xtacacs tacacs+ radius server_group <string 15> local_enable none}
Description	Configures a user-defined or default method list of authentication methods for promoting a user's privilege to Admin level. The sequence of methods will affect the authentication result. For example, if the sequence is tacacs+ first, followed by tacacs and local_enable, when a user tries to login, the authentication request will be sent to the first server host in the tacacs+ built-in server group. If the first server host in the tacacs+ group is missing, the authentication request will be sent to the second server host in the tacacs+ group, and so on. If all server hosts in the tacacs+ group are missing, the authentication request will be sent to the first server host in the tacacs group. If all server hosts in the tacacs group are missing, the local enable password in the device will be used to authenticate the user's password. The local enable password in the device can be configured using the "config admin local_password" CLI command.
Parameters	<p><i>default</i> - Specify the default method list of authentication methods.</p> <p><i>method_list_name</i> - Specify the user-defined method list of authentication methods.</p> <p><i>tacacs</i> - Specify authentication by the built-in server group "tacacs".</p> <p><i>xtacacs</i> - Specify authentication by the built-in server group "xtacacs".</p> <p><i>tacacs+</i> - Specify authentication by the built-in server group "tacacs+".</p> <p><i>radius</i> - Specify authentication by the built-in server group "radius".</p> <p><i>server_group</i> - Specify authentication by the user-defined server group.</p> <p><i>local_enable</i> - Specify authentication by the local enable password in the device.</p> <p><i>none</i> - Specify no authentication.</p>
Restrictions	Only Administrator can issue this command.

Example usage:

To configure a user-defined method list called "method_list_name" that will be used to promote a user's privilege to Admin level:

```
DGS-3450:admin# config authen_enable method_list_name enable_list_1 method tacacs+ tacacs local_enable
Command: config authen_enable method_list_name enable_list_1 method tacacs+ tacacs local_enable

Success.

DGS-3450:admin#
```

delete authen_enable method_list_name

Purpose	This command is used to delete a user-defined method list of authentication methods for promoting a user's privilege to Admin level.
Syntax	delete authen_enable method_list_name <string 15>

delete authen_enable method_list_name

Description	Deletes a user-defined method list of authentication methods for promoting a user's privilege to Admin level.
Parameters	<string 15> - The user-defined method list name
Restrictions	Only Administrator can issue this command.

Example usage:

To delete the user-defined method list called "enable_list_1", that is used to promote a user's privilege to Admin level:

```
DGS-3450:admin# delete authen_enable method_list_name enable_list_1
Command: delete authen_enable method_list_name enable_list_1

Success.

DGS-3450:admin#
```

show authen_enable

Purpose	This command is used to display the method list of authentication methods for promoting a user's privilege to Admin level.
Syntax	show authen_enable [default method_list_name <string 15> all]
Description	Displays the method list of authentication methods used for promoting a user's privilege to Admin level.
Parameters	<i>default</i> - Display the default user-defined method list for promoting a user's privilege to Admin level. <i>method_list_name</i> - Display the specific user-defined method list for promoting a user's privilege to Admin level. <i>all</i> - Display all the method lists for promoting a user's privilege to Admin level.
Restrictions	Only Administrator can issue this command.

Example usage:

To display all the method lists that are used for promoting a user's privilege to Admin level:

```
DGS-3450:admin# show authen_enable all
Command: show authen_enable all

Method List Name  Priority  Method Name      Comment
-----
enable_list_1    1        tacacs+          Built-in Group
                  2        tacacs           Built-in Group
                  3        mix_1            User-defined Group
                  4        local            Keyword

enable_list_2    1        tacacs+          Built-in Group
                  2        radius           Built-in Group

Total Entries : 2

DGS-3450:admin#
```

config authen application

Purpose	This command is used to configure login or enable method lists for all or the specified applications.
Syntax	config authen application [console telnet ssh http all] [login enable] [default method_list_name <string 15>]
Description	Configures login or enable method lists for all or the specified applications.
Parameters	<p><i>console</i> - Application: Console.</p> <p><i>telnet</i> - Application: Telnet.</p> <p><i>ssh</i> - Application: SSH.</p> <p><i>http</i> - Application: Web.</p> <p><i>all</i> - Application: Console, Telnet, SSH, and Web.</p> <p><i>login</i> - Specify the method list of authentication methods for user's attempting to log in.</p> <p><i>enable</i> - Specify the method list of authentication methods for promoting a user's privilege to Admin level.</p> <p><i>default</i> - Specify the default method list.</p> <p><i>method_list_name</i> - Specify the user-defined method list name.</p>
Restrictions	Only Administrator can issue this command.

Example usage:

To configure a login method list for Telnet called "login_list_1":

```
DGS-3450:admin# config authen application telnet login method_list_name login_list_1
Command: config authen application telnet login method_list_name login_list_1

Success.

DGS-3450:admin#
```

show authen application

Purpose	This command is used to display the login/enable method list for all applications.
Syntax	show authen application
Description	Displays the login/enable method list for all applications.
Parameters	None.
Restrictions	Only Administrator can issue this command.

Example usage:

To display the login/enable method lists for all applications:

```
DGS-3450:admin# show authen application
Command: show authen application

Application   Login Method List   Enable Method List
-----
Console      default             default
Telnet       login_list_1        default
HTTP         default             default

DGS-3450:admin#
```

create authen server_group

Purpose	This command is used to create a user-defined authentication server group.
Syntax	create authen server_group <string 15>
Description	Creates a user-defined authentication server group. The maximum number of supported server groups, including the built-in server groups, is 8. Each group can have a maximum of 8 server hosts..
Parameters	<i><string 15></i> - Specify the user-defined server group name.
Restrictions	Only Administrator can issue this command.

Example usage:

To create a user-defined authentication server group called "mix_1":

```
DGS-3450:admin# create authen server_group mix_1
Command: create authen server_group mix_1

Success.

DGS-3450:admin#
```

config authen server_group

Purpose	This command is used to add or remove an authentication server host to or from the specified server group.
Syntax	config authen server_group [tacacs xtacacs tacacs+ radius <string 15>] [add delete] server_host <ipaddr> protocol [tacacs xtacacs tacacs+ radius]
Description	Adds or removes an authentication server host to or from the specified server group. The built-in "tacacs", "xtacacs", "tacacs+", and "radius" server groups only accept server hosts with the same protocol, but a user-defined server group can accept server hosts with different protocols. The server host must be created first by using the "create authen server_host" CLI command.
Parameters	<p><i>server_group tacacs</i> - Specify the built-in server group "tacacs".</p> <p><i>server_group xtacacs</i> - Specify the built-in server group "xtacacs".</p> <p><i>server_group tacacs+</i> - Specify the built-in server group "tacacs+".</p> <p><i>server_group radius</i> - Specify the built-in server group "radius".</p> <p><i>server_group</i> - Specify a user-defined server group.</p> <p><i>add</i> - Add a server host to a server group.</p> <p><i>delete</i> - Remove a server host from a server group.</p> <p><i>server_host</i> - Specify the server host's IP address.</p> <p><i>protocol tacacs</i> - Specify TACACS for the server host's authentication protocol</p> <p><i>protocol xtacacs</i> - Specify XTACACS for the server host's authentication protocol</p> <p><i>protocol tacacs+</i> - Specify TACACS+ for the server host's authentication protocol</p> <p><i>protocol radius</i> - Specify RADIUS for the server host's authentication protocol</p>
Restrictions	Only Administrator can issue this command.

Example usage:

To add an authentication server host with an IP address of 10.1.1.222 to server group "mix_1", specifying the TACACS+ protocol:

```
DGS-3450:admin# config authen server_group mix_1 add server_host 10.1.1.222 protocol
tacacs+
Command: config authen server_group mix_1 add server_host 10.1.1.222 protocol tacacs+

Success.

DGS-3450:admin#
```

delete authen server_group

Purpose	This command is used to delete a user-defined authentication server group.
Syntax	delete authen server_group <string 15>
Description	Deletes a user-defined authentication server group.
Parameters	<string 15> - Specify the user-defined server group name that will be deleted.
Restrictions	Only Administrator can issue this command.

Example usage:

To delete a user-defined authentication server group called "mix_1":

```
DGS-3450:admin# delete authen server_group mix_1
Command: delete authen server_group mix_1

Success.

DGS-3450:admin#
```

show authen server_group

Purpose	This command is used to display the authentication server groups.
Syntax	show authen server_group {<string 15>}
Description	Displays the authentication server groups.
Parameters	<string 15> - Specify the built-in or user-defined server group name to display.
Restrictions	Only Administrator can issue this command.

Example usage:

To display all authentication server groups:

```
DGS-3450:admin# show authen server_group
```

```
Command: show authen server_group
```

```
Server Group : mix_1
```

Group Name	IP Address	Protocol
-----	-----	-----
mix_1	10.1.1.222	TACACS+
	10.1.1.223	TACACS
radius	10.1.1.224	RADIUS
tacacs	10.1.1.225	TACACS
tacacs+	10.1.1.226	TACACS+
xtacacs	10.1.1.227	XTACACS

```
Total Entries : 5
```

```
DGS-3450:admin#
```

create authen server_host

Purpose	This command is used to create an authentication server host.
Syntax	create authen server_host <ipaddr> protocol [tacacs xtacacs tacacs+ radius] { port <int 1-65535> key [<key_string 254> none] timeout <int 1-255> retransmit <int 1-20> }
Description	Creates an authentication server host. When an authentication server host is created, the IP address and protocol are the index. This means that more than one authentication protocol service can be run on the same physical host. The maximum number of supported server hosts is 16.
Parameters	<p><i>server_host</i> - Specify the server host's IP address.</p> <p><i>protocol tacacs</i> - Specify that the server host's authentication protocol will be TACACS.</p> <p><i>protocol xtacacs</i> - Specify that the server host's authentication protocol will be XTACACS.</p> <p><i>protocol tacacs+</i> - Specify that the server host's authentication protocol will be TACACS+.</p> <p><i>protocol radius</i> - Specify that the server host's authentication protocol will be RADIUS.</p> <p><i>port</i> - The port number of the authentication protocol for the server host. Default value for TACACS/XTACACS/TACACS+ is 49. Default value for RADIUS is 1812.</p> <p><i>key</i> - The key for TACACS+ and RADIUS authentication. If the value is null, no encryption will apply. This value is meaningless for TACACS and XTACACS.</p> <p><i>none</i> - No encryption for TACACS+ and RADIUS authentication. This value is meaningless for TACACS and XTACACS.</p> <p><i>timeout</i> - The time in seconds to wait for the server reply. Default value is 5 seconds.</p> <p><i>retransmit</i> - The count for re-transmissions. This value is meaningless for TACACS+. Default value is 2.</p>
Restrictions	Only Administrator can issue this command.

Example usage:

To create a TACACS+ authentication server host, specifying a listening port number of 15555 and a timeout value of 10 seconds:


```
DGS-3450:admin# reate authen server_host 10.1.1.222 protocol tacacs+ port 15555 timeout 10
Command: create authen server_host 10.1.1.222 protocol tacacs+ port 15555 timeout 10

Success.

DGS-3450:admin#
```

config authen server_host

Purpose	This command is used to configure an authentication server host.
Syntax	config authen server_host <ipaddr> protocol [tacacs xtacacs tacacs+ radius] { port <int 1-65535> key [<key_string 254> none] timeout <int 1-255> retransmit <int 1-20> }
Description	Configures an authentication server host.
Parameters	<p><i>server_host</i> - Specify the server host's IP address.</p> <p><i>protocol tacacs</i> - Specify that the server host's authentication protocol will be TACACS.</p> <p><i>protocol xtacacs</i> - Specify that the server host's authentication protocol will be XTACACS.</p> <p><i>protocol tacacs+</i> - Specify that the server host's authentication protocol will be TACACS+.</p> <p><i>protocol radius</i> - Specify that the server host's authentication protocol will be RADIUS.</p> <p><i>port</i> - The port number of the authentication protocol for the server host. Default value for TACACS/XTACACS/TACACS+ is 49. Default value for RADIUS is 1812.</p> <p><i>key</i> - The key for TACACS+ and RADIUS authentication. If the value is null, no encryption will apply. This value is meaningless for TACACS and XTACACS.</p> <p><i>none</i> - No encryption for TACACS+ and RADIUS authentication. This value is meaningless for TACACS and XTACACS.</p> <p><i>timeout</i> - The time in seconds for waiting for the server reply. Default value is 5 seconds.</p> <p><i>retransmit</i> - The count for re-transmissions. This value is meaningless for TACACS+. Default value is 2.</p>
Restrictions	Only Administrator can issue this command.

Example usage:

To configure the TACACS+ authentication server host with an IP address of 10.1.1.222 to have the key value "This is a secret":

```
DGS-3450:admin# config authen server_host 10.1.1.222 protocol tacacs+ key "This is a secret"
Command: config authen server_host 10.1.1.222 protocol tacacs+ key "This is a secret"

Success.

DGS-3450:admin#
```

delete authen server_host

Purpose	This command is used to delete an authentication server host.
Syntax	delete authen server_host <ipaddr> protocol [tacacs xtacacs tacacs+ radius]
Description	Deletes an authentication server host.
Parameters	<p><i>server_host</i> - Specify the server host's IP address.</p> <p><i>protocol tacacs</i> - Specify that the server host's authentication protocol is TACACS.</p>

delete authen server_host

protocol xtacacs - Specify that the server host's authentication protocol is XTACACS.
protocol tacacs+ - Specify that the server host's authentication protocol is TACACS+.
protocol radius - Specify that the server host's authentication protocol is RADIUS.

Restrictions Only Administrator can issue this command.

Example usage:

To delete an authentication server host, with an IP address of 10.1.1.222, that is running the TACACS+ protocol:

```
DGS-3450:admin# delete authen server_host 10.1.1.222 protocol tacacs+
Command: delete authen server_host 10.1.1.222 protocol tacacs+
```

Success.

```
DGS-3450:admin#
```

show authen server_host

Purpose	This command is used to display the authentication server hosts.
Syntax	show authen server_host
Description	Displays the authentication server hosts.
Parameters	None.
Restrictions	Only Administrator can issue this command.

Example usage:

To display all authentication server hosts:

```
DGS-3450:admin# show authen server_host
Command: show authen server_host
```

SRV IP Address	Protocol	Port	Timeout	Retransmit	Key
-----	-----	-----	-----	-----	-----
10.1.1.222	TACACS+	15555	10	No Use	This is a secret

Total Entries : 1

```
DGS-3450:admin#
```

config authen parameter response_timeout

Purpose	This command is used to configure the amount of time the Switch will wait for a user to authenticate through a console, Telnet, or SSH application.
Syntax	config authen parameter response_timeout <int 0-255>
Description	Configure the amount of time the Switch will wait for a user to authenticate through a console, Telnet, or SSH application.
Parameters	<i><int 0-255></i> - The amount time the Switch will wait for a user to authenticate through a console, Telnet, or SSH application. 0 means there is no time out. Default value is 30 seconds.
Restrictions	Only Administrator can issue this command.

Example usage:

To configure the amount of time the Switch will wait for a user to authenticate through a console, Telnet, or SSH application to 60 seconds:

```
DGS-3450:admin# config authen parameter response_timeout 60
Command: config authen parameter response_timeout 60

Success.

DGS-3450:admin#
```

config authen parameter attempt

Purpose	This command is used to configure the maximum number of attempts a user can try to login or promote the privilege on a console, Telnet, or SSH application.
Syntax	config authen parameter attempt <int 1-255>
Description	Used to configure the maximum number of attempts that a user can try to login or promote the privilege on a console, Telnet, or SSH application. If failed login attempts exceeds this number, the connection or access will be locked.
Parameters	<int 1-255> - Specify the maximum number of attempts that a user can try to login or promote the privilege on a console or telnet or SSH application. Default value is 3.
Restrictions	Only Administrator can issue this command.

Example usage:

To configure the maximum attempts for user's trying to login or promote the privilege to be 9:

```
DGS-3450:admin# config authen parameter attempt 9
Command: config authen parameter attempt 9

Success.

DGS-3450:admin#
```

show authen parameter

Purpose	This command is used to display the parameters of authentication.
Syntax	show authen parameter
Description	Displays the parameters of authentication.
Parameters	None.
Restrictions	Only Administrator can issue this command.

Example usage:

To display the parameters of authentication:

```
DGS-3450:admin# show authen parameter
Command: show authen parameter

Response timeout : 60 seconds
User attempts    : 9

DGS-3450:admin#
```

enable admin

Purpose	This command is used to enter the administrator level privilege
Syntax	enable admin
Description	<p>Promote the "user" privilege level to "admin" level. When the user enters this command, the authentication method tacacs, xtacacs, tacacs+, user-defined server groups, local_enable or none will be used to authenticate the user. Since TACACS, XTACACS and RADIUS do not support the "enable" function by their selves,, if the user wants to use either one of these three protocols to enable authentication, the user must create a special account on the server host first, which has a username of "enable", and then configure its password as the enable password to support the "enable" function.</p> <p>This command can not be used when the authentication policy is disabled.</p> <p>For switches with 3-levels of privilege, this command can be used by users with user level and operator level privileges to access the administrator privilege level.</p>
Parameters	None.
Restrictions	None.

Example usage:

To enable administrator level privileges:

```
DGS-3450:admin# enable admin
Password:*****

DGS-3450:admin#
```

config admin local_enable

Purpose	This command is used to configure the local enable password of the administrator level privilege.
Syntax	config admin local_enable
Description	<p>Configure the local enable password for the enable command. When the user chooses the "local_enable" method to promote the privilege level, the enable password of the local device is needed.</p> <p>When the password information is not specified in the command, the system will prompt the user to input the password interactively. In this case, the user can only input a plain text password. If the password is present in the command, the user can select to input the password in plain text or encrypted form. The encryption algorithm is based on SHA-1.</p>
Parameters	None.
Restrictions	Only Administrator can issue this command.

Example usage:

To configure the administrator password:

```
DGS-3450:admin# config admin local_enable
Command: config admin local_enable

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

DGS-3450:admin#
```

ACCESS CONTROL LIST (ACL) COMMANDS

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

Command	Parameters
create access_profile	[ethernet {vlan source_mac <macmask 000000000000-ffffffff> destination_mac <macmask 000000000000-ffffffff> 802.1p ethernet_type} ip {vlan source_ip_mask <netmask> destination_ip_mask <netmask> dscp [icmp {type code} igmp {type} tcp {src_port_mask <hex 0x0-0xffff> dst_port_mask <hex 0x0-0xffff> flag_mask [all {urg ack psh rst syn fin}]} udp {src_port_mask <hex 0x0-0xffff> dst_port_mask <hex 0x0-0xffff>} protocol_id_mask <hex 0x0-0xff> {user_define_mask <hex 0x0-0xffffffff>}}] packet_content_mask { offset_chunk_1 <value 0-31> <hex 0x0-0xffffffff> offset_chunk_2 <value 0-31> <hex 0x0-0xffffffff> offset_chunk_3 <value 0-31> <hex 0x0-0xffffffff> offset_chunk_4 <value 0-31> <hex 0x0-0xffffffff>} ipv6 {class flowlabel source_ipv6_mask <ipv6mask> destination_ipv6_mask <ipv6mask> [tcp {src_port_mask <hex 0x0-0xffff> dst_port_mask <hex 0x0-0xffff>} udp {src_port_mask <hex 0x0-0xffff> dst_port_mask <hex 0x0-0xffff>}]}] profile_id <value 1-6>
delete access_profile	[profile_id <value 1-6> all]
config access_profile	profile_id <value 1-6> [add access_id [auto_assign <value 1-128>] [ethernet {vlan <vlan_name 32> source_mac <macaddr 000000000000-ffffffff> destination_mac <macaddr 000000000000-ffffffff> 802.1p <value 0-7> ethernet_type <hex 0x0-0xffff>} port [<portlist> all] [permit {priority <value 0-7> {replace_priority} rx_rate [no_limit <value 1-156249>]} replace_dscp <value 0-63> counter [enable disable]} mirror {group_id <value 1-4>} deny] ip {vlan <vlan_name 32> source_ip <ipaddr> destination_ip <ipaddr> dscp <value 0-63> [icmp {type <value 0-255> code <value 0-255>} igmp {type <value 0-255>} tcp {src_port <value 0-65535> dst_port <value 0-65535> urg ack psh rst syn fin} udp {src_port <value 0-65535> dst_port <value 0-65535>} protocol_id <value 0 - 255> {user_define <hex 0x0-0xffffffff>}}] port [<portlist> all] [permit {priority <value 0-7> {replace_priority} rx_rate [no_limit <value 1-156249>]} replace_dscp <value 0-63> counter [enable disable]} mirror {group_id <value 1-4>} deny] packet_content {offset_chunk_1 <hex 0x0-0xffffffff> offset_chunk_2 <hex 0x0-0xffffffff> offset_chunk_3 <hex 0x0-0xffffffff> offset_chunk_4 <hex 0x0-0xffffffff>} port [<portlist> all] [permit {priority <value 0-7> {replace_priority} rx_rate [no_limit <value 1-156249>]} replace_dscp <value 0-63> counter [enable disable]} mirror {group_id <value 1-4>} deny] ipv6 {class <value 0-255> flowlabel <hex 0x0-0xffff> source_ipv6 <ipv6addr> destination_ipv6 <ipv6addr> [tcp {src_port <value 0-65535> dst_port <value 0-65535>} udp {src_port <value 0-65535> dst_port <value 0-65535>}}] port [<portlist> all] [permit {priority <value 0-7> {replace_priority} rx_rate [no_limit <value 1-156249>]} counter [enable disable]} mirror {group_id <value 1-4>} deny]}] {time_range <range_name 32>} delete access_id <value 1-128>]
config flow_meter	profile_id <value 1-6> access_id <value 1-128> [[tr_tcm cir <value 0-156249> {cbs <value 0-16384>} pir <value 0-156249> {pbs <value 0-16384>} sr_tcm cir <value 0-156249> cbs <value 0-16384> ebs <value 0-16384> } {conform [permit replace_dscp <value 0-63>] {counter [enable disable]}} exceed [permit replace_dscp <value 0-63> drop] {counter [enable disable]} violate [permit replace_dscp <value 0-63> drop] {counter [enable disable]} delete]
show flow_meter	{profile_id <value 1-6> {access_id <value 1-128>}}
config time_range	<range_name 32> [hours start_time <time hh:mm:ss> end_time <time hh:mm:ss> weekdays <daylist> delete]
show time_range	

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

create access_profile

Purpose Used to create access list rules.

create access_profile

Syntax	<pre>create access_profile [ethernet {vlan source_mac <macmask 000000000000- ffffffff> destination_mac <macmask 000000000000-ffffffff> 802.1p ethernet_type} ip {vlan source_ip_mask <netmask> destination_ip_mask <netmask> dscp [icmp {type code} igmp {type} tcp {src_port_mask <hex 0x0- 0xffff> dst_port_mask <hex 0x0-0xffff> flag_mask [all {urg ack psh rst syn fin}]} udp {src_port_mask <hex 0x0-0xffff> dst_port_mask <hex 0x0-0xffff>} protocol_id_mask <hex 0x0-0xff> {user_define_mask <hex 0x0-0xffffffff>}}] packet_content_mask { offset_chunk_1 <value 0-31> <hex 0x0-0xffffffff> offset_chunk_2 <value 0-31> <hex 0x0-0xffffffff> offset_chunk_3 <value 0-31> <hex 0x0-0xffffffff> offset_chunk_4 <value 0-31> <hex 0x0-0xffffffff>} ipv6 {class flowlabel source_ipv6_mask <ipv6mask> destination_ipv6_mask <ipv6mask> [tcp {src_port_mask <hex 0x0-0xffff> dst_port_mask <hex 0x0-0xffff>} udp {src_port_mask <hex 0x0-0xffff> dst_port_mask <hex 0x0-0xffff>}]}] profile_id <value 1-6></pre>
Description	The create access_profile command creates access list rules.
Parameters	<p><i>vlan</i> - Specifies a vlan mask. Only the last 12 bits of the mask will be considered.</p> <p><i>source_mac</i> - Specifies the source mac mask.</p> <p><i>destination_mac</i> - Specifies the destination mac mask.</p> <p><i>802.1p</i> - Specifies 802.1p priority tag mask.</p> <p><i>ethernet_type</i> - Specifies the ethernet type mask.</p> <p><i>vlan</i> - Specifies a vlan mask. Only the last 12 bits of the mask will be considered.</p> <p><i>source_ip_mask</i> - Specifies an IP source submask.</p> <p><i>destination_ip_mask</i> - Specifies an IP destination submask.</p> <p><i>dscp</i> - Specifies the dscp mask.</p> <p><i>icmp</i> - Specifies that the rule applies to icmp traffic.</p> <p style="padding-left: 20px;"><i>type</i> - Specifies that the rule applies to icmp type traffic.</p> <p style="padding-left: 20px;"><i>code</i> - Specifies that the rule applies to icmp code traffic.</p> <p><i>igmp</i> - Specifies that the rule applies to igmp traffic.</p> <p style="padding-left: 20px;"><i>type</i> - Specifies that the rule applies to igmp type traffic.</p> <p><i>tcp</i> - Specifies that the rule applies to tcp traffic.</p> <p style="padding-left: 20px;"><i>src_port_mask</i> - Specifies the tcp source port mask.</p> <p style="padding-left: 20px;"><i>dst_port_mask</i> - Specifies the tcp destination port mask.</p> <p style="padding-left: 20px;"><i>flag_mask</i> - Specifies the TCP flag field mask.</p> <p><i>udp</i> - Specifies that the rule applies to udp traffic.</p> <p style="padding-left: 20px;"><i>src_port_mask</i> - Specifies theudp source port mask.</p> <p style="padding-left: 20px;"><i>dst_port_mask</i> - Specifies theudp destination port mask.</p> <p><i>protocod_id_mask</i> - Specifies that the rule applies to the ip protocol id traffic.</p> <p style="padding-left: 20px;"><i>user_define_mask</i> - Specifies that the rule applies to the ip protocol id and the mask options behind the IP header length is 20 bytes.</p> <p><i>ipv6</i> - Specifies ipv6 filtering mask. The field is optional by project.</p> <p style="padding-left: 20px;"><i>class</i> - Specifies the ipv6 class.</p> <p style="padding-left: 20px;"><i>flowlabel</i> - Specifies the ipv6 flowlabel.</p> <p style="padding-left: 20px;"><i>source_ipv6_mask</i> - Specifies an IPv6 source submask.</p> <p style="padding-left: 20px;"><i>destination_ipv6_mask</i> - Specifies an IPv6 destination submask.</p> <p style="padding-left: 20px;"><i>src_port_mask</i> - Specifies an IPv6 L4(TCP/UDP) source port submask</p> <p style="padding-left: 20px;"><i>des_port_mask</i> - Specifies an IPv6 L4(TCP/UDP) destination port submask</p> <p><i>profile_id</i> - Specifies the index of access list profile. The range is depend on project..</p> <p><i>offset_chunk_1, offset_chunk_2, offset_chunk_3, offset_chunk_4</i> - Specifies the frame content offset and mask. Up to 4 trunk offset and masks in maximum could be configured. A trunk mask presents 4 bytes.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create an Ethernet access profile:

```
DGS-3450:admin# create access_profile ethernet vlan source_mac 00-00-00-00-00-01
destination_mac 00-00-00-00-00-02 802.1p ethernet_type profile_id 1
Command: create access_profile ethernet vlan source_mac 00-00-00-00-00-01 destination_mac
00-00-00-00-00-02 802.1p ethernet_type profile_id 1

Success.

DGS-3450:admin# create access_profile ip source_ip_mask 20.0.0.0 destination_ip_mask
10.0.0.0 dscp icmp type code profile_id 2
Command: create access_profile ip source_ip_mask 20.0.0.0 destination_ip_mask 10.0.0.0
dscp icmp type code profile_id 2

Success.

DGS-3450:admin#
```

To create an option 2 packet content mask access profile:

```
DGS-3450:admin# create access_profile packet_content_mask offset_chunk_1 0 0xFFFFFFFF
offset_chunk_2 1 0xFFFFFFFF offset_chunk_3 2 0xFFFFFFFF offset_chunk_4 3 0xFFFFFFFF
profile_id 3
Command: create access_profile packet_content_mask offset_chunk_1 0 0xFFFFFFFF
offset_chunk_2 1 0xFFFFFFFF offset_chunk_3 2 0xFFFFFFFF offset_chunk_4 3 0xFFFFFFFF
profile_id 3

Success.

DGS-3450:admin#
```

delete access_profile

Purpose	Used to delete access list rules.
Syntax	delete access_profile [profile_id <value 1-6> all]
Description	The delete access_profile command deletes access list rules. Delete access_profile command can only delete the profile which is created by ACL module.
Parameters	<i>profile_id</i> - Specifies the index of access list profile. The range is depend on project.. <i>all</i> - Specifies the whole access list profile to delete.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete access list rules:

```
DGS-3450:admin#delete access_profile profile_id 6
```

```
Command: delete access_profile profile_id 6
```

```
Success.
```

```
DGS-3450:admin#
```

config access_profile

Purpose	Used to configure access list entry.
Syntax	config access_profile profile_id <value 1-6> [add access_id [auto_assign <value 1-128>] [ethernet {vlan <vlan_name 32> source_mac <macaddr 000000000000-ffffffff> destination_mac <macaddr 000000000000-ffffffff> 802.1p <value 0-7> ethernet_type <hex 0x0-0xffff>} port [<portlist> all] [permit {priority <value 0-7> {replace_priority} rx_rate [no_limit <value 1-156249>] replace_dscp <value 0-63> counter [enable disable]} mirror {group_id <value 1-4>} deny] ip {vlan <vlan_name 32> source_ip <ipaddr> destination_ip <ipaddr> dscp <value 0-63> [icmp {type <value 0-255> code <value 0-255>} igmp {type <value 0-255>} tcp {src_port <value 0-65535> dst_port <value 0-65535> urg ack psh rst syn fin} udp {src_port <value 0-65535> dst_port <value 0-65535>} protocol_id <value 0 - 255> {user_define <hex 0x0-0xffffffff>}}] port [<portlist> all] [permit {priority <value 0-7> {replace_priority} rx_rate [no_limit <value 1-156249>] replace_dscp <value 0-63> counter [enable disable]} mirror {group_id <value 1-4>} deny] packet_content {offset_chunk_1 <hex 0x0-0xffffffff> offset_chunk_2 <hex 0x0-0xffffffff> offset_chunk_3 <hex 0x0-0xffffffff> offset_chunk_4 <hex 0x0-0xffffffff>} port [<portlist> all] [permit {priority <value 0-7> {replace_priority} rx_rate [no_limit <value 1-156249>] replace_dscp <value 0-63> counter [enable disable]} mirror {group_id <value 1-4>} deny] ipv6 {class <value 0-255> flowlabel <hex 0x0-0xffff> source_ipv6 <ipv6addr> destination_ipv6 <ipv6addr> [tcp {src_port <value 0-65535> dst_port <value 0-65535>} udp {src_port <value 0-65535> dst_port <value 0-65535>}}] port [<portlist> all] [permit {priority <value 0-7> {replace_priority} rx_rate [no_limit <value 1-156249>] counter [enable disable]} mirror {group_id <value 1-4>} deny]}{time_range <range_name 32>} delete access_id <value 1-128>]
Description	The config access_profile command configures access list entry. ACL mirror function will be worked after mirror enabled and mirror port has been configured by mirror command. When apply a access rule to a target, if the target is VLAN, then the setting for value the VLAN field will not take effect.
Parameters	<i>profile_id</i> - Specifies the index of access list profile. The range is depend on project. <i>access_id</i> - Specifies the index of access list entry. The range of this value is 1-65535, but the supported max entry number is depend on project. <i>auto_assign</i> - while add to multiple ports , the access id will be auto assigned. <i>vlan</i> - Specifies a vlan name <i>source_mac</i> - Specifies the source mac <i>destination_mac</i> - Specifies the destination mac <i>802.1p</i> - Specifies the value of 802.1p priority tag, the vaule can be configured between 1 to 7 <i>ethernet_type</i> - Specifies the Ethernet type <i>vlan</i> - Specifies a vlan name <i>source_ip</i> - Specifies an IP source address <i>destination_ip</i> - Specifies an IP destination address <i>dscp</i> - Specifies the value of dscp, the value can be configured 0 to 63 <i>icmp</i> – See below: <i>type</i> - Specifies that the rule applies to the value of icmp type traffic <i>code</i> - Specifies that the rule applies to the value of icmp code traffic

config access_profile

igmp – See below:

type - Specifies that the rule applies to the value of igmp type traffic

tcp – See below:

src_port - Specifies that the rule applies the range of tcp source port

dst_port - Specifies the range of tcp destination port range

flag - Specifies the TCP flag fields .

udp – See below:

src_port - Specifies the range of tcp source port range

dst_port - Specifies the range of tcp destination port mask

protocod_id - Specifies that the rule applies to the value of ip protocol id traffic

user_define - Specifies that the rule applies to the ip protocol id and the mask options behind the IP header length is 20 bytes.

packet_content - Specifies the packet content for the user defined mask.

ipv6 - Specifies the rule applies to ipv6 fields . The field is optional by project.

class - Specifies the value of ipv6 class.

flowlabel - Specifies the value of ipv6 flowlabel.

source_ipv6 - Specifies the value of ipv6 source address.

destination_ipv6 - Specifies the value of ipv6 destination address.

src_port - Specifies the value of ipv6 L4(TCP/UDP) source port

dst_port - Specifies the value of ipv6 L4(TCP/UDP) destination port

port - Specifies a list of port to apply the rule.

permit - Specifies the packets that match the access profile are permit by the switch

priority - Specifies that priority of the packet will be changed if the packet match the access rule.

replace_priority - Specifies 802.1p priority of the outgoing packet will be marked too.

replace_dscp - Specifies that DSCP of the outgoing packet will be marked by the new value.

counter - Specifies whether counter feature will be enabled / disabled. If the rule is binded with *flow_meter*, then “counter” here will be overridden.

deny - Specifies the packets that match the access profile are filtered by the switch

mirror - Specifies the packets that match the access profile are sent the copied one to the mirror port.

time_range - Specifies name of this time range entry.

offset_chunk_1, offset_chunk_2, offset_chunk_3, offset_chunk_4 - Specifies the content of the trunk to be monitored.

Restrictions

Only Administrator and Operator-level users can issue this command.

Example usage:

To configure an access list rule entry:

```
DGS-3450:admin# config access_profile profile_id 1 add access_id 1 ip vlan default
source_ip 20.2.2.3 destination_ip 10.1.1.252 dscp 3 icmp type 11 code 32 port 1 mirror
group_id 1 time_range testdaily
Command: config access_profile profile_id 1 add access_id 1 ip vlan default source_ip
20.2.2.3 destination_ip 10.1.1.252 dscp 3 icmp type 11 code 32 port 1 mirror group_id 1
time_range testdaily
```

Mirror function must be enabled and mirror port must be configured.

Success.

```
DGS-3450:admin#
```

To configure an rule entry for packet content mask profile:

```
DGS-3450:admin# config access_profile profile_id 5 add access_id auto_assign
packet_content offset_chunk_1 0xAAAAAAAA offset_chunk_2 0BBBBBBBBB offset_chunk_3
0xFFFFFFFF offset_chunk_4 0xEEEEEEEEE port all permit
Command: config access_profile profile_id 5 add access_id auto_assign packet_content
offset_chunk_1 0xAAAAAAAA offset_chunk_2 0BBBBBBBBB offset_chunk_3 0xFFFFFFFF
offset_chunk_4 0xEEEEEEEEE port all permit
```

Success.

```
DGS-3450:admin#
```

show access_profile

Purpose	Used to display current access list table.
Syntax	show access_profile {profile_id <value 1-6>}
Description	The show access_profile command displays current access list table.
Parameters	<i>profile_id</i> - Specifies the index of access list profile. The range is depend on project.
Restrictions	None.

Example usage:

To display current access list table:

```

DGS-3450:admin# show access_profile
Command: show access_profile

Access Profile Table

Total Unused Rule Entries: 765
Total Used Rule Entries : 3

Access Profile ID: 1                                TYPE : Packet Content
=====
Owner          : ACL
MASK Option :
-----
Offset_chunk_1: 1      value:FFFFFFFF
Offset_chunk_2: 2      value:EEEEEEEE
Offset_chunk_3: 3      value:DDDDDDDD
Offset_chunk_4: 4      value:CCCCCCCC

Access ID : 1                Mode: Permit                priority: 3
Port: 1:1
-----
Offset_chunk_1: 1      value:11111111
Offset_chunk_2: 2      value:22222222
Offset_chunk_3: 3      value:11111111
Offset_chunk_4: 4      value:44444444
=====
Unused rule entries: 127

DGS-3450:admin#
    
```

config flow_meter profile_id

Purpose	To configure packet flow-based metering based on an access profile and rule.
Syntax	config flow_meter profile_id <value 1-6> access_id <value 1-128> [[tr_tcm cir <value 0-156249> {cbs <value 0-16384>} pir <value 0-156249> {pbs <value 0-16384>} sr_tcm cir <value 0-156249> cbs <value 0-16384> ebs <value 0-16384>] {conform [permit replace_dscp <value 0-63>} {counter [enable disable]}] exceed [permit replace_dscp <value 0-63> drop] {counter [enable disable]} violate [permit replace_dscp <value 0-63> drop] {counter [enable disable]} delete]
Description	<p>This command is used to configure the flow-based metering function. The metering function support three modes, single rate two colors, single rate three color, and two rate three color. The access rule must first be created before the parameters of this function can be applied.</p> <p>For the single rate two color mode, users may set the preferred bandwidth for this rule, in Kbps and once the bandwidth has been exceeded, overflow packets will be either dropped or be set to a drop precedence, depending on user configuration. The drop precedence will be used by RED. With RED, the packet with higher drop precedence will be dropped with higher probability.</p> <p>For the single rate three color mode, users need to specify the committed rate in Kbps, the committed burst size and the excess burst size.</p> <p>For the two rate three color mode, users need to specify the committed rate in Kbps, the committed burst size, the peak rate and the peak burst size.</p> <p>There can be two cases to map the color of packet, color blind mode and color aware mode. In the color-blind case, the determination for the color of packet is based on metering result. In the color-aware case, the determination for the color of packet is based metering result and the ingress DSCP.</p> <p>When the color blind or color aware is not specified, color blind is the default mode.</p> <p>The green color packet will be treated the conforming action, the yellow color packet will be</p>

config flow_meter profile_id

	treated the exceeding action, and the red color packet will be treated the violating action.
Parameters	<p><i>profile_id</i> - Specifies the profile_ID.</p> <p><i>access_id</i> - Specifies the access_ID.</p> <p><i>tr_tcm</i> - Specify the “two rate three color mode”.</p> <p><i>cir</i> - Specify the “committed information rate”.</p> <ol style="list-style-type: none"> 1. The unit is 64Kbps 2. The max rate 156249*64Kbps <p><i>cbs</i> - Specify the “committed burst size”.</p> <ol style="list-style-type: none"> 1. The unit is Kbytes. That is to say, 1 means 1Kbytes. 2. This parameter is an optional parameter. The default value is 4*1024. 3. The max set value is 16*1024. <p><i>pir</i> - Specify the “Peak Information Rate”.</p> <ol style="list-style-type: none"> 1. The unit is 64Kbits 2. The max rate is 156249*64Kbps <p><i>pbs</i> - Specify the “peak burst size”.</p> <ol style="list-style-type: none"> 1. The unit is Kbytes. 2. This parameter is an optional parameter. The default value is 4*1024. 3. The max set value is 16*1024. <p><i>sr_tcm</i> - Specify the “single rate three color mode”.</p> <p><i>cir</i> - Specify the “committed information rate”.</p> <ol style="list-style-type: none"> 1. The unit is 64Kbps 2. The max rate is 156249*64Kbps <p><i>cbs</i> - Specify the “committed burst size”.</p> <ol style="list-style-type: none"> 1. The unit is Kbytes. 2. The max set value is 16*1024. <p><i>ebs</i> - Specify the “Excess Burst Size”.</p> <ol style="list-style-type: none"> 1. The unit is Kbytes. 2. The max set value is 16*1024. <p><i>conform</i> - Specify the action when packet is in “green color”.</p> <p><i>permit</i> - Permit the packet.</p> <p><i>replace_dscp</i> - Change the dscp of packet.</p> <p><i>exceed</i> - Specify the action when packet is in “yellow color”.</p> <p><i>permit</i> - Permit the packet.</p> <p><i>replace_dscp</i> - Change the dscp of packet.</p> <p><i>drop</i> - Drop the packet.</p> <p><i>violate</i> - Specify the action when packet is in “red color”.</p> <p><i>permit</i> - Permit the packet.</p> <p><i>replace_dscp</i> - Change the dscp of packet.</p> <p><i>counter</i> - Specify the counter.</p> <ol style="list-style-type: none"> 1. This is optional. The default is “disable”. 2. The resource may be limited such that counter can not be turned on. The limitation is project dependent. 3. <i>counter</i> will be cleared when the function is disabled. <p><i>delete</i> - Delete the specified flow_meter.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure a two rates thress color flow meter:

```
DGS-3450:admin# config flow_meter profile_id 1 access_id 1 tr_tcm cir 1000 cbs 200 pir
2000 pbs 200 exceed replace_dscp 21 violate drop
Command: config flow_meter profile_id 1 access_id 1 tr_tcm cir 1000 cbs 200 pir 2000 pbs
200 exceed replace_dscp 21 violate drop
DGS-3450:admin#
```

show flow_meter

Purpose	To configure packet flow-based metering based on an access profile and rule.
Syntax	show flow_meter {profile_id <value 1-6> {access_id <value 1-128>}}
Description	This command displays the flow meter configuration.
Parameters	<i>profile_id</i> - Specifies the profile_ID. <i>access_id</i> - Specifies the access_ID.
Restrictions	None.

Example usage:

To display the flow meter configuration:

```
DGS-3450:admin# show flow_meter
Command: show flow_meter

Flow Meter Information
-----
Profile ID:4      Access ID:1      Mode : trTCM
CIR:1000(64Kbps)  CBS:200(Kbyte)   PIR:2000(64Kbps)  PBS:200(Kbyte)
Action:
  Conform : Permit           Counter: Disabled
  Exceed  : Permit           Replace DSCP: 21   Counter: Disabled
  Violate : Drop             Counter: Disabled

Total Entries: 1
DGS-3450:admin#
```

config time_range

Purpose	Used to configure the range of time to activate a function on the switch.
Syntax	config time_range <range_name 32> [hours start_time <time hh:mm:ss> end_time <time hh:mm:ss> weekdays <daylist> delete]
Description	This command defines a specific range of time to activate a function on the Switch by specifying which time range in a day and which days in a week are covered in the time range. Note that the specified time range is based on SNTP time or configured time. If this time is not available, then the time range will not be met.
Parameters	<i><range_name 32></i> - Specifies the name of the time range settings. <i>start_time</i> - Specifies the starting time in a day. (24-hr time) For example, 19:00 means 7PM. 19 is also acceptable. <i>start_time</i> must be smaller than <i>end_time</i> . <i>end_time</i> - Specifies the ending time in a day. (24-hr time) <i>weekdays</i> - Specify the list of days contained in the time range. Use a dash to define a period of days. Use a comma to separate specific days. For example, mon-fri (Monday to Friday), sun, mon, fri (Sunday, Monday and Friday) <i>delete</i> - Deletes a time range profile. When a time_range profile has been associated with

config time_range

	ACL entries, the delete of this time_range profile will fail.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the range of time to activate a function on the switch.

```
DGS-3450:admin# config time_range weekend hours start_time 0:0:0 end_time 23:59:59 weekdays sun,sat
Command: config time_range weekend hours start_time 0:0:0 end_time 23:59:59 weekdays sun,sat

Success.

DGS-3450:admin#
```

show time_range

Purpose	Used to display time range information.
Syntax	show time_range
Description	The show time_range command displays current time range setting.
Parameters	None.
Restrictions	None.

Example usage:

To display current time range setting:

```
DGS-3450:admin#show time_range
Command: show time_range

Time Range Information
-----
Range Name      : weekend
Weekdays       : Sun,Sat
Start Time      : 00:00:00
End Time        : 23:59:59

Total Entries :1

DGS-3450:admin#
```


ACL FLOW METERING COMMANDS

Before configuring the ACL Flow Meter, here is a list of acronyms and terms users will need to know.

trTCM – Two Rate Three Color Marker. This, along with the srTCM, are two methods available on the switch for metering and marking packet flow. The trTCM meters and IP flow and marks it as a color based on the flow's surpassing of two rates, the CIR and the PIR.

- **CIR** – Committed Information Rate. Common to both the trTCM and the srTCM, the CIR is measured in bytes of IP packets. IP packet bytes are measured by taking the size of the IP header but not the link specific headers. For the trTCM, the packet flow is marked green if it doesn't exceed the CIR and yellow if it does. The configured rate of the CIR must not exceed that of the PIR. The CIR can also be configured for unexpected packet bursts using the CBS and PBS fields.
- **CBS** – Committed Burst Size. Measured in bytes, the CBS is associated with the CIR and is used to identify packets that exceed the normal boundaries of packet size. The CBS should be configured to accept the biggest IP packet that is expected in the IP flow.
- **PIR** – Peak Information Rate. This rate is measured in bytes of IP packets. IP packet bytes are measured by taking the size of the IP header but not the link specific headers. If the packet flow exceeds the PIR, that packet flow is marked red. The PIR must be configured to be equal or more than that of the CIR.
- **PBS** – Peak Burst Size. Measured in bytes, the PBS is associated with the PIR and is used to identify packets that exceed the normal boundaries of packet size. The PBS should be configured to accept the biggest IP packet that is expected in the IP flow.

srTCM – Single Rate Three Color Marker. This, along with the trTCM, are two methods available on the switch for metering and marking packet flow. The srTCM marks its IP packet flow based on the configured CBS and EBS. A packet flow that does not reach the CBS is marked green, if it exceeds the CBS but not the EBS its marked yellow, and if it exceeds the EBS its marked red.

- **CBS** – Committed Burst Size. Measured in bytes, the CBS is associated with the CIR and is used to identify packets that exceed the normal boundaries of packet size. The CBS should be configured to accept the biggest IP packet that is expected in the IP flow.
- **EBS** – Excess Burst Size. Measured in bytes, the EBS is associated with the CIR and is used to identify packets that exceed the boundaries of the CBS packet size. The EBS is to be configured for an equal or larger rate than the CBS.

DSCP – Differentiated Services Code Point. The part of the packet header where the color will be added. Users may change the DSCP field of incoming packets.

The ACL Flow Meter function will allow users to color code IP packet flows based on the rate of incoming packets. Users have two types of Flow metering to choose from, trTCM and srTCM, as explained previously. When a packet flow is placed in a color code, the user can choose what to do with packets that have exceeded that color-coded rate.

Green – When an IP flow is in the green mode, its configurable parameters can be set in the Conform field, where the packets can have their DSCP field changed. This is an acceptable flow rate for the ACL Flow Meter function.

Yellow – When an IP flow is in the yellow mode, its configurable parameters can be set in the Exceed field. Users may choose to either **Permit** or **Drop** exceeded packets. Users may also choose to change the DSCP field of the packets.

Red – When an IP flow is in the red mode, its configurable parameters can be set in the Exceed field. Users may choose to either **Permit** or **Drop** exceeded packets. Users may also choose to change the DSCP field of the packets.

Users may also choose to count exceeded packets by clicking the **Counter** check box. If the counter is enabled, the counter setting in the access profile will be disabled.

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

Command	Parameters
config flow_meter profile_id	<value 1-6> access_id <value 1-128> [[tr_tcm cir <value 0-156249> {cbs <value 0-16384>} pir <value 0-156249> {pbs <value 0-16384>} sr_tcm cir <value 0-156249> cbs <value 0-16384> ebs <value 0-16384> } {conform [permit replace_dscp <value 0-63>] {counter [enable disable]}} exceed [permit replace_dscp <value 0-63> drop] {counter [enable disable]} violate [permit replace_dscp <value 0-63> drop] {counter [enable disable]} delete]
show flow_meter	{profile_id <value 1-6> {access_id <value 1-128>}}

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

config flow_meter profile_id

Purpose	Used to configure the flow metering function for ACL..
Syntax	config flow_meter profile_id <value 1-6> access_id <value 1-128>[[tr_tcm cir <value 0-156249> {cbs <value 0-16384>} pir <value 0-156249> {pbs <value 0-16384>} sr_tcm cir <value 0-156249> cbs <value 0-16384> ebs <value 0-16384>] {conform [permit replace_dscp <value 0-63>} {counter [enable disable]]} exceed [permit replace_dscp <value 0-63> drop] {counter [enable disable]} violate [permit replace_dscp <value 0-63> drop] {counter [enable disable]} delete]
Description	This command is used to configure the parameters for the flow metering function for ACL entries created on the switch.
Parameters	<p><i>profile_id</i> <value 1-6> – Enter the pre-configured Profile ID for which to configure the ACL Flow Metering parameters.</p> <p><i>access_id</i> <value 1-128> – Enter the pre-configured Access ID for which to configure the ACL Flow Metering parameters.</p> <p><i>tr_tcm</i> - Choosing this field will allow users to employ the Two Rate Three Color Mode and set the following parameters to determine the color rate of the IP packet flow.</p> <ul style="list-style-type: none"> • <i>cir</i> <value 0-156249> – The Committed Information Rate can be set between 1 and 156249. IP flow rates at or below this level will be considered <i>green</i>. IP flow rates that exceed this rate but not the PIR rate are considered <i>yellow</i>. • <i>cbs</i> <value 0-16384> – The Committed Burst Size. Used to gauge packets that are larger than the normal IP packets. This field does not have to be set for this feature to function properly but is to be used in conjunction with the CIR setting. The CBS should be configured to accept the biggest IP packet that is expected in the IP flow. • <i>pir</i> <value 0-16384> – The Peak information Rate. IP flow rates that exceed this setting will be considered as <i>red</i>. This field must be set at an equal or higher value than the CIR. • <i>pbs</i> <value 0-16384> – The Peak Burst Size. This optional field is to be used in conjunction with the PIR. The PBS should be configured to accept the biggest IP packet that is expected in the IP flow. <p><i>sr_tcm</i> – Choosing this field will allow users to employ the Single Rate Three Color Mode and set the following parameters to determine the color rate of the IP packet flow.</p> <ul style="list-style-type: none"> • <i>cir</i> <value 0-156249> – The Committed Information Rate can be set between 1-156249. The color rates are based on the following two fields which are used in conjunction with the CIR. • <i>cbs</i> <value 0-16384> – Committed Burst Size. Measured in bytes, the CBS is associated with the CIR and is used to identify packets that exceed the normal boundaries of packet size. The CBS should be configured to accept the biggest IP packet that is expected in the IP flow. Packet flows which are lower than this configured value are marked green. Packet flows which exceed this value but are less than the EBS value are marked yellow. <p><i>ebs</i> <value 0-16384> – Excess Burst Size. Measured in bytes, the EBS is associated with the CIR and is used to identify packets that exceed the boundaries of the CBS packet size. The EBS is to be configured for an equal or larger rate than the CBS. Packet flows that exceed this value are marked as red.</p> <p><i>conform</i> – This field denotes the <i>green</i> packet flow. Green packet flows may have their DSCP field rewritten to a value stated in this field. Users may also choose to count green packets by checking the Counter check box.</p> <ul style="list-style-type: none"> • <i>permit</i> – Enter this parameter to allow packet flows that are in the green flow. • <i>replace_dscp</i> <value 0-63> – Packets that are in the green flow may have their DSCP field rewritten using this parameter and entering the DSCP value to replace. • <i>counter [enable disable]</i> – Use this parameter to enable or disable the packet counter for the specified ACL entry in the green flow. <p><i>exceed</i> – This field denotes the <i>yellow</i> packet flow. Yellow packet flows may have excess packets permitted through or dropped. Users may replace the DSCP field of these packets by checking its radio button and entering a new DSCP value in the allotted field.</p> <ul style="list-style-type: none"> • <i>permit</i> – Enter this parameter to allow packet flows that are in the yellow flow.

config flow_meter profile_id

- *replace_dscp* <value 0-63> – Packets that are in the yellow flow may have their DSCP field rewritten using this parameter and entering the DSCP value to replace.
- *drop* – Enter this parameter to drop packets that are in the yellow flow.
- *counter* [*enable* | *disable*] – Use this parameter to enable or disable the packet counter for the specified ACL entry in the yellow flow.

violate – This field denotes the *red* packet flow. Red packet flows may have excess packets permitted through or dropped. Users may replace the DSCP field of these packets by checking its radio button and entering a new DSCP value in the allotted field.

- *permit* – Enter this parameter to allow packet flows that are in the red flow.
- *replace_dscp* <value 0-63> – Packets that are in the red flow may have their DSCP field rewritten using this parameter and entering the DSCP value to replace.
- *drop* – Enter this parameter to drop packets that are in the red flow.
- *counter* [*enable* | *disable*] – Use this parameter to enable or disable the packet counter for the specified ACL entry in the red flow.

delete – Use this parameter to delete the specified flow meter.

Restrictions

Only Administrator and Operator-level users can issue this command. Only two counters may be enabled at any given time.

Example usage:

To enable the sFlow function:

```
DGS-3450:admin# config flow_meter profile_id 1 access_id 1 tr_tcm cir 1000 cbs 200 pir 2000 pbs 200 exceed replace_dscp 21 violate drop
Command: config flow_meter profile_id 1 access_id 1 tr_tcm cir 1000 cbs 200 pir 2000 pbs 200 exceed replace_dscp 21 violate drop
```

Success.

```
DGS-3450:admin#
```

show flow_meter

Purpose	Used to display the ACL flow meter parameters set on the switch.
Syntax	show flow_meter {profile_id <value 1-6> {access_id <value 1-128>}}
Description	This command will display the flow meter parameters set on the switch.
Parameters	<i>profile_id</i> <value 1-6> – Enter the profile ID of the ACL entry to be viewed for flow metering. <i>access_id</i> <value 1-128> – Enter the access ID corresponding to the ACL entry to be viewed.
Restrictions	None.

Example usage:

To enable the sFlow function:

```
DGS-3450:admin# show flow_meter profile_id 1 access_id 1
Command: show flow_meter profile_id 1 access_id 1

Profile ID : 1          Access ID : 1          Mode: trTCM
CIR: 1000(64kbps)     CBS: 200(Kbyte)      PIR: 2000(64kbps)    PBS : 200(Kbyte)
Action:
Conform : Permit                               Counter : Disabled
Exceed  : Permit   Replace DSCP: 21             Counter : Disabled
Violate : Drop                                   Counter : Disabled

Total Entries : 1

DGS-3450:admin#
```

ADDRESS RESOLUTION PROTOCOL (ARP) COMMANDS

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

Command	Parameters
create arprentry	<ipaddr> <macaddr>
delete arprentry	[<ipaddr> all]
config arprentry	<ipaddr> <macaddr>
config arp_aging time	<min 0-65535>
clear arptable	
show arprentry	{ipif <ipif_name 12> ipaddress <ipaddr> static mac_address <macaddr>}

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

create arprentry

Purpose	Used to create a static entry in the ARP table.
Syntax	create arprentry <ipaddr> <macaddr>
Description	This command is used to enter a static ARP entry into the switch's ARP table.
Parameters	<i>ipaddr</i> - The IP address of the end node or station. <i>macaddr</i> - The MAC address corresponding to the IP address above.
Restrictions	Only Administrator and 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:

```
DGS-3450:admin# create arprentry 10.48.74.121 00-50-BA-00-07-36
Command: create arprentry 10.48.74.121 00-50-BA-00-07-36

Success.

DGS-3450:admin#
```

delete arprentry

Purpose	Used to delete a static entry from the ARP table.
Syntax	delete arprentry [<ipaddr> all]
Description	This command is used to delete an ARP entry, by specifying either the IP address of the entry or all. Specifying 'all' clears the switch's ARP table.
Parameters	<i>ipaddr</i> - The IP address of the end node or station. <i>all</i> - Delete all ARP entries.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete an entry of IP address 10.48.74.121 from the ARP table:

```
DGS-3450:admin# delete arpentry 10.48.74.121
Command: create arpentry 10.48.74.121

Success.

DGS-3450:admin#
```

config arpentry

Purpose	Used to configure a static entry's MAC address in the ARP table.
Syntax	config arpentry <ipaddr> <macaddr>
Description	This command configures a static entry's MAC address in the ARP table. Specify the IP address and MAC address of the entry.
Parameters	<i>ipaddr</i> - The IP address of the end node or station. <i>macaddr</i> - The MAC address corresponding to the IP address above.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure a static ARP entry with IP address 10.48.74.121 to have a MAC address of 00-50-BA-00-07-37:

```
DGS-3450:admin# config arpentry 10.48.74.121 00-50-BA-00-07-37
Command: config arpentry 10.48.74.121 00-50-BA-00-07-37

Success.

DGS-3450:admin#
```

config arp_aging time

Purpose	Used to configure the aging out time for an ARP entry.
Syntax	config arp_aging time <min 0-65535>
Description	This command sets the maximum amount of time, in minutes, that a dynamic ARP entry can remain in the switch's ARP table, without being accessed, before it is dropped from the table.
Parameters	<i>min</i> - The ARP age-out time, in minutes. The default is 20. The range is 0 to 65535.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure an ARP aging time of 30 minutes:

```
DGS-3450:admin# config arp_aging time 30
Command: config arp_aging time 30

Success.

DGS-3450:admin#
```

clear arptable

Purpose	Used to clear all the dynamic ARP entries from the ARP table.
Syntax	clear arptable
Description	This command is used to clear all the dynamic entries from ARP table.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To clear the ARP table:

```
DGS-3450:admin# clear arptable
Command: clear arptable

Success.

DGS-3450:admin#
```

show arpreentry

Purpose	Used to display the ARP table.
Syntax	show arpreentry {ipif <ipif_name 12> ipaddress <ipaddr> static mac_address <macaddr> }
Description	This command is used to displays the ARP table. You can filter the display by IP address, interface name, static entries or MAC address.
Parameters	<i>ipif_name</i> - The name of the IP interface the end node or station for which the ARP table entry was made, resides on. <i>ipaddr</i> - The IP address of the end node or station. <i>static</i> - Display the static entries in the ARP table. <i>macaddr</i> - Displays the ARP entry by MAC address.
Restrictions	None.

Example usage:

To display the ARP table:


```
DGS-3450:admin# show arpentry
```

```
Command: show arpentry
```

```
ARP Aging Time : 20
```

Interface	IP Address	MAC Address	Type
System	10.0.0.0	FF-FF-FF-FF-FF-FF	Local/Broadcast
System	10.1.1.1	00-02-03-04-05-06	Static
System	10.1.1.2	00-02-03-04-05-06	Dynamic
System	10.1.1.3	00-02-03-04-05-06	Static
System	10.90.90.90	00-01-02-03-04-00	Local
System	10.255.255.255	FF-FF-FF-FF-FF-FF	Local/Broadcast

```
Total Entries: 6
```

```
DGS-3450:admin#
```

BPDU ATTACK PROTECTION COMMANDS

Users at different sites connected across a service-provider network need to use various Layer 2 protocols to scale their topologies to include all remote sites, as well as the local sites. STP must run properly, and every VLAN should build a proper spanning tree that includes the local site and all remote sites across the service-provider network.

Layer 2 protocol tunneling is a feature designed for service providers who carry traffic of multiple customers across their networks and are required to maintain the Layer 2 protocol configurations of each customer without impacting the traffic of other customers.

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

Command	Parameters
config bpdu_protection ports	[<portlist> all] {state [enable disable] mode [drop block shutdown] } (1)
config bpdu_protection recovery_timer	[<sec 60-1000000> infinite]
config bpdu_protection	[trap log] [none attack_detected attack_cleared both]
enable bpdu_protection	
disable bpdu_protection	
show bpdu_protection	{ports {<portlist>}}

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

config bpdu_protection ports

Purpose	Used to configure bpdu_protection state and mode.
Syntax	config bpdu_protection ports [<portlist> all] {state [enable disable] mode [drop block shutdown] } (1)
Description	<p>The config bpdu_protection ports command is used to configure the BPDP protection function for the ports on the switch. In generally, there are two states in BPDU protection function. One is normal state, and another is under attack state. The under attack state have three modes: drop, block, and shutdown. A BPDU protection enabled port will enter under attack state when it receives one STP BPDU packet. And it will take action based on the configuration. Thus, BPDU protection can only be enabled on STP disabled port.</p> <p>BPDU protection has high priority than fbpdu setting configured by configure STP command in determination of BPDU handling. That is, when fbpdu is configured to forward STP BPDU but BPDU protection is enabled, then the port will not forward STP BPDU.</p> <p>BPDU protection also has high priority than BPDU tunnel port setting in determination of BPDU handling.</p> <p>That is, when a port is configured as BPDU tunnel port for STP, it will forward STP BPDU. But if the port is BPDU protection enabled. Then the port will not forward STP BPDU</p>
Parameters	<p><i>portlist</i> - Specified a range of ports to be configured (port number).</p> <p><i>all</i> - For set all ports in the system, you may use "all" parameter.</p> <p><i>state</i> - Specified the bpdu_protection state. The default state is disable</p> <p><i>enable</i> - Enable bpdu_protection</p> <p><i>disable</i> - Disable bpdu_protection</p> <p><i>mode</i> - Specified the bpdu_protection mode. The default mode is shutdown</p> <p><i>drop</i> - Drop all received BPDU packets when the port enters under_attack state.</p> <p><i>block</i> - Drop all packets (include BPDU and normal packets) when the port enters under_attack state.</p> <p><i>shutdown</i> - Shut down the port when the port enters under_attack state.</p>

config bpdu_protection ports

Restrictions

Only Administrator and Operator-level users can issue this command.

Example usage:

To set the port state enable and drop mode:

```
DGS-3450:admin# config bpdu_protection ports 1 state enable mode drop
Commands: config bpdu_protection ports 1 state enable mode drop

Success.

DGS-3450:admin#
```

config bpdu_protection recovery_interval

Purpose	Used to configure bpdu_protection recovery timer.
Syntax	config bpdu_protection recovery_timer [<sec 60-1000000> infinite]
Description	When a port enters under attack state, it can be disabled or blocked based on the configuration. The state can be recovered manually or by the auto recovery mechanism. This command is used to configure the auto-recovery timer. To manually recover the port, the user needs to disable and re-enable the port.
Parameters	<i>recovery_timer</i> - Specified the bpdu_protection Auto-Recovery recovery_timer. The default value of recovery_timer is 60. <i>infinite</i> - The port will not be auto recovered. <sec 60 –1000000> - The timer (in seconds) used by the Auto-Recovery mechanism to recover the port. The valid range is 60 to 1000000.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the bpdu_protection recovery_timer to 120 seconds for the entire switch:

```
DGS-3450:admin# config bpdu_protection recovery_timer 120
Commands: config bpdu_protection recovery_timer 120

Success.

DGS-3450:admin#
```

config bpdu_protection

Purpose	Used to configure bpdu_protection trap state or log state.
Syntax	config bpdu_protection [trap log] [none attack_detected attack_cleared both]
Description	The config bpdu_protection trap command is used to configure the bpdu_protection trap state or state for the entire switch.
Parameters	<i>trap</i> - To specify the trap state. <i>log</i> - To specify the log state. <i>none</i> - Neither attack_detected nor attack_cleared is trapped or logged. <i>attack_detected</i> - Events will be logged or trapped when the BPDU attacks is detected. <i>attack_cleared</i> - Events will be logged or trapped when the BPDU attacks is cleared. <i>both</i> - The events of attack_detected and attack_cleared shall be trapped or logged.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To config the bpdu_protection trap state as both for the entire switch:

```
DGS-3450:admin# config bpdu_protection trap both
Commands: config bpdu_protection trap both

Success.

DGS-3450:admin#
```

enable bpdu_protection

Purpose	Used to enable bpdu_protection globally.
Syntax	enable bpdu_protection
Description	The enable bpdu_protection command is used to enable bpdu_protection function globally for the entire switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable bpdu_protection function globally for the entire switch:

```
DGS-3450:admin# enable bpdu_protection
Commands: enable bpdu_protection

Success.

DGS-3450:admin#
```

disable bpdu_protection

Purpose	Used to disalbe bpdu_protection globally.
Syntax	disable bpdu_protection
Description	The disable bpdu_protection command is used to disable bpdu_protection function globally for the entire switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable bpdu_protection function globally for the entire switch:

```
DGS-3450:admin# disable bpdu_protection
Commands: disable bpdu_protection

Success.

DGS-3450:admin#
```

show bpdu_protection

Purpose	Used to show bpdu_protection status.
Syntax	show bpdu_protection {ports {<portlist>}}
Description	The show bpdu_protection command is used to display bpdu_protection global configuration or per port configuration and current status.
Parameters	<i>portlist</i> - Specified a range of ports to be configured.
Restrictions	None.

Example usage:

To show the bpdu_protection for the entire switch:

```
DGS-3450:admin# show bpdu_protection
Commands: show bpdu_protection

BPDU Protection Global Settings
-----
BPDU Protection status           : Enabled
BPDU Protection Recovery Time    : 60 seconds
BPDU Protection Trap State       : None
BPDU Protection Log State        : None

DGS-3450:admin#
```

To show the bpdu_protection status ports 1-12:

```
DGS-3450:admin# show bpdu_protection ports 1-12
Commands: show bpdu_protection ports 1-12

Port      State      Mode      Status
-----
1         Enabled   shutdown  Normal
2         Enabled   shutdown  Normal
3         Enabled   shutdown  Normal
4         Enabled   shutdown  Normal
5         Enabled   shutdown  Under Attack
6         Enabled   shutdown  Normal
7         Enabled   shutdown  Normal
8         Enabled   shutdown  Normal
9         Enabled   shutdown  Normal
10        Enabled   Block     Normal
11        Disabled  shutdown  Normal
12        Disabled  shutdown  Normal

DGS-3450:admin#
```

COMMAND HISTORY LIST

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

Command	Parameters
?	{<command>}
config command_history	<value 1-40>
show command_history	

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

?	
Purpose	Used to display all commands in the Command Line Interface (CLI).
Syntax	? {<command>}
Description	This command will display all of the commands available through the Command Line Interface (CLI).
Parameters	{<command>} – Entering the question mark with an appropriate command will list all the corresponding parameters for the specified command, along with a brief description of the commands function and similar commands having the same words in the command.
Restrictions	None.

Example usage:

To display all of the commands in the CLI:

```
DGS-3450:admin# ?
..
?
cd
clear
clear address_binding dhcp_snoop binding_entry ports
clear arptable
clear attack_log
clear counters
clear dhcp_binding
clear fdb
clear log
clear mac_based_access_control auth_mac
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 guest_vlan ports
config 802.1x init
CTRL+C ESC q Quit SPACE n Next Page Enter Next Entry a All
```

To display the parameters for a specific command:

```
DGS-3450:admin# ? config stp
Command:? config stp

Command: config stp
Usage: {maxage <value 6-40>|maxhops <value 1-20> |hellotime <value 1-10>| forwa
rdldelay <value 4-30>|txholdcount <value 1-10>|fbpdu [enable|disable]|lbd [enable
|disable] |lbd_recover_timer [<value 0> | <value 60-1000000>]}
Description: Used to update the STP Global Configuration.
config stp instance_id
config stp mst_config_id
config stp mst_ports
config stp ports
config stp priority
config stp version

DGS-3450:admin#
```

config command_history

Purpose	Used to configure the command history.
Syntax	config command_history <value 1-40>
Description	This command is used to configure the command history.
Parameters	<value 1-40> – The number of previously executed commands maintained in the buffer. Up to 40 of the latest executed commands may be viewed.
Restrictions	None.

Example usage

To configure the command history:


```
DGS-3450:admin# config command_history 20
Command: config command_history 20

Success.

DGS-3450:admin#
```

show command_history

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

Example usage

To display the command history:

```
DGS-3450:admin# show command_history
Command: show command_history

?
? show
show vlan
show command history

DGS-3450:admin#
```

COMMAND LOGGING COMMANDS

The command logging function is used to log the commands that have successfully been configured to the switch via the command line interface. The requirement is to log the command itself, along with information about the user account that entered the command into the system log and the informational severity level. Commands that do not cause a change in the switch configuration or operation (such as show) will not be logged. A save command will change the configuration file hence it will be logged. Information about saving or viewing the system log is described in the syslog functional specification and is out of the scope of this UIS.

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

Command	Parameters
enable command logging	
disable command logging	
show command logging	

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

enable command logging

Purpose	Used to enable command logging.
Syntax	enable command logging
Description	The enable command logging command is used to enable the command logging function. Note: When the switch is under the booting procedure, all configuration commands will not be logged. When the user has logged in using AAA authentication, the user name should not be changed if the user has used the "enable admin" command to replace its privilege.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable the command logging function:

```
DGS-3450:admin# enable command logging
Command: enable command logging

Success.

DGS-3450:admin#
```

disable command logging

Purpose	Used to disable the command logging function.
Syntax	disable command logging
Description	The disable command logging command is used to disable the command logging function.
Parameters	None.

disable command logging

Restrictions	Only Administrator and Operator-level users can issue this command.
--------------	---

Example usage:

To disable the command logging function:

```
DGS-3450:admin# disable command logging
Command: disable command logging

Success.

DGS-3450:admin#
```

show command logging

Purpose	This command displays the switch's general command logging configuration status
Syntax	show command logging
Description	Use this command to show the command logging configuration status.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To show the command logging configuration status:

```
DGS-3450:admin# show command logging
Command: show command logging

Command Logging State : Disabled

DGS-3450:admin#
```

COMPOUND AUTHENTICATION COMMANDS

The Compound Authentication chapter describes the Common feature for access control functionalities and specifications.

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

Command	Parameters
create authentication guest_vlan	[vlan <vlan_name 32> vlanid <vlanid 1-4094>]
delete authentication guest_vlan	[vlan <vlan_name 32> vlanid <vlanid 1-4094>]
config authentication guest_vlan	[vlan <vlan_name 32> vlanid <vlanid 1-4094>] [add delete] ports [<portlist> all]
config authentication ports	[<portlist> all] {auth_mode [port_based host_based { vlanid <vidlist> state [enable disable] }]} multi_authen_methods[none any dot1x_impb impb_jwac] (1)
show authentication guest_vlan	
show authentication ports	{<portlist>}
enable authorization attributes	
disable authorization attributes	
show authorization	
config authentication server failover	[local permit block]
show authentication	

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

create authentication guest_vlan

Purpose	Used to assign a static VLAN to be guest VLAN.
Syntax	create authentication guest_vlan [vlan <vlan_name 32> vlanid <vlanid 1-4094>]
Description	The create guest_vlan command will assign a static VLAN to be guest VLAN. The specific VLAN which assigned to guest VLAN must be existed. The specific VLAN which assigned to guest VLAN can't be deleted. For further description of this command please see description for config authentication guest_vlan ports.
Parameters	<vlan_name 32> - Specify the guest VLAN by VLAN name. vlanid - Specify the guest VLAN by VLAN ID.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create an authentication guest VLAN:

```
DGS-3450:admin# create authentication guest_vlan vlan guestVLAN
Command: create authentication guest_vlan vlan guestVLAN

Success.

DGS-3450:admin#
```

delete authentication guest_vlan

Purpose	Used to delete guest VLAN configuration.
Syntax	delete authentication guest_vlan [vlan <vlan_name 32> vlanid <vlanid 1-4094>]
Description	The delete guest_vlan command will delete guest VLAN setting, but won't delete the static VLAN. All ports which enable guest VLAN will move to original VLAN after deleting guest VLAN. For further description of this command please see description for config authentication guest_vlan ports.
Parameters	<i><vlan_name 32></i> - Specify the guest VLAN by VLAN name. <i>vlanid</i> - Specify the guest VLAN by VLAN ID.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete an authentication guest VLAN:

```
DGS-3450:admin# delete authentication guest_vlan vlan guestVLAN
Command: delete authentication guest_vlan vlan guestVLAN

Success.

DGS-3450:admin#
```

config authentication guest_vlan ports

Purpose	Used to configure security port(s) as specified guest VLAN member.
Syntax	config authentication guest_vlan [vlan <vlan_name 32> vlanid <vlanid 1-4094>] [add delete] ports [<portlist> [all]
Description	Used to configure security port(s) as specified guest VLAN member.
Parameters	<i>vlan_name</i> - Assigned a VLAN as guest VLAN. The VLAN must be an existed static VLAN. <i>vlanid</i> - Assigned a VLAN as guest VLAN. The VLAN must be an existed static VLAN. <i>add</i> - Specifies to add port list to the guest VLAN. <i>delete</i> - Specifies to delete port list from the guest VLAN. <i>portlist</i> - Specify the configured port(s).
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure an authentication guest VLAN:

```
DGS-3450:admin# config authentication guest_vlan vlan gv add ports all
Command: config authentication guest_vlan vlan gv add ports all

Success.

DGS-3450:admin#
```

config authentication ports

Purpose	Used to configure security port(s).
Syntax	config authentication ports [<portlist> all] {auth_mode [port_based host_based {vlanid <vidlist> state [enable disable] }]} multi_authen_methods[none any dot1x_impb impb_jwac]} (1)
Description	The user can use this command to configure authorization mode and authentication method on ports.
Parameters	<p><i>portlist</i> - Specify port(s) to configure.</p> <p><i>auth_mode</i> - <i>port_based</i> - If one of the attached hosts passes the authentication, all hosts on the same port will be granted to access network. If the user fails to authorize, this port will keep trying the next authentication</p> <p><i>host_based</i> - Every user can be authenticated individually. V2.01 and later, can authenticate client on specific authentication VLAN(s).</p> <p><i>vlanid</i> - Specific authentication VLAN(s).</p> <p><i>enable</i> - Assign the specified VID list as authentication VLAN(s).</p> <p><i>disable</i> - Remove the specified VID list from authentication VLAN(s).</p> <p>If "vlanid" is not specified, or all VLANs is disabled, means do not care which VLAN the client comes from, the client will be authenticated if the client's MAC (not care the VLAN) is not authenticated. After the client is authenticated, the client will not be re-authenticated when received from other VLANs.</p> <p>All VLANs are disabled by default.</p> <p>NOTE: When port's authorization mode is changed to port based, previously authentication VLAN(s) on this port will be clear.</p> <p><i>multi_authen_methods</i> - Specifies the method for compound authentication.</p> <p><i>none</i> - Compound authentication is not enabled,</p> <p>For project that support single authentication mode, the authentication method is defined by individual authentication module.</p> <p>For project that does not support single authentication mode, access authentication is disabled on the port.</p> <p><i>any</i> - If any one of the authentication method (802.1X, MAC-AC, WAC and JWAC) passes, then pass.</p> <p><i>dot1x_impb</i> - Dot1x will be verified first, and then IMPB will be verified. Both authentication need to be passed.</p> <p><i>impb_jwac</i> - JWAC will be verified first, and then IMPB will be verified. Both authentication need to be passed.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

The following example sets authorization mode and authentication VLAN for all port:

```
DGS-3450:admin# config authentication ports all auth_mode host_based vlanid 1-3 state enable
Command: config authentication ports all auth_mode host_based vlanid 1-3 state enable

Success.

DGS-3450:admin#
```

show authentication guest_vlan

Purpose	Used to show guest VLAN setting.
Syntax	show authentication guest_vlan
Description	The show guest VLAN command allows you to show the information of guest VLAN.
Parameters	None.
Restrictions	None.

Example usage:

This example displays the guest VLAN setting:

```
DGS-3450:admin# show authentication guest_vlan
Command: show authentication guest_vlan

Guest VLAN VID          : 1
Guest VLAN Member Ports : 4

Guest VLAN VID          : 3
Guest VLAN Member Ports : 1,8

Total Entries: 2

DGS-3450:admin#
```

show authentication ports

Purpose	Used to display authentication setting on port(s).
Syntax	show authentication ports {<portlist>}
Description	User can use this command to display authentication method and authorization mode on ports.
Parameters	<i>portlist</i> - Display compound authentication on specify port(s). If not specify the port, displays compound authentication setting of all ports.
Restrictions	None.

Example usage:

This example displays authentication setting for all ports:

```
DGS-3450:admin# show authentication ports
Command: show authentication ports

Port   Methods           Auth Mode  Authentication VLAN(s)
-----
 1      None              Host based 1,3,5,9,11,88,16
                                     18,56
 2      Any               Port based
 3      802.1X_IMPBB     Host based
 4      None              Host based 2000,2005
 5      IMPB_JWAC        Port based
 6      None              Host based
 7      None              Host based 1-20
 8      802.1X_IMPBB     Host based
 9      None              Host based

DGS-3450:admin#
```

enable authorization

Purpose	The enable authorization command will enable authorization.
Syntax	enable authorization attributes
Description	Used to enable authorization attributes. When the authorization for attributes is enabled, whether the authorized attributes (for example VLAN, 802.1p default priority, and ACL) assigned by the RADIUS server or local database will be accepted which depends on the individual module's setting. Authorization for attributes is enabled by default.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

This example sets authorization global state enabled:

```
DGS-3450:admin# enable authorization attributes
Command: enable authorization attributes

Success.

DGS-3450:admin#
```

disable authorization

Purpose	The disable authorization command will disable authorization.
Syntax	disable authorization attributes
Description	Used to disable authorization attributes. When the authorization for attributes is disabled, the authorized attributes (for example VLAN, 802.1p default priority, and ACL) assigned by the RADIUS server or local database will be ignored even if the individual module's setting is enabled. Authorization for attributes is enabled by default.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

This example sets authorization global state disabled:

```
DGS-3450:admin# disable authorization attributes
Command: disable authorization attributes

Success.

DGS-3450:admin#
```

show authorization

Purpose	Used to show authorization status.
Syntax	show authorization
Description	Used to show authorization status.
Parameters	None.
Restrictions	None.

Example usage:

This example displays authorization status:

```
DGS-3450:admin# show authorization
Command: show authorization

Authorization for Attributes: Enabled.

DGS-3450:admin#
```

config authentication server failover

Purpose	Used to configure authentication server failover function.
Syntax	config authentication server failover [local permit block]
Description	<p>Description</p> <p>When authentication server fails, administrator can configure to:</p> <ul style="list-style-type: none"> • Use local DB to authenticate the client <ul style="list-style-type: none"> ○ The switch will resort to using local database to authenticate the client. If the client fails on local authentication, the client is regarded as un-authenticated, otherwise, it authenticated. • Pass authentication <ul style="list-style-type: none"> ○ The client is always regarded as authenticated. If guest VLAN enabled, client will stay at guest VLAN, otherwise, it will stay at original VLAN. • Block the client (default setting) <ul style="list-style-type: none"> ○ The client is always regarded as un-authenticated.
Parameters	<p><i>local</i> - Use local DB to authenticate the client.</p> <p><i>permit</i> - The client is always regarded as authenticated.</p> <p><i>block</i> - Block the client (Default setting)</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

Set authentication server auth fail over state:

```
DGS-3450:admin# config authentication server failover local
Command: config authentication server failover local

Success.

DGS-3450:admin#
```

show authentication

Purpose	Used to show authentication global configuration.
Syntax	show authentication
Description	Used to show authentication global configuration.
Parameters	None.
Restrictions	None.

Example usage:

To show authentication:

```
DGS-3450:admin# show authentication
Command: show authentication

Authentication Server Failover: Block.

DGS-3450:admin# show authentication
Command: show authentication

Authentication Server Failover: Permit.

DGS-3450:admin# show authentication
Command: show authentication

Authentication Server Failover: Local.

DGS-3450:admin#
```

CONFIGURATION COMMANDS

Configuration function is used to conserve several configuration files in switch. With configuration function, user could conserve several same configurations in switch, one for currently use, other for back up, and user could conserve several different configurations in switch for different condition use.

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

Command	Parameters
download cfg_fromTFTP	[<ipaddr> <ipv6addr> <domain_name 255>] src_file <path_filename 64> {[<config_id 1-2> increment]}
upload cfg_toTFTP	[<ipaddr> <ipv6addr> <domain_name 255>] dest_file <path_filename 64> {<config_id 1-2>} {[include exclude begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}} {[include exclude begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}} {[include exclude begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}}}]}
show config	[current_config { [include exclude begin] <filter_string 80> {<filter_string 80>{<filter_string 80>}} { [include exclude begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}} { [include exclude begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}}}] config_in_nvram <config_id 1-2> { [include exclude begin] <filter_string 80> {<filter_string 80>{<filter_string 80>}} { [include exclude begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}} { [include exclude begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}}}] information]
config configuration	config_id <config_id 1-2> [delete boot_up active]
save config	<config_id 1-2>

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

download cfg_fromTFTP

Purpose	Used to down load a switch configuration file from TFTP server
Syntax	download cfg_fromTFTP [<ipaddr> <ipv6addr> <domain_name 255>] src_file <path_filename 64> {[<config_id 1-2> increment]}
Description	This command is used to download a config file from a TFTP server. For projects that support file system, the stored file name must be specified, for projects that support multiple configurations, the configuration ID can be specified. If the configuration ID is not specified, the boot up configuration is implied.
Parameters	<p><i>ipaddr</i> - The IPv4 address of the TFTP server.</p> <p><i>ipv6addr</i> - The IPv6 address of the TFTP server.</p> <p><i>domain_name</i> - The domain name of the host.</p> <p><i>src_file</i> - The pathname specifies the DOS pathname on the TFTP server. It can be a relative pathname or an absolute pathname.</p> <p><i>config_id</i> - Specifies the configuration file ID. If config_id is not specified, it refers to the boot up configuration file.</p> <p><i>increment</i> - If increment is specified, then the existing configuration will not be cleared before applying of the new configuration. If it is not specified, then the existing configuration will be cleared before applying of the new configuration.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To download the configuration file “desxxxx.cfg” from TFTP server at IP address 10.54.71.1:

```
DGS-3450:admin# download cfg_fromTFTP 10.54.71.1 src_file desxxxx.cfg
Command: download cfg_fromTFTP 10.54.71.1 src_file desxxxx.cfg

Connecting to server..... Done.
Download configuration..... Done.

DGS-3450:admin#
```

To download configuration file from TFTP server tftp.cfgmngmt.com:

```
DGS-3450:admin# download cfg_fromTFTP tftp.cfgmngmt.com src_file desxxxx.cfg
Command: download cfg_fromTFTP tftp.cfgmngmt.com src_file desxxxx.cfg

Connecting to server..... Done.
Download configuration..... Done.

DGS-3450:admin#
```

upload cfg_toTFTP

Purpose	Used to upload a configuration file from device to TFTP server.
Syntax	upload cfg_toTFTP [<ipaddr> <ipv6addr> <domain_name 255>] dest_file <path_filename 64> {<config_id 1-2>} {[include exclude begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}} {[include exclude begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}} {[include exclude begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}}}}
Description	<p>Used to upload a configuration file from the device to the TFTP server. Note that, for stacking system, only the master’s configuration file is allowed to be uploaded.</p> <p>The output stream of the configuration data can be filtered by the expression specified at the end of the command. The expression can contain up to three multiple filter evaluations. A filter evaluation begins with a filter type (include, exclude, and begin), followed by up to three filter strings (ex: “stp”). A filter string is enclosed by symbol “. The following describes the meaning of the each filter type.</p> <p>include: includes lines that contain the specified filter string. exclude: excludes lines that contain the specified filter string begin: The first line that contains the specified filter string will be the first line of the output.</p> <p>The relationship of multiple filter strings following the same filter type is OR. That is, one line is qualified if one of specified filter strings is matched. If more than one filter evaluation is specified; the output of filtered by the former evaluation will be used as the input of the latter evaluation.</p> <p>For example, if the following expression is specified include “stp” exclude “port” The result of the above example is all lines that include the “stp” string but exclude the “port” string.</p>
Parameters	<p><i>ipaddr</i> - The IPv4 address of the TFTP server. <i>ipv6addr</i> - The IPv6 address of the TFTP server. <i>domain_name</i> - The domain name of the host.</p>

upload cfg_toTFTP

dest_file - The pathname specifies the DOS pathname on the TFTP server. It can be a relative pathname or an absolute pathname.

config_id - Specifies the configuration file ID. If configuration ID is not specified, it refers to the boot up configuration file.

filter_string - A filter string is enclosed by symbol ". Thus, the filter string itself cannot contain the "character. The filter string is case sensitive.

Restrictions Only Administrator and Operator-level users can issue this command.

Example usage:

To upload the boot up configuration file to TFTP server and save as "cfg":

```
DGS-3450:admin# upload cfg_toTFTP 10.48.74.121 dest_file c:\cfg\DGS-XXXXS\cfg
Command: upload cfg_toTFTP 10.48.74.121 dest_file c:\cfg\DGS-XXXXS\cfg
```

```
Connecting to server... Done.
Upload Configuration... Done.
```

```
DGS-3450:admin#
```

In case that the designated file does not exist:

```
DGS-3450:admin# upload cfg_toTFTP 10.48.74.121 dest_file c:\cfg\DGS-XXXXS\cfg
Command: upload cfg_toTFTP 10.48.74.121 dest_file c:\cfg\DGS-XXXXS\cfg
```

```
The designated file does not exist.
Abort.
```

```
DGS-3450:admin#
```

show config

Purpose Display the content of the current configuration, the configuration to be used in next boot, or the configuration file specified by the command.

Syntax **show config current_config** [current_config { [include | exclude | begin] <filter_string 80> {<filter_string 80>{<filter_string 80>}}{ [include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}}}{ [include | exclude | begin] <filter_string 80> {<filter_string 80>}}}]config_in_nvram <config_id 1-2> { [include | exclude | begin] <filter_string 80> {<filter_string 80>{<filter_string 80>}}{ [include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}}}{ [include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}}}] information]

Description Display the content of the current configuration, the configuration to be used in next boot, or the configuration file specified by the command.

The output stream of the configuration data can be filtered by the expression specified at the end of the command. The expression can contain up to three multiple filter evaluations. A filter evaluation begins with a filter type (include, exclude, and begin), followed by up to three filter strings (ex: "stp"). A filter string is enclosed by symbol ". The following describes the meaning of the each filter type.

include: includes lines that contain the specified filter string.

exclude: excludes lines that contain the specified filter string

begin: The first line that contains the specified filter string will be the first line of the output.

show config

The relationship of multiple filter strings following the same filter type is OR. That is, one line is qualified if one of specified filter strings is matched.

If more than one filter evaluation is specified; the output of filtered by the former evaluation will be used as the input of the latter evaluation.

For example, if the following expression is specified, Include “stp” exclude “port”

The result of the above example is all lines that include the “stp” string but exclude the “port” string.

Parameters

current_config - Specifies the current configuration.

config_in_nvram - Specifies which configuration file. If the configuration ID is not specified, the boot up configuration is implied.

filter_string - A filter string is enclosed by symbol ". Thus, the filter string itself cannot contain the "character. The filter string is case sensitive.

Restrictions

Only Administrator and Operator-level users can issue this command.

Example usage:

The following example illustrates how the special filters ‘account’ affect the configuration display:

```
DGS-3450:admin# show config current_config include "account"
Command: show config current_config include "account"

create account admin brent
config accounting service network state disable
config accounting service shell state disable
config accounting service system state disable

DGS-3450:admin#
```

config configuration

Purpose

Used to select a configuration file as the next boot up configuration or to apply a specific configuration to the system. This command is required when multiple configuration files are supported.

Syntax

config configuration config_id <config_id 1-2> [delete | boot_up | active]

Description

Used to select a configuration file as the next boot up configuration or to apply a specific configuration to the system. This command is required when multiple configuration files are supported.

Parameters

config_id - Specifies which configuration file.

delete - Specifies to delete the configuration.

boot_up - Specifies it as a boot up file.

active - Specifies to apply the configuration.

Restrictions

Only Administrator and Operator-level users can issue this command.

Example usage:

To configure configuration as boot-up 1:

```
DGS-3450:admin#config configuration 1 boot_up
Command: config configuration 1 boot_up

Success.

DGS-3450:admin#
```

save config

Purpose	Used to save the current configuration to a file.
Syntax	save {config <config_id 1-2>}
Description	Used to save the current configuration to a file. This command is required to be supported regardless of whether file system is supported or whether multiple configuration files are supported. The configuration will only save to the master unit.
Parameters	<i>config_id</i> - Specifies the configuration file ID. If configuration ID is not specified, it refers to the boot up configuration file.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To save the configuration:

```
DGS-3450:admin#save config 1
Command: save config

Saving configuration 1 to NV-RAM..... Done.

DGS-3450:admin#
```

COUNTER COMMANDS

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

Command	Parameters
show packet ports	<portlist>
show error ports	<portlist>
show utilization ports	
clear counters	{ports <portlist>}

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

show packet ports

Purpose	Used to show statistics about the packets which were sent and received by the switch.
Syntax	show packet ports <portlist>
Description	The show packet ports command shows statistics about the packets which were sent and received by the switch.
Parameters	<i>portlist</i> - Specifies a range of ports to be displayed. (Unit ID: port number).
Restrictions	None.

Example usage:

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


```
DGS-3450:admin# show packet ports 2:7
```

```
Command: show packet ports 2:7
```

```
Port number : 2:7
```

Frame Size/Type	Frame Counts	Frames/sec
64	0	0
65-127	0	0
128-255	0	0
256-511	0	0
512-1023	0	0
1024-1518	0	0
1519-1522	0	0
1519-2047	0	0
2048-4095	0	0
4096-9216	0	0
Unicast RX	0	0
Multicast RX	0	0
Broadcast RX	0	0
Frame Type	Total	Total/sec
RX Bytes	0	0
RX Frames	0	0
TX Bytes	0	0
TX Frames	0	0

show error ports

Purpose	Use to show error statistics information for a range of ports.
Syntax	show error ports <portlist>
Description	The show error ports command shows error statistics for a range of ports.
Parameters	<i>portlist</i> - Specifies a range of ports to be displayed. (Unit ID: port number).
Restrictions	None.

Example usage:

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

```
DGS-3450:admin# show error ports 1:3
```

```
Command: show error ports 1:3
```

```
Port number : 1:3
```

RX Frames		TX Frames	
CRC Error	0	Excessive Deferral	0
Undersize	0	CRC Error	0
Oversize	0	Late Collision	0
Fragment	0	Excessive Collision	0
Jabber	0	Single Collision	0
Drop Pkts	0	Collision	0
Buffer Full Drop	0		
ACL Drop	0		
Multicast Drop	0		
VLAN Ingress Drop	0		

show utilization

Purpose	Use to show real-time port utilization statistics.
Syntax	show utilization ports {<portlist>}
Description	The show utilization command displays real-time ports utilization statistics.
Parameters	<i>portlist</i> - Specifies a range of ports to be displayed. (Unit ID: port number).
Restrictions	None.

Example usage:

To show the ports utilization:

```
DGS-3450:admin# show utilization ports
Command: show utilization ports
```

Port	TX/sec	RX/sec	Util	Port	TX/sec	RX/sec	Util
1:1	0	0	0	1:22	0	0	0
1:2	0	0	0	1:23	0	0	0
1:3	0	0	0	1:24	0	0	0
1:4	0	0	0	1:25	0	0	0
1:5	0	0	0	1:26	19	49	1
1:6	0	0	0	2:1	0	0	0
1:7	0	0	0	2:2	0	0	0
1:8	0	0	0	2:3	0	0	0
1:9	0	0	0	2:4	0	0	0
1:10	0	0	0	2:5	0	0	0
1:11	0	0	0	2:6	0	0	0
1:12	0	0	0	2:7	0	30	1
1:13	0	0	0	2:8	0	0	0
1:14	0	0	0	2:9	30	0	1
1:15	0	0	0	2:10	0	0	0
1:16	0	0	0	2:11	0	0	0
1:17	0	0	0	2:12	0	0	0
1:18	0	0	0	2:13	0	0	0
1:19	0	0	0	2:14	0	0	0
1:20	0	0	0	2:15	0	0	0
1:21	0	0	0	2:16	0	0	0

clear counter

Purpose	Used to clear the switch's statistics counters.
Syntax	clear counters {ports <portlist>}
Description	The clear counters command clears the switch's statistics counters.
Parameters	<i>portlist</i> - Specifies a range of ports to be configured. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and the end of the port list range are separated by a dash.

For example:

1:3 would specify unit 1, port 3;

2:4 specifies unit 2, port 4;

1:3-2:4 specifies all of the ports between unit 1, port 3 and unit 2, port 4 – in numerical order.

clear counter

If no parameter is specified, system will counter all of the ports.

Restrictions

Only Administrator and Operator-level users can issue this command.

Example usage:

To clear the switch's statistics counters:

```
DGS-3450:admin# clear counters ports 2:7-2:9
```

```
Command: clear counters ports 2:7-2:9
```

```
Success.
```

```
DGS-3450:admin#
```

DEBUG COMMANDS

Software Debug is used to define the common behavior of each module's debug function and collect and save basic OS information when exceptions happen.

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

Command	Parameters
debug error_log	[dump clear upload_toTFTP <ipaddr> <path_filename 64>]
debug buffer	[utilization dump clear upload_toTFTP <ipaddr> <path_filename 64>]
debug output	[module <module_list> all] [buffer console]
debug config error_reboot	[enable disable]
debug show status	{ module <module_list> }
debug config state	[enable disable]
debug show error_reboot state	

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

debug error_log

Purpose	Use this command to dump, clear or upload the software error log to a TFTP server.
Syntax	debug error_log [dump clear upload_toTFTP <ipaddr> <path_filename 64>]
Description	Dump, clear or upload the debug log to a TFTP server. The "error log" here refers to the software error log stored in NVRAM.
Parameters	<p><i>dump</i> - Display the debug message of the debug log.</p> <p><i>clear</i> - Clear the debug log.</p> <p><i>upload_toTFTP</i> - Upload the debug log to a TFTP server specified by IP address.</p> <p><i><ipaddr></i> - Specifies the IPv4 address of the TFTP server.</p> <p><i><path_filename 64></i> - The pathname specifies the DOS pathname on the TFTP server. It can be a relative pathname or an absolute pathname.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To dump the error log:

```
DGS-3450:admin# debug error_log dump
Command: debug error_log dump

*****
# debug log: 1
# level: fatal
# clock: 10000ms
# time : 2010/03/11 13:00:00

===== SOFTWARE FATAL ERROR =====
Invalid mutex handle : 806D6480

Current TASK : bcmARL.0

----- TASK STACKTRACE -----
->802ACE98
->8018C814
->8028FF44
->8028352C
->801D703C
->8013B8A4
->802AE754
->802A5E0C
->802A5D6C

-----
TASK  NAME  StackTop  CurStkSP  StackSize  SchCnt  PRIO(I)  STATUS
8069E7D0  FWD-ETH  823E9798  823E95C4  1K/ 32K   2    160/160  Q:IP_PKT
806A3E70  SysLogTask  80BD040C  80BD0298  1K/ 16K   3    180/180
          E:SysLogEvent
806A4340  PktStorm  80BF3188  80BF2DAC  2K/ 16K   807E4  190/190
          Q:ST_Storm
```

To clear the error log:

```
DGS-3450:admin# debug error_log clear
Command: debug error_log clear

Success.

DGS-3450:admin#
```

To upload the error log to TFTP server:

```
DGS-3450:admin# debug error_log upload_toTFTP 10.0.0.90 debug-log.txt
Command: debug error_log upload_toTFTP 10.0.0.90 debug-log.txt

Connecting to server..... Done.
Upload error log      ..... Done.

DGS-3450:admin#
```

debug buffer

Purpose	Use this command to show the debug buffer's state, or dump, clear, or upload the debug buffer to a TFTP server.
Syntax	debug buffer [utilization dump clear upload_toTFTP <ipaddr> <path_filename 64>]
Description	Show the debug buffer's state or dump, clear or upload the debug buffer to TFTP server. The "buffer" here refers to the module debug message stored in RAM.
Parameters	<p><i>utilization</i> - Display the debug buffer's state.</p> <p><i>dump</i> - Display the debug message in the debug buffer.</p> <p><i>clear</i> - Clear the debug buffer.</p> <p><i>upload_toTFTP</i> - Upload the debug buffer to a TFTP server specified by IP address.</p> <p><i><ipaddr></i> - Specifies the IPv4 address of the TFTP server.</p> <p><i><path_filename 64></i> - The pathname specifies the DOS pathname on the TFTP server. It can be a relative pathname or an absolute pathname.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To show the debug buffer's state:

```
DGS-3450:admin# debug buffer utilization
Command: debug buffer utilization

Allocate from      :      System memory
Total size       :      2 MB
Utilization rate  :      30%

DGS-3450:admin#
```

To clear the debug buffer:

```
DGS-3450:admin# debug buffer clear
Command: debug buffer clear

Success.

DGS-3450:admin#
```

To upload the messages stored in debug buffer to TFTP server:

```
DGS-3450:admin# debug buffer upload_toTFTP 10.0.0.90 debugcontent.txt
Command: debug buffer upload_toTFTP 10.0.0.90 debugcontent.txt

Connecting to server..... Done.
Upload debug file      ..... Done.

DGS-3450:admin#
```

debug output

Purpose	Use the command to set a specified module's debug message output to debug buffer or local console. If the user uses the command in a Telnet session, the error message also is output to the local console.
Syntax	debug output [module <module_list> all] [buffer console]

debug output

Description	Set specified module's debug message output to debug buffer or local console.
Parameters	<p><i><module_list></i> - The module list.</p> <p><i>all</i> - Control output method of all modules.</p> <p><i>buffer</i> - Direct the debug message of the module output to debug buffer(default).</p> <p><i>console</i> - Direct the debug message of the module output to local console.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To set all module debug message outputs to local console:

```
DGS-3450:admin# debug output all console
Command: debug output all console

Success.

DGS-3450:admin#
```

debug config error_reboot

Purpose	This command is used to set if the switch needs to be rebooted when a fatal error occurs. When the error occurs, the watchdog timer will be disabled by the system first, and then all debug information will be saved in NVRAM. If the error_reboot is enabled, the watchdog shall be enabled after all information is stored into NVRAM.
Syntax	debug config error_reboot [enable disable]
Description	Set if the switch needs to be rebooted when a fatal error occurs.
Parameters	<p><i>enable</i> - Need reboot switch when fatal error happens.(if the project do not define the default setting, enable for default)</p> <p><i>disable</i> - Do not need reboot switch when fatal error happens, system will hang-up for debug and enter the debug shell mode for debug..</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To set the switch to not need a reboot when a fatal error occurs:

```
DGS-3450:admin# debug config error_reboot disable
Command: debug config error_reboot disable

Success.

DGS-3450:admin#
```

debug show status

Purpose	Use the command to show the specified module's debug status.
Syntax	debug show status { module <module_list> }
Description	<p>Show the debug handler state and the specified module's debug status.</p> <p>If the input module list is empty, the states of all registered modules which support debug module will be shown.</p>

debug show status

Parameters	<module_list> - The module list.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To show the specified module's debug state:

```
DGS-3450:admin# debug show status module MSTP
Command: debug show status module MSTP

Debug Global State: Enabled
MSTP : Enabled

DGS-3450:admin#
```

To show the debug state:

```
DGS-3450:admin# debug show status
Command: debug show status

Debug Global State: Enabled

SYS   : Enabled
OS    : Enabled
MSTP  : Enabled
ACL   : Disabled
CLI   : Enabled
SNMP  : Disabled
IGMP  : Enabled

DGS-3450:admin#
```

debug config state

Purpose	Use the command to set the state of the debug.
Syntax	debug config state [enable disable]
Description	Use the command to set the state of the debug.
Parameters	<i>enable</i> - Enable the debug state. <i>disable</i> - Disable the debug state.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To set the debug state to disabled:

```
DGS-3450:admin# debug config state disable
Command: debug config state disable

Success.

DGS-3450:admin#
```


debug show error_reboot state

Purpose	Use the command to show the error reboot status.
Syntax	debug show error_reboot state
Description	Show the error reboot status.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To show the error reboot status.

```
DGS-3450:admin# debug show error_reboot state
Command: debug show error_reboot state

Error Reboot: Enabled

DGS-3450:admin#
```

DHCP LOCAL RELAY COMMANDS

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

Command	Parameters
config dhcp_local _relay	vlan [<vlan_name 32> vlanid <vlanid>] state [enable disable]
enable dhcp_local_relay	
disable dhcp_local_relay	
show dhcp_local_relay	

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

config dhcp_local_relay

Purpose	Used to enable or disable DHCP local relay function to vlan.
Syntax	config dhcp_local _relay vlan [<vlan_name 32> vlanid <vlanid>] state [enable disable]
Description	The config dhcp_local_relay vlan command is used to enable /disable DHCP local relay function for specified vlan. When DHCP local relay is enabled for the VLAN, the DHCP packet will be relayed in broadcast way without change of the source MAC address and gateway address. DHCP option 82 will be automatically added.
Parameters	<i>vlan_name</i> - The name of the VLAN to be enabled DHCP local relay. <i>state</i> - Enable or disable DHCP local relay for specified vlan.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable DHCP local relay for default vlan:

```
DGS-3450:admin# config dhcp_local_relay vlan default state enable
Command: config dhcp_local_relay vlan default state enable

Success.

DGS-3450:admin#
```

enable dhcp_local_relay

Purpose	Used to enable the DHCP local relay function on the switch.
Syntax	enable dhcp_local_relay
Description	The enable dhcp_local _relay command globally enables the DHCP local relay function on the switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable the DHCP local relay function:

```
DGS-3450:admin# enable dhcp_local_relay
Command: enable dhcp_local_relay

Success.

DGS-3450:admin#
```

disable dhcp_local_relay

Purpose	Used to disable the DHCP local relay function on the switch.
Syntax	disable dhcp_local_relay
Description	The disable dhcp_local _relay command globally disables the DHCP local relay function on the switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable the DHCP local relay function:

```
DGS-3450:admin# disable dhcp_local_relay
Command: disable dhcp_local_relay

Success.

DGS-3450:admin#
```

show dhcp_local_relay

Purpose	Used to display the current DHCP local relay configuration.
Syntax	show dhcp_local_relay
Description	The show dhcp_local_relay command displays the current DHCP local relay configuration.
Parameters	None.
Restrictions	None.

Example usage:

To display local dhcp relay status:

```
DGS-3450:admin# show dhcp_local_relay
Command: show dhcp_local_relay

DHCP/BOOTP Local Relay Status           : Disabled
DHCP/BOOTP Local Relay VLAN List       : 1,3-4

DGS-3450:admin#
```

DHCP RELAY COMMANDS

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

Command	Parameters
config dhcp_relay	{hops <value 1-16> time <sec 0-65535>}
config dhcp_relay add	ipif <ipif_name 12> <ipaddr>
config dhcp_relay delete	ipif <ipif_name 12> <ipaddr>
config dhcp_relay option_82	{ state [enable disable] check [enable disable] policy [replace drop keep]
enable dhcp_relay	
disable dhcp_relay	
show dhcp_relay	{ipif <ipif_name 12>}
config dhcp_relay option_60 state	[enable disable]
config dhcp_relay option_60 add	string <mutiword 255> relay <ipaddr> [exact-match partial-match]
config dhcp_relay option_60 default	[relay <ipaddr> mode [relay drop]
config dhcp_relay option_60 delete	[string <mutiword 255> {relay <ipaddr>} ipaddress <ipaddr> all default {<ipaddr>}]
show dhcp_relay option_60	{[string <mutiword 255> ipaddress <ipaddr> default]}
config dhcp_relay option_61 state	[enable disable]
config dhcp_relay option_61 add	[mac_address <macaddr> string <mutiword 255>] [relay <ipaddr> drop]
config dhcp_relay option_61 default	[relay <ipaddr> drop]
config dhcp_relay option_61 delete	[mac_address <macaddr> string <mutiword 255> all]
show dhcp_relay option_61	

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

config dhcp_relay

Purpose	Used to configure the DHCP relay feature of the switch.
Syntax	config dhcp_relay { hops <value 1-16> time <sec 0-65535>}
Description	The config dhcp_relay command configures the DHCP relay feature of the switch.
Parameters	<p><i>hops</i> - Specifies the maximum number of relay hops that the DHCP/BOOTP packets can cross. The range is 1 to 16. The default value is 4. The DHCP packet will be dropped when the relay hop count in the received packet is equal to or greater than this setting.</p> <p><i>time</i> - The secs field in the DHCP packet must be equal to or greater than this setting to be relayed by the router. The default value is 0.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure DHCP relay status:

```
DGS-3450:admin# config dhcp_relay hops 4 time 2
Command: config dhcp_relay hops 4 time 2

Success.

DGS-3450:admin#
```

config dhcp_relay add

Purpose	Used to add an IP destination address to the switch's DHCP relay table. Used to configure a DHCP server for relay of packets.
Syntax	config dhcp_relay add ipif <ipif_name 12> <ipaddr>
Description	The config dhcp_relay add command adds an IP address as a destination to forward (relay) DHCP/BOOTP packets. This server IP can either have the same network address as the network address of this ipif or not. If the network address is different, the system will automatically route the relayed packet.
Parameters	<i>ipif</i> - The name of the IP interface which contains the IP address below. < <i>ipaddr</i> > - The DHCP/BOOTP server IP address.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To add a DHCP/BOOTP server to the relay table:

```
DGS-3450:admin# config dhcp_relay add ipif System 10.43.21.12
Command: config dhcp_relay add ipif System 10.43.21.12

Success.

DGS-3450:admin#
```

config dhcp_relay delete

Purpose	Used to delete one or all IP destination addresses from the switch's DHCP relay table.
Syntax	config dhcp_relay delete ipif <ipif_name 12> <ipaddr>
Description	The config dhcp_relay delete command is used to delete one or all of the IP destination addresses in the switch's relay table.
Parameters	<i>ipif</i> - The name of the IP interface which contains the IP address below. < <i>ipaddr</i> > - The DHCP/BOOTP server IP address.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete a DHCP/BOOTP server to the relay table:

```
DGS-3450:admin# config dhcp_relay delete ipif System 10.43.21.12
Command: config dhcp_relay delete ipif System 10.43.21.12

Success.

DGS-3450:admin#
```

config dhcp_relay option_82

Purpose	Used to configure the processing of DHCP 82 option for the DHCP relay function.
Syntax	config dhcp_relay option_82 { state [enable disable] check [enable disable] policy [replace drop keep]}
Description	Configures the processing of DHCP 82 option for the DHCP relay function. When DHCP 82 option is enabled, the DHCP packet received from the client will be inserted with option 82 field before being relayed to the server. The DHCP 82 option contained 2 suboptions which is circuit ID suboption and remote ID suboption. The formats for the circuit ID suboption and the remote ID suboption are as following. For the circuit ID suboption of a standalone switch, the module field is always zero.
Parameters	<p><i>state</i> - When the state is enabled, the DHCP packet will be inserted with the option 82 field before being relayed to server. The DHCP packet will be processed based on the behaviour defined in check and policy setting. When the state is disabled, the DHCP packet will be relayed directly to server without further check and processing on the packet. The default setting is disabled.</p> <p><i>check</i> - When the state is enabled; For packet come from client side, the packet should not have the option 82's field. If the packet has this option field, it will be dropped. For packets come from the server side, the packet should have the option 82's field. If the packet does not have option field and does not have correct option fields, the packet will be dropped. The default setting is disabled.</p> <p><i>policy</i> - Specifies the way to process the packet come from the client side which has the 82 option field, and it is not dropped since the check function is disabled.</p> <p><i>replace</i> - Replace the exiting option 82 field in the packet.</p> <p><i>drop</i> - Discard if the packet has the option 82 field.</p> <p><i>keep</i> - Retain the existing option 82 field in the packet. The default setting is replace.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure dhcp_relay option 82:

```
DGS-3450:admin# config dhcp_relay option_82 state enable
Command: config dhcp_relay option_82 state enable

Success.

DGS-3450:admin# config dhcp_relay option_82 check disable
Command: config dhcp_relay option_82 check disable

Success.

DGS-3450:admin# config dhcp_relay option_82 policy replace
Command: config dhcp_relay option_82 policy replace

Success.

DGS-3450:admin#
```

enable dhcp_relay

Purpose	Used to enable the DHCP relay function on the switch.
Syntax	enable dhcp_relay
Description	The enable dhcp_relay command enables the DHCP relay function on the switch.

enable dhcp_relay

Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable the DHCP relay function:

```
DGS-3450:admin# enable dhcp_relay
Command: enable dhcp_relay

Success.

DGS-3450:admin#
```

disable dhcp_relay

Purpose	Used to disable DHCP relay function on the switch.
Syntax	disable dhcp_relay
Description	The disable dhcp_relay command disables the DHCP relay function on the switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable the DHCP relay function:

```
DGS-3450:admin# disable dhcp_relay
Command: disable dhcp_relay

Success.

DGS-3450:admin#
```

show dhcp_relay

Purpose	Used to display the current DHCP relay configuration.
Syntax	show dhcp_relay {ipif <ipif_name 12>}
Description	The show dhcp_relay command displays the current DHCP relay configuration.
Parameters	<i>ipif</i> - IP interface name. If no parameter specified, the system will display all dhcp relay configuration.
Restrictions	None.

Example usage:

To display dhcp relay status:

```
DGS-3450:admin# show dhcp_relay ipif System
Command: show dhcp_relay ipif System

DHCP/BOOTP Relay Status      : Disabled
DHCP/BOOTP Hops Count Limit  : 4
DHCP/BOOTP Relay Time Threshold : 0
DHCP Relay Agent Information Option 82 State : Disabled
DHCP Relay Agent Information Option 82 Check : Disabled
DHCP Relay Agent Information Option 82 Policy : Replace
DHCP Relay Agent Information Option 82 Remote ID : 00-80-11-00-11-22

Interface      Server 1      Server 2      Server 3      Server 4
-----
System         10.48.74.122 10.23.12.34  10.12.34.12  10.48.75.121

DGS-3450:admin#
```

config dhcp_relay option_60 state

Purpose	Used to config dhcp_relay option_60 state.
Syntax	config dhcp_relay option_60 state [enable disable]
Description	<p>This decides whether dhcp_relay will process the DHCP option 60 or not.</p> <p>When option_60 is enabled, if the packet does not have option 60, then the relay servers cannot be determined based on option 60. The relay servers will be determined based on either option 61 or per IPIF configured servers.</p> <p>If the relay servers are determined based on option 60 or option 61, then per IPIF configured servers will be ignored.</p> <p>If the relay servers are not determined either by option 60 or option 61, then per IPIF configured servers will be used to determine the relay servers.</p>
Parameters	<p><i>state</i> - See below:</p> <p><i>enable</i> - Enables the function dhcp_relay use option_60 rules to relay dhcp packet.</p> <p><i>disable</i> - Disables the function dhcp_relay use option_60 rules to relay dhcp packet.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the state of dhcp_relay option 60:

```
DGS-3450:admin# config dhcp_relay option_60 state enable
Command: config dhcp_relay option_60 state enable

Success

DGS-3450:admin#
```

config dhcp_relay option_60 add

Purpose	Used to add a entry for DHCP Relay option 60.
Syntax	config dhcp_relay option_60 add string <mutiword 255> relay <ipaddr> [exact-match partial-match]
Description	<p>This command configures the option 60 relay rules. Note that different string can be specified with the same relay server, and the same string can be specified with multiple relay servers.</p> <p>The system will relay the packet to all the matching servers.</p>

config dhcp_relay option_60 add

Parameters	<p><i>string</i> - The specified string.</p> <p><i>relay</i> - Specify a relay server IP address.</p> <p><i>exact-match</i> - The option 60 string in the packet must full match with the specified string.</p> <p><i>partial-match</i> - The option 60 string in the packet only need partial match with the specified string.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To add a entry for DHCP Relay option 60:

```
DGS-3450:admin# config dhcp_relay option_60 add string "abc" relay 10.90.90.1 exact-match
Command: config dhcp_relay option_60 add string "abc" relay 10.90.90.1 exact-match

Success

DGS-3450:admin#
```

config dhcp_relay option_60 default

Purpose	This command is used to configure the DHCP Relay option 60 as the default Relay Server.
Syntax	config dhcp_relay option_60 default [relay <ipaddr>] mode [relay drop]
Description	<p>When there are no match servers found for the packet based on option 60, the relay servers will be determined by the default relay server setting.</p> <p>When there is no matching found for the packet, the relay servers will be determined based on the default relay servers.</p> <p>When drop is specified, the packet with no matching rules found will be dropped without further process.</p> <p>If the setting is no- drop, then the packet will be processed further based on option 61. The final relay servers will be the union of option 60 default relay servers and the relay servers determined by option 61.</p>
Parameters	<p><i>relay</i> - The specified IP address for dhcp_relay forward. Specify a relay server IP for the packet that has mathcing option 60 rules.</p> <p><i>drop</i> - Specify to drop the packet that has no matching option 60 rules.</p> <p><i>relay</i> - The packet will be relayed based on the relay rules.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the DHCP Relay option 60 as the default Relay Server:

```
DGS-3450:admin# config dhcp_relay option_60 default mode drop
Command: config dhcp_relay option_60 default mode drop

Success

DGS-3450:admin#
```

config dhcp_relay option_60 delete

Purpose	This command is used to delete the DHCP Relay option 60 entry.
---------	--

config dhcp_relay option_60 delete

Syntax	config dhcp_relay option_60 delete [string <mutiword 255> {relay <ipaddr>} ipaddress <ipaddr> all default {< ipaddr>}]
Description	This can delete the entry by user specified. When all is specified, all rules excluding the default rules are deleted.
Parameters	<i>string</i> - Delete all the entry whose string is equal to the string of specified if ipaddress is not specified <i>relay <ipaddr></i> - Delete one entry, whose string and IP address are equal to the string and IP address specified by the user. <i>all</i> - Delete all the entry. Default relay servers are excluded. <i>ipaddress</i> - Delete all the entry whose ipaddress is equal to the specified ipaddress. <i>default</i> - Delete all default relay ipaddress if ipaddress is not specified. <i><ipaddr></i> - Delete the default relay ipaddress that is specified by the user.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete the DHCP Relay option 60 entry:

```
DGS-3450:admin# config dhcp_relay option_60 delete string "abc" relay 10.90.90.1
Command: config dhcp_relay option_60 delete string "abc" relay 10.90.90.1
```

Success

```
DGS-3450:admin#
```

show dhcp_relay option_60

Purpose	This command is used to show the DHCP Relay option 60 entry.
Syntax	show dhcp_relay option_60 {[string <mutiword 255> ipaddress < ipaddr> default]}
Description	This show dhcp_relay option_60 entry by the user specified.
Parameters	<i>string</i> - Show the entry which's string equal the string of specified. <i>ipaddress</i> - Show the entry whose ipaddress equal the specified ipaddress. <i>default</i> - Show the default behaviour of dhcp_relay option60.
Restrictions	None.

Example usage:

To show the DHCP Relay option 60 entry:

```
DGS-3450:admin# show dhcp_relay option_60
Command: show dhcp_relay option_60
Default processing Mode: drop

Default Servers:
    10.90.90.100
    10.90.90.101
    10.90.90.102

Matching Rules:

String                Match Type            IP Address
-----
101                   Partial Match        110.1.1.4
102                   Partial Match        110.1.1.4
103                   Partial Match        110.1.1.4

Total Entries   : 3

DGS-3450:admin#
```

config dhcp_relay option_61 state

Purpose	This command is used to configure the DHCP Relay option 61 state.
Syntax	config dhcp_relay option_61 state [enable disable]
Description	<p>This decides whether dhcp_relay will process the DHCP option 61 or not.</p> <p>When option_61 is enabled, if the packet does not have option 61, then the relay servers cannot be determined based on option 61.</p> <p>If the relay servers are determined based on option 60 or option 61, then per IPIF configured servers will be ignored.</p> <p>If the relay servers are not determined either by option 60 or option 61, then per IPIF configured servers will be used to determine the relay servers.</p>
Parameters	<p><i>state</i> - See below:</p> <p><i>enable</i> - Enable the function dhcp_relay use option_61 ruler to relay dhcp packet.</p> <p><i>disable</i> - Disable the function dhcp_relay use option_61 ruler to relay dhcp packet.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the state of dhcp_relay option 61:

```
DGS-3450:admin# config dhcp_relay option_61 state enable
Command: config dhcp_relay option_61 state enable

Success

DGS-3450:admin#
```

config dhcp_relay option_61 add

Purpose	This command is used to add a rule for DHCP Relay option 61.
Syntax	config dhcp_relay option_61 add [mac_address <macaddr> string <mutiword 255>] [relay <ipaddr> drop]

config dhcp_relay option_61 add

Description	This command adds a rule to determine the relay server based on option 61. The match rule can base on either MAC address or a user-specified string. Only one relay server can be specified for a MAC-address or a string, If relay servers are determined based on option 60, and one relay server is determined based on option 61, the final relay servers will be the union of these two sets of the servers.
Parameters	<i>mac_address</i> - The client's client-ID which is the hardware address of client. <i>string</i> - The client's client-ID, which is specified by administrator. <i>relay</i> - Specify to relay the packet to a IP address. <i>drop</i> - Specify to drop the packet.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To add a rule for DHCP Relay option 61:

```
DGS-3450:admin# config dhcp_relay option_61 add mac_address 00-11-22-33-44-55 drop
Command: config dhcp_relay option_61 add mac_address 00-11-22-33-44-55 drop

Success

DGS-3450:admin#
```

config dhcp_relay option_61 default

Purpose	This command is used to configure the default ruler for option 61.
Syntax	config dhcp_relay option_61 default [relay <ipaddr> drop]
Description	Up to default server IP address can be specified. This setting will be used to determine the rule to process those packets that have no option 61 matching rules. The default default-rule is drop.
Parameters	<i>relay</i> - Specify to relay the packet that has no option matching 61 matching rules to an IP address. <i>drop</i> - Specify to drop the packet that have no option 61 matching rules.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the default ruler for option 61:

```
DGS-3450:admin# config dhcp_relay option_61 default drop
Command: config dhcp_relay option_61 default drop

Success

DGS-3450:admin#
```

config dhcp_relay option_61 delete

Purpose	This command is used to delete an option 61 rule.
Syntax	config dhcp_relay option_61 delete [mac_address <macaddr> string <mutiword 255> all]

config dhcp_relay option_61 delete

Description	This command is used to delete an option 61 rule.
Parameters	<i>mac_address</i> - The entry with the specified MAC address will be deleted. <i>string</i> - The entry with the specified string will be deleted. <i>all</i> - All rules excluding the default rule will be deleted.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete an option 61 rule:

```
DGS-3450:admin# config dhcp_relay option_61 delete mac_address 00-11-22-33-44-55
Command: config dhcp_relay option_61 delete mac_address 00-11-22-33-44-55
```

Success

```
DGS-3450:admin#
```

show dhcp_relay option_61

Purpose	This command is used to show all rulers for option 61.
Syntax	show dhcp_relay option_61
Description	This command is used to show all rulers for option 61.
Parameters	None.
Restrictions	None,

Example usage:

To show all rulers for option 61:

```
DGS-3450:admin# show dhcp_relay option_61
Command: show dhcp_relay option_61
```

```
Default Relay Rule: 10.90.90.200
```

Matching Rules:

Client-ID	Type	Relay rule
-----	----	-----
00-0D-88-11-8B-6A	MAC Address	101.1.90.20
00-11-22-33-44-55	MAC Address	111.111.111.111
00-11-22-33-44-56	MAC Address	111.111.111.111

```
Total Entries: 3
```

```
DGS-3450:admin#
```

DHCP SERVER SCREENING COMMANDS

The DHCP Server Screening Commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

The DHCP Server Screening commands allow you not only to restrict all DHCP Server packets but also to receive any specified DHCP server packets by any specified DHCP client, it is useful when one or more than one DHCP servers are present on the network and both provide DHCP services to different distinct groups of clients. Enabling the DHCP filter for the first time will create both an access profile and access rule per port, following this other access rules can be created. These rules are used to block all DHCP server packets. Similarly, the addition of a permit DHCP entry will create one access profile and one access rule the first time the DHCP client MAC address is the client MAC address, and the Source IP address is the same as the DHCP server's IP address (UDP port number 67). These rules are used to permit the DHCP server packets with specific fields, which the user configures.

When the DHCP Server filter function is enabled, all DHCP Server packets will be filtered from a specific port. Also, you are allowed to create entries for specific port-based Server IP address and Client MAC address binding entries. Be aware that the DHCP Server filter function must be enabled first. Once all settings are complete, all DHCP Server packets will be filtered from a specific port except those that meet the Server IP Address and Client MAC Address binding.

Command	Parameters
config filter dhcp_server	[add permit server_ip <ipaddr> {client_mac <macaddr>} ports [<portlist> all] delete permit server_ip <ipaddr> {client_mac <macaddr>} ports [<portlist> all] ports [<portlist> all] state [enable disable]]
show filter dhcp_server	
config filter dhcp_server trap_log	[enable disable]
config filter dhcp_server illegal_server_log_suppress_duration	[1min 5min 30min]

Each command is listed in detail in the following sections.

config filter dhcp_server

Purpose	DHCP server packets except those that have been IP/client MAC bound will be filtered. This command is used to configure the state of the function for filtering of DHCP server packet and to add/delete the DHCP server/client binding entry.
Syntax	config filter dhcp_server [add permit server_ip <ipaddr> {client_mac <macaddr>} ports [<portlist> all] delete permit server_ip <ipaddr> {client_mac <macaddr>} ports [<portlist> all] ports [<portlist> all] state [enable disable]]
Description	This command has two purposes: to filter all DHCP server packets on the specified port(s) and to allow some DHCP server packets to be forwarded if they are on the pre-defined server IP address/MAC address binding list. Thus the DHCP server can be restricted to service a specified DHCP client. This is useful when there are two or more DHCP servers present on a network.
Parameters	<p><i>ipaddr</i> – The IP address of the DHCP server to be filtered.</p> <p><i>macaddr</i> – The MAC address of the DHCP client.</p> <p><i>state</i> – To Enable/disable the filter DHCP server state.</p> <p><i>portlist</i> – The port list of filter DHCP server.</p>

config filter dhcp_server

Restrictions	<p>Only Administrator and Operator-level users can issue this command.</p> <p>Enabling the DHCP filter will create one access profile and create one access rule per port (UDP port 67).</p> <p>Addition of a DHCP filter permit entry will create one access profile and create one access rule (DA = client MAC address, SA = source IP address and UDP port 67).</p>
--------------	---

Example usage:

To add an entry from the DHCP server/client filter list in the switch's database:

```
DGS-3450:admin# config filter dhcp_server add permit server_ip 10.1.1.1 client_mac 00-00-00-00-00-01 ports 1:1-1:3
Command: config filter dhcp_server add permit server_ip 10.1.1.1 client_mac 00-00-00-00-00-01 ports 1:1-1:3

Success.

DGS-3450:admin#
```

To configure the filter DHCP server state:

```
DGS-3450:admin# config filter dhcp_server ports 1:1-1:3 state enable
Command: config filter dhcp_server ports 1:1-1:3 state enable

Success.

DGS-3450:admin#
```

show filter dhcp_server

Purpose	Used to display current DHCP server/client filter list created on the switch.
Syntax	Show filter dhcp_server
Description	This command is used to display DHCP server/client filter list created on the switch. The log ceasing unauthorized duration and the log/trap state.
Parameters	None.
Restrictions	None.

Example usage:

To display the DHCP server/client filter list created on the switch the log ceasing unauthorized duration and the log/trap state:

```
DGS-3450:admin# show filter dhcp_server
Command: show filter dhcp_server

Filter DHCP Server Trap_Log State: Disabled

  Enabled Ports: 1:1-1:3

Illegal Server Log Suppress Duration:5 minutes
Filter DHCP Server/Client Table
Server IP Address Client MAC Address  Port
-----
10.1.1.1          00-00-00-00-00-01  1:1-1:3

Total Entries: 1

DGS-3450:admin#
```

config filter dhcp_server trap_log

Purpose	Used to configure the trap and log related to the DHCP server filter.
Syntax	config filter dhcp_server trap_log [enable disable]
Description	Used to enable/disable trap/log related to DHCP server filter.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable log and trap for the DHCP server filter event:

```
DGS-3450:admin# config filter dhcp_server trap_log disable
Command: config filter dhcp_server trap_log disable

Success.

DGS-3450:admin#
```

config filter dhcp_server illegal_server_log_suppress_duration

Purpose	This function is used to configure the illegal server log suppress duration.
Syntax	config filter dhcp_server illegal_server_log_suppress_duration [1min 5min 30min]
Description	The DHCP server filtering function filters any illegal DHCP server packets. The DHCP server who sends the illegal packets will be logged. This command is used to suppress the logging of DHCP servers who continue to send illegal DHCP packets. The same illegal DHCP server IP address that is detected will be logged only once regardless of how many illegal packets are sent.
Parameters	<i>illegal_server_log_suppress_duration</i> – The log can be suppressed by 1 minute, 5 minutes or 30 minutes. The default value is 5 minutes.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the illegal_server_log_suppress_duration for 30 minutes:


```
DGS-3450:admin# config filter dhcp_server illegal_server_log_suppress_duration 30min
```

```
Command: config filter dhcp_server illegal_server_log_suppress_duration 30min
```

```
Success.
```

```
DGS-3450:admin#
```

DHCP SERVER COMMANDS

For this release, the Switch now has the capability to act as a DHCP server to devices within its locally attached network. DHCP, or Dynamic Host Configuration Protocol, allows the switch to delegate IP addresses, subnet masks, default gateways and other IP parameters to devices that request this information. This occurs when a DHCP enabled device is booted on or attached to the locally attached network. This device is known as the DHCP client and when enabled, it will emit query messages on the network before any IP parameters are set. When the DHCP server receives this request, it returns a response to the client, containing the previously mentioned IP information that the DHCP client then utilizes and sets on its local configurations.

The user can configure many DHCP related parameters that it will utilize on its locally attached network, to control and limit the IP settings of clients desiring an automatic IP configuration, such as the lease time of the allotted IP address, the range of IP addresses that will be allowed in its DHCP pool, the ability to exclude various IP addresses within the pool as not to make identical entries on its network, or to assign the IP address of an important device (such as a DNS server or the IP address of the default route) to another device on the network.

Users also have the ability to bind IP addresses within the DHCP pool to specific MAC addresses in order to keep consistent the IP addresses of devices that may be important to the upkeep of the network that require a static IP address.

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

Command	Parameters
create dhcp pool	<pool_name 12>
delete dhcp pool	[<pool_name 12> all]
create dhcp pool manual_binding	<pool_name 12> <ipaddr> hardware_address <macaddr> {type [Ethernet IEEE802]}
delete dhcp pool manual_binding	<pool_name 12> [<ipaddr> all]
show dhcp pool manual_binding	{<pool_name 12>}
show dhcp_binding	{<pool_name 12>}
clear dhcp_binding	{<pool_name 12>}
config dhcp ping_packets	<number 2-10>
config dhcp ping_timeout	<millisecond 500-2000>
config dhcp pool boot_file	<pool_name 12> <file_name 64>
config dhcp pool default_router	<pool_name 12> <ipaddr> {<ipaddr>} {<ipaddr>}
config dhcp pool dns_server_address	<pool_name 12> <ipaddr> {<ipaddr>} {<ipaddr>}
config dhcp pool domain_name	<pool_name 12> <domain_name 64>
config dhcp pool lease	<pool_name 12> [<day 0-365> <hour 0-23> <minute 0-59> infinite]
config dhcp pool netbios_name_server	<pool_name 12> <ipaddr> {<ipaddr>} {<ipaddr>}
config dhcp pool netbios_node_type	<pool_name 12> [broadcast peer_to_peer mixed hybrid]
config dhcp pool network_addr	<pool_name 12> <network_address>
config dhcp pool next_server	<pool_name 12> <ipaddr>
enable dhcp_server	
disable dhcp_server	
show dhcp_server	
create dhcp excluded_address begin_address	<ipaddr> end_address <ipaddr>
delete dhcp excluded_address	[begin_address <ipaddr> end_address <ipaddr> all]
show dhcp excluded_address	
show dhcp pool	{ <pool_name 12> }

Each command is listed in detail in the following sections.

create dhcp pool

Purpose	Used to create a DHCP pool.
Syntax	create dhcp pool <pool_name 12>
Description	This command will create a DHCP pool for the DHCP server. Once created, this pool may be modified for accepting DHCP clients into this pool.
Parameters	<pool_name 12> – Enter an name of up to 12 alphanumeric characters to identify the pool to be created with this command.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create the DHCP pool Floor2:

```
DGS-3450:admin# create dhcp pool Floor2
Command:create dhcp pool Floor2
```

Success.

```
DGS-3450:admin#
```

delete dhcp pool

Purpose	Used to delete a DHCP pool.
Syntax	delete dhcp pool [<pool_name 12> all]
Description	This command will delete a DHCP pool that was created with the create dhcp pool command.
Parameters	<pool_name 12> – Enter an name of up to 12 alphanumeric characters to identify the pool to be deleted with this command. all – Enter this command to delete all created DHCP pool.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete the DHCP pool Floor2:

```
DGS-3450:admin# delete dhcp pool Floor2
Command:delete dhcp pool Floor2
```

Success.

```
DGS-3450:admin#
```

create dhcp pool manual_binding

Purpose	Used to create a DHCP pool manual binding entry.
Syntax	create dhcp pool manual_binding <pool_name 12> <ipaddr> hardware_address <macaddr> {type [Ethernet IEEE802]}
Description	This command will create a DHCP manual pool binding entry for a previously created pool. When a MAC address is entered in this command, it will be bound to a IP address from the given pool either by the user, or automatically by the Switch.
Parameters	<p><i><pool_name 12></i> – Enter the name of the previously created pool that will contain the manual binding entry.</p> <p><i><ipaddr></i> – Enter the IP address to be statically bound to a device within the local network that will be specified by entering the Hardware Address in the following field.</p> <p><i>hardware_address <macaddr></i> – Enter the MAC address of the device to be statically bound to the IP address entered in the previous field.</p> <p><i>type [Ethernet IEEE802]</i> – This field is used to specify the type of connection for which this manually bound entry will be set. <i>Ethernet</i> will denote that the manually bound device is connected directly to the Switch, while the <i>IEEE802</i> denotes that the manually bound device is outside the local network of the Switch.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create a manual binding DHCP entry:

```
DGS-3450:admin# create dhcp pool manual_binding engineering 10.10.10.1 hardware_address
02.02.02.02.02 type Ethernet
Command: create dhcp pool manual_binding engineering 10.10.10.1 hardware_address
02.02.02.02.02 type Ethernet

Success.

DGS-3450:admin#
```

delete dhcp pool manual_binding

Purpose	Used to delete a previously created DHCP manual binding entry.
Syntax	delete dhcp pool manual_binding <pool_name 12> [<ipaddr> all]
Description	This command will delete a DHCP manual binding entry created with the create dhcp pool manual_binding command.
Parameters	<p><i><pool_name 12></i> – Enter the previously created pool name from which to delete a manual binding DHCP entry.</p> <p><i><ipaddr></i> – Enter the IP address of the manual binding entry to be deleted.</p> <p><i>all</i> – Enter this command to delete all manual binding entries for the given pool.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete a manual binding DHCP entry:

```
DGS-3450:admin# delete dhcp pool manual_binding Floor2 10.10.10.1
Command: delete dhcp pool manual_binding Floor2 10.10.10.1

Success.

DGS-3450:admin#
```

show dhcp pool manual_binding

Purpose	Used to display the manual binding settings for a DHCP pool.
Syntax	show dhcp pool manual_binding {<pool_name 12>}
Description	This command will display the manual binding entries for the selected DHCP pool.
Parameters	<pool_name 12> – Enter the name of the DHCP pool for which to view manual binding entries. Entering this command without the pool name will display all manual binding entries of the DHCP server.
Restrictions	None.

Example usage:

To display the manual binding entries of the DHCP pool accounting:

```
DGS-3450:admin# show dhcp pool manual_binding accounting
Command: show dhcp pool manual_binding accounting

Pool Name      IP Address      Identifier (Hardware_Address)  Type
-----
accounting     192.168.0.1    01-22-b7-35-ce-99             Ethernet
accounting     192.168.0.2    0a-52-f7-34-ce-88             Ethernet

Total Entries : 2

DGS-3450:admin#
```

show dhcp_binding

Purpose	Used to show the DHCP binding information.
Syntax	show dhcp_binding {<pool_name 12>}
Description	This command is used to display the DHCP binding information by created pool. Entering the command without the pool name will display all information regarding DHCP binding on the switch.
Parameters	<pool_name 12> – Enter the name of the DHCP pool for which to view binding information.
Restrictions	None.

Example usage:

To display the DHCP binding information on the Switch:

```
DGS-3450:admin# show dhcp_binding
```

```
Command:show dhcp_binding
```

Pool Name	IP Address	Hardware Address	Type	Status	Life Time (secs)
-----	-----	-----	-----	-----	-----
engineering	192.168.0.1	01-22-b7-35-ce-99	Ethernet	Manual	864000

```
Total Entries : 1
```

```
DGS-3450:admin#
```

clear dhcp_binding

Purpose	Used to clear the DHCP binding information.
Syntax	clear dhcp_binding {<pool_name 12>}
Description	This command is used to clear the DHCP binding settings for a particular created DHCP pool.
Parameters	<i><pool_name 12></i> – Enter the name of the DHCP pool for which to clear the binding information.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To display the DHCP binding information on the Switch:

```
DGS-3450:admin# clear dhcp_binding
```

```
Command:clear dhcp_binding
```

```
Success.
```

```
DGS-3450:admin#
```

config dhcp ping_packets

Purpose	Used to set the number of ping packets that will be sent out to find if an IP address is available.
Syntax	config dhcp ping_packets <number 2-10>
Description	This command will set the number of ping packets that will be sent out to find if an IP address is available to be allocated as a valid DHCP IP address.
Parameters	<i><number 2-10></i> – Enter a number between 2 and 10 to denote the number of ping packets that the Switch will send out on the network containing the IP address to be allotted. If the ping request is not returned, the IP address is considered unique to the local network and then allotted to the requesting client. The default setting is 2 packets.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the number of ping packets to be used for DHCP:

```
DGS-3450:admin# config dhcp ping_packets 2
Command: config dhcp ping_packets 2

Success.

DGS-3450:admin#
```

config dhcp ping_timeout

Purpose	Used to set the time the Switch will wait before timing out a ping packet.
Syntax	config dhcp ping_timeout <millisecond 500-2000>
Description	This command is used set the time the Switch will wait before timing out a ping packet. If no answer is received, the IP address is considered unused and may be allocated to a requesting client.
Parameters	<i><millisecond 500-2000></i> – The user may set a time between <i>500</i> and <i>2000</i> milliseconds that the Switch will wait before timing out a ping packet. The default setting is <i>500</i> milliseconds.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the Ping timeout:

```
DGS-3450:admin# config dhcp ping_timeout 500
Command: config dhcp ping_timeout 500

Success.

DGS-3450:admin#
```

config dhcp pool boot_file

Purpose	Used to specify the Boot File that will be used as the boot image of the DHCP client
Syntax	config dhcp pool boot_file <pool_name 12> <file_name 64>
Description	This command is used to specify the Boot File that will be used as the boot image of the DHCP client. This image is usually the operating system that the client uses to load its IP parameters.
Parameters	<i><pool_name 12></i> – Enter the previously created pool name from which the boot file will be set. <i><file_name 64></i> – Enter the name of the boot file that will be used for DHCP clients.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To set the boot file:

```
DGS-3450:admin# config dhcp pool boot_file accounting boot.had
Command: config dhcp pool boot_file accounting boot.had

Success.

DGS-3450:admin#
```


config dhcp pool default_router

Purpose	Used to configure the default router for the DHCP client.
Syntax	config dhcp pool default_router <pool_name 12> <ipaddr> {<ipaddr>} {<ipaddr>}
Description	This command is used to configure the default router for DHCP clients requesting DHCP information for the switch. Users may add up to three IP addresses to identify the router, but must specify at least one.
Parameters	<i><pool_name 12></i> – Enter the previously created pool name for which to add a default router. <i><ipaddr></i> – Enter the IP address for the default router for this pool. Users may specify up to three default routers but users must add at least one.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the default router:

```
DGS-3450:admin# config dhcp pool default_router accounting 10.245.32.1
Command: config dhcp pool default_router accounting 10.245.32.1
```

Success.

```
DGS-3450:admin#
```

config dhcp pool dns_server_address

Purpose	Used to configure the IP addresses of DNS servers for a specific DHCP pool.
Syntax	config dhcp pool dns_server_address <pool_name 12> <ipaddr> {<ipaddr>} {<ipaddr>}
Description	This command is used to configure the DNS server IP addresses for a specific DHCP pool for the switch. The DNS Server correlates IP addresses to host names when queried. Users may add up to three DNS Server addresses.
Parameters	<i><pool_name 12></i> – Enter the previously created pool name for which to add a DNS address. <i><ipaddr></i> – Enter the IP address for the DNS server for this pool. Users may specify up to three DNS servers.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the DNS server address for a DHCP pool:

```
DGS-3450:admin# config dhcp pool dns_server_address accounting 10.245.32.1
Command: config dhcp pool dns_server_address accounting 10.245.32.1
```

Success.

```
DGS-3450:admin#
```

config dhcp pool domain_name

Purpose	Used to configure the domain name for the DHCP pool of the Switch.
Syntax	config dhcp pool domain_name<pool_name 12> <domain_name 64>
Description	This command is used to configure the domain name for the DHCP pool of the Switch. This domain name represents a general group of networks that collectively make up the domain.
Parameters	<i><pool_name 12></i> – Enter the previously created pool name for which to add a default router. <i><domain_name 64></i> – The Domain Name may be an alphanumeric string of up to 64 characters.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the domain name for a DHCP pool:

```
DGS-3450:admin# config dhcp pool domain_name accounting d_link.com
Command: config dhcp pool domain_name accounting d_link.com
```

Success.

```
DGS-3450:admin#
```

config dhcp pool lease

Purpose	Used to configure the lease time of DHCP clients within a DHCP pool.
Syntax	config dhcp pool lease<pool_name 12> [<day 0-365> <hour 0-23> <minute 0-59> infinite]
Description	Using this command, the user can specify the lease time for the DHCP client. This time represents the amount of time that the allotted address is valid on the local network.
Parameters	<i><pool_name 12></i> – Enter the previously created pool name for which to set the lease time for accepted DHCP clients. <i>day 0-365</i> – Enter the amount of days for the lease. The default setting is one day. <i>hour 0-23</i> – Enter the number of hours for the lease. <i>minute 0-59</i> – Enter the number of minutes for the lease. <i>infinite</i> – Enter this parameter to set the allotted IP address to never be timed out of its lease.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the lease time for the DHCP pool:

```
DGS-3450:admin# config dhcp pool lease accounting infinite
Command: config dhcp pool lease accounting infinite
```

Success.

```
DGS-3450:admin#
```

config dhcp pool netbios_name_server

Purpose	Used to configure the IP address(es) for the Net BIOS name server,
Syntax	config dhcp pool netbios_name_server <pool_name 12> <ipaddr> {<ipaddr>}
{<ipaddr>}
Description	This command is used to enter the IP address of a Net BIOS Name Server that will be available to a Microsoft DHCP Client. This Net BIOS Name Server is actually a WINS (Windows Internet Naming Service) Server that allows Microsoft DHCP clients to correlate host names to IP addresses within a general grouping of networks. The user may establish up to three Net BIOS Name Servers.
Parameters	<pool_name 12> – Enter the previously created pool name for which to set the Net BIOS name server for DHCP clients. <ipaddr> – Enter the IP address for the Net BIOS name server for this pool. Users may specify up to three Net BIOS name servers.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the Net BIOS name server for the DHCP pool:

```
DGS-3450:admin# config dhcp pool netbios_name_server accounting 10.98.254.2
Command: config dhcp pool netbios_name_server accounting 10.98.254.2

Success.

DGS-3450:admin#
```

config dhcp pool netbios_node_type

Purpose	Used to set the Net BIOS node type for the DHCP server.
Syntax	config dhcp pool netbios_node_type <pool_name 12> [broadcast peer_to_peer mixed hybrid]
Description	This command is used to allow users to set the type of node server for the previously configured Net BIOS Name server. The user has four choices for node types which are <i>Broadcast</i> , <i>Peer to Peer</i> , <i>Mixed</i> and <i>Hybrid</i> .
Parameters	<pool_name 12> – Enter the previously created pool name for which to set the Net BIOS node type for DHCP clients. [broadcast peer_to_peer mixed hybrid] – Users may choose the node type for the Net BIOS from one of the four listed.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the Net BIOS node type for the DHCP pool:

```
DGS-3450:admin# config dhcp pool netbios_node_type accounting hybrid
Command: config dhcp pool netbios_node_type accounting hybrid

Success.

DGS-3450:admin#
```

config dhcp pool network_addr

Purpose	Used to configure the network address and corresponding subnet mask for the DHCP pool.
Syntax	config dhcp pool network_addr <pool_name 12> <network_address>
Description	This command will allow users to enter the IP address pool to be assigned to requesting DHCP Clients. This address will not be chosen but the first 3 sets of numbers in the IP address will be used for the IP address of requesting DHCP Clients. (ex. If this entry is given the IP address 10.10.10.2, then assigned addresses to DHCP Clients will resemble 10.10.10.x, where x is a number between 1 and 255 but does not include the assigned 10.10.10.2)
Parameters	<p><pool_name 12> – Enter the previously created pool name for which to set the network address.</p> <p><network_address> – IP address and netmask that is the address of this DHCP pool. The address and mask information can be specified using the traditional format (for example, 10.1.2.3/255.0.0.0 or in CIDR format, 10.1.2.3/8).</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the network address for the DHCP pool:

```
DGS-3450:admin# config dhcp pool network_addr accounting 10.1.1.1/8
Command:config dhcp pool network_addr accounting 10.1.1.1/8

Success.

DGS-3450:admin#
```

config dhcp pool next_server

Purpose	Used to configure the IP address of the server that has the boot file for the DHCP pool.
Syntax	config dhcp pool next_server <pool_name 12> <ipaddr>
Description	This command is used to configure the IP address of the server that has the boot file for the DHCP pool.
Parameters	<p><pool_name 12> – Enter the previously created pool name for which to set the next server.</p> <p><ipaddr> – Enter the IP address of the next server which has the boot file.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the IP address of the next server:

```
DGS-3450:admin# config dhcp pool next_server accounting 10.99.88.77
Command: config dhcp pool next_server accounting 10.99.88.77

Success.

DGS-3450:admin#
```

enable dhcp_server

Purpose	Used to enable the DHCP function on the switch.
Syntax	enable dhcp_server
Description	This command, along with the disable dhcp_server will enable and disable the DHCP server function without affecting configurations.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable DHCP server:

```
DGS-3450:admin# enable dhcp_server
Command: enable dhcp_server

Success.

DGS-3450:admin#
```

disable dhcp_server

Purpose	Used to disable the DHCP function on the switch.
Syntax	disable dhcp_server
Description	This command, along with the enable dhcp_server will enable and disable the DHCP server function without affecting configurations.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable the DHCP server:

```
DGS-3450:admin# disable dhcp_server
Command: disable dhcp_server

Success.

DGS-3450:admin#
```

show dhcp_server

Purpose	Used to display the DHCP server settings.
Syntax	show dhcp_server
Description	This command will display the DHCP server settings for its Global state, ping packet count and ping timeout.
Parameters	None.
Restrictions	None.

Example usage:

To display the DHCP server settings:

```
DGS-3450:admin# show dhcp_server
Command: show dhcp_server

DHCP Server Global State: Disable
Ping Packet Number       : 2
Ping Timeout             : 500 ms

DGS-3450:admin#
```

create dhcp excluded_address begin_address

Purpose	Used to configure IP addresses that will be excluded from the DHCP Server pool of addresses.
Syntax	create dhcp excluded_address begin_address <ipaddr> end_address <ipaddr>
Description	This command will allow the user to set an IP address, or a range of IP addresses that are NOT to be included in the range of IP addresses that the Switch will allot to clients requesting DHCP service.
Parameters	<i>begin_address <ipaddr></i> – Enter the beginning IP address of the range of IP addresses to be excluded from the DHCP pool. <i>end_address <ipaddr></i> – Enter the ending IP address of the range of IP addresses to be excluded from the DHCP pool.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure IP an address that will be excluded from the DHCP server pool of addresses:

```
DGS-3450:admin# create dhcp excluded_address begin_address 10.10.10.1 end_address
10.10.10.10
Command: create dhcp excluded_address begin_address 10.10.10.1 end_address 10.10.10.10

Success.

DGS-3450:admin#
```

delete dhcp excluded_address

Purpose	Used to delete IP addresses that have been configured as excluded from the DHCP Server pool of addresses.
Syntax	delete dhcp excluded_address [begin_address <ipaddr> end_address <ipaddr> all]
Description	This command will allow the user to delete a previously set IP address, or a range of IP addresses that are NOT to be included in the range of IP addresses that the Switch will allot to clients requesting DHCP service.
Parameters	<p><i>begin_address <ipaddr></i> – Enter the beginning IP address of the range of IP addresses to be deleted from the excluded IP address list, from the DHCP pool.</p> <p><i>end_address <ipaddr></i> – Enter the ending IP address of the range of IP addresses to be deleted from the excluded IP address list, from the DHCP pool.</p> <p>all – Enter this command to delete all excluded IP addresses, from the DHCP pool.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete IP addresses that have been configured as excluded from the DHCP server pool of addresses:

```
DGS-3450:admin# delete dhcp excluded_address begin_address 10.10.10.1 end_address
10.10.10.10
Command: delete dhcp excluded_address begin_address 10.10.10.1 end_address 10.10.10.10

Success.

DGS-3450:admin#
```

show dhcp excluded_address

Purpose	Used to display the excluded IP addresses of the DHCP server function.
Syntax	show dhcp excluded_address
Description	This command is used to display the excluded IP addresses of the DHCP server function.
Parameters	None.
Restrictions	None.

Example usage:

To display the DHCP server settings:

```
DGS-3450:admin# show dhcp excluded_address
Command: show dhcp excluded_address

Index          Begin_Address      End_Address
-----          -
1              192.168.0.1       192.168.0.100
2              10.10.10.10       10.10.10.10

Total Entries : 2

DGS-3450:admin#
```

show dhcp pool

Purpose	Used to show the DHCP pool information.
Syntax	show dhcp pool {<pool_name 12>}
Description	This command is used to display the DHCP pool information. Entering the command without the pool name will display all DHCP pool information on the switch.
Parameters	<pool_name 12> – Enter the name of the DHCP pool for which to view DHCP pool information.
Restrictions	None.

Example usage:

To display the DHCP pool information:

```
DGS-3450:admin# show dhcp pool Floor2
Command: show dhcp pool Floor2

Pool Name           :Floor2
Network Address     :10.0.0.0/8
Domain Name         :
DNS Server Address  :0.0.0.0
NetBIOS Name Server :0.0.0.0
NetBIOS Node Type   :Broadcast
Default Router      :0.0.0.0
Pool Lease          :1 Days, 0 Hours, 0 Minutes
Boot File           :
Next Server         :0.0.0.0

Total Pool Entry: 1

DGS-3450:admin#
```


DHCPV6 CLIENT COMMANDS

The DHCPV6 Client commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameters
config ipif	<ipif_name 12> [{ ipaddress <network_address> vlan <vlan_name 32> state [enable disable] proxy_arp [enable disable] {local [enable disable]}} (1) bootp dhcp ipv6 ipv6address <ipv6networkaddr> dhcpv6_client [enable disable]]
debug dhcpv6_client state	[enable disable]
debug dhcpv6_client output	[buffer console]
debug dhcpv6_client packet	{all receiving sending} state [enable disable]

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

config ipif

Purpose	Use this command to configure the DHCPV6 client state for the interface.
Syntax	config ipif <ipif_name 12> [{ ipaddress <network_address> vlan <vlan_name 32> state [enable disable] proxy_arp [enable disable] {local [enable disable]}} (1) bootp dhcp ipv6 ipv6address <ipv6networkaddr> dhcpv6_client [enable disable]]
Description	The command is used to configure the DHCPV6 client state for one interface.
Parameters	<p><i>ipif <ipif_name 12></i> - The name of the IP interface.</p> <p><i>ipaddress <network_address></i> - Configures a network on an IP interface. The address should specify a host address and length of network mask. Since an IP interface can have only one IPv4 address, the newly configured address will overwrite the original one.</p> <p><i>vlan <vlan_name 32></i> - Name of the VLAN where the IPIF is operated.</p> <p><i>proxy_arp</i> - Enable or disable the proxy ARP function. This is for the IPv4 function. Default: Disabled.</p> <p><i>local</i> - This setting controls whether the system provides the proxy reply for the ARP packets destined for an IP address located in the same interface as the received interface. When proxy ARP is enabled for an interface, the system will do the proxy reply for the ARP packets destined for an IP address located in a different interface. For ARP packets destined for an IP address located in the same interface, the system will check this setting to determine whether to reply. Default: Disabled.</p> <p><i>state</i> - Enable or disable the state of the IP interface.</p> <p><i>bootp</i> - Use BOOTP to obtain the IPv4 address.</p> <p><i>dhcp</i> - Use DHCP to obtain the IPv4 address.</p> <p><i>ipv6 ipv6address</i> - IPv6 network address: The address should specify a host address and length of network prefix. There can be multiple V6 addresses defined on an interface. Thus, as a new address is defined, it is added on this IP interface.</p> <p><i>dhcpv6_client</i> - See below:</p> <ul style="list-style-type: none"> <i>enable</i> - Enable the DHCPV6 client state of the interface. <i>disable</i> - Disable the DHCPV6 client state of the interface.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the DHCPV6 client state of the System interface to enabled:

```
DGS-3450:admin# config ipif System dhcpv6_client state enable
Command : config ipif System dhcpv6_client state enable

success

DGS-3450:admin#
```

To display IP interface settings:

```
DGS-3450:admin# show ipif System
Command: show ipif System

IP Interface           : System
VLAN Name              : default
Interface Admin state  : Enabled
DHCPv6 Client State   : Enabled
IPv4 Address           : 10.90.90.90/8 (Manual) Primary
Proxy ARP              : Disabled (Local : Disabled)
IPv6 Link-Local Address : FE80::219:5BFF:FEF5:26C0/128
IPv6 Global Unicast Address : 2000::2/64 (Manual)
IPv6 Global Unicast Address : 3000::3/64 (DHCPv6)
IP MTU                 : 1580

DGS-3450:admin#
```

debug dhcpv6_client state

Purpose	Enable or disable the DHCPv6 client debug function.
Syntax	debug dhcpv6_client state [enable disable]
Description	Use this command to enable or disable the DHCPv6 client debug function.
Parameters	<i>state</i> - See below: <i>enable</i> - Enable the DHCPv6 client debug function. <i>disable</i> - Disable the DHCPv6 client debug function.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enabled the DHCPv6 client debug function:

```
DGS-3450:admin# debug dhcpv6_client state enable
Command:  debug dhcpv6_client state enable

Success.

DGS-3450:admin#
```

debug dhcpv6_client output

Purpose	Used to set the debug message to output to buffer or console.
Syntax	debug dhcpv6_client output [buffer console]
Description	Set message output to buffer or console.
Parameters	<i>buffer</i> - Let the debug message output to buffer. <i>console</i> - Let the debug message output to console.

debug dhcpv6_client output

Restrictions Only Administrator and Operator-level users can issue this command.

Example usage:

To set debug information to output to console:

```
DGS-3450:admin# debug dhcpv6_client output console
Command: debug dhcpv6_client output console

Success.

DGS-3450:admin#
```

debug dhcpv6_client packet

Purpose	Used to enable or disable the debug information flag for DHCPv6 client packets, including packet receiving and sending.
Syntax	debug dhcpv6_client packet {all receiving sending} state [enable disable]
Description	Enable or disable the debug information flag for DHCPv6 client packets, including packet receiving and sending.
Parameters	<p><i>all</i> - Set packet receiving and sending debug flags.</p> <p><i>receiving</i> - Set packet receiving debug flag.</p> <p><i>sending</i> - Set packet sending debug flag.</p> <p><i>enable</i> - Enable the designated flags.</p> <p><i>disable</i> - Disable the designated flags.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable DHCPv6client packet sending debug flags:

```
DGS-3450:admin# debug dhcpv6_client packet sending state enable
Command: debug dhcpv6_client packet sending state enable

Success.

DGS-3450:admin#
```

DHCPV6 RELAY COMMANDS

The DHCPV6 Relay commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameters
config dhcpv6_relay hop_count	<value 1-32>
config dhcpv6_relay	[add delete] ipif <ipif_name 12> <ipv6addr>
config dhcpv6_relay ipif	[<ipif_name 12> all] state [enable disable]
show dhcpv6_relay	{ipif <ipif_name 12>}
enable dhcpv6_relay	
disable dhcpv6_relay	
debug dhcpv6_relay state	[enable disable]
debug dhcpv6_relay output	[buffer console]
debug dhcpv6_relay packet	{all receiving sending} state [enable disable]
debug dhcpv6_relay hop_count state	[enable disable]

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

config dhcpv6_relay hop_count

Purpose	This command is used to configure the DHCPV6 relay hop count of the switch.
Syntax	config dhcpv6_relay hop_count <value 1-32>
Description	This command is used to configure the DHCPV6 relay hop count of the switch.
Parameters	<i>hop_count</i> - The hop count is the number of relay agents that have to be relayed in this message. The range is 1 to 32. The default value is 4.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the maximum hops of a DHCPV6 relay packet that can be transferred to 4:

```
DGS-3450:admin# config dhcpv6_relay hop_count 4
Command: config dhcpv6_relay hop_count 4

Success.

DGS-3450:admin#
```

config dhcpv6_relay

Purpose	This command is used to add or delete a destination IP address to or from the switch's DHCPV6 relay table.
Syntax	config dhcpv6_relay [add delete] ipif <ipif_name 12> <ipv6addr>
Description	This command can add or delete an IPv6 destination address to forward (relay) DHCPV6 packets.

config dhcpv6_relay

Parameters	<p><i>add</i> - Add an IPv6 destination to the DHCPv6 relay table.</p> <p><i>delete</i> - Delete an IPv6 destination from the DHCPv6 relay table</p> <p><i>ipif_name</i> - The name of the IP interface in which DHCPv6 relay is to be enabled.</p> <p><i>ipv6addr</i> - The DHCPv6 server IP address.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To add a DHCPv6 server to the relay table:

```
DGS-3450:admin# config dhcpv6_relay add ipif System 2001:DB8:1234:0:218:FEFF:FEFB:CC0E
Command: config dhcpv6_relay add ipif System 2001:DB8:1234:0:218:FEFF:FEFB:CC0E
Success.
DGS-3450:admin#
```

config dhcpv6_relay ipif

Purpose	This command is used to configure the DHCPv6 relay state of one or all of the specified interfaces.
Syntax	config dhcpv6_relay ipif [<ipif_name 12> all] state [enable disable]
Description	This command is used to configure the DHCPv6 relay state of one or all of the specified interfaces.
Parameters	<p><i>ipif_name</i> - The name of the IP interface. The value all indicates all configured IP interfaces.</p> <p><i>state</i> - See below:</p> <ul style="list-style-type: none"> <i>enable</i> - Choose this parameter to enable the DHCPv6 relay state of the interface. <i>disable</i> - Choose this parameter to disable the DHCPv6 relay state of the interface.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the DHCPv6 relay state of the System interface to enable:

```
DGS-3450:admin# config dhcpv6_relay ipif System state enable
Command: config dhcpv6_relay ipif System state enable
Success.
DGS-3450:admin#
```

show dhcpv6_relay

Purpose	This command displays the current DHCPv6 relay configuration.
Syntax	show dhcpv6_relay {ipif <ipif_name 12>}
Description	This command will display the current DHCPv6 relay configuration of all interfaces, or if an IP interface name is specified, the DHCPv6 relay configuration for that IP interface.
Parameters	<i>ipif_name</i> - The name of the IP interface that will be displayed in the current DHCPv6 relay configuration.

show dhcpv6_relay

If no IP interface is specified, all configured DHCPv6 relay interfaces will be displayed.

Restrictions

Only Administrator and Operator-level users can issue this command.

Example usage:

This is an example to show the DHCPv6 relay configuration of all interfaces:

```
DGS-3450:admin# show dhcpv6_relay
Command: show dhcpv6_relay

DHCPv6 Hops Count Limit      : 4
DHCPv6 Global State          : Disabled
-----
System Interface:
DHCPv6 Relay Status          : Disabled
Server Address                : 2001:DB8:1234:0:218:FEFF:FEFB:1
Server Address                : 3ffe::500
Server Address                : 3ffe::600
Server Address                : ff05::1:3%Ipif1

Ipif_1 Interface:
DHCPv6 Relay Status          : Enabled
Server Address                : 2001:DB8:1234:1:218:FEFF:FEFB:2

Ipif_2 Interface:
DHCPv6 Relay Status          : Disabled

Total Entries : 3

DGS-3450:admin#
```

To show the DHCPv6 relay configuration of the System interface:

```
DGS-3450:admin# show dhcpv6_relay ipif System
Command: show dhcpv6_relay ipif System

DHCPv6 Hops Count Limit      : 4
DHCPv6 Global State          : Disabled
-----
System Interface:
DHCPv6 Relay Status          : Disabled
Server Address                : 2001:DB8:1234:0:218:FEFF:FEFB:1
Server Address                : 3ffe::500
Server Address                : 3ffe::600
Server Address                : ff05::1:3%Ipif1

DGS-3450:admin#
```

enable dhcpv6_relay

Purpose

Used to enable the DHCPv6 relay function on the Switch.

Syntax

enable dhcpv6_relay

Description

This command is used to enable the DHCPv6 relay global state on the Switch.

enable dhcpv6_relay

Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the DHCPv6 relay global state to enable:

```
DGS-3450:admin# enable dhcpv6_relay
Command: enable dhcpv6_relay
```

Success.

```
DGS-3450:admin#
```

disable dhcpv6_relay

Purpose	Used to disable the DHCPv6 relay function on the Switch
Syntax	disable dhcpv6_relay
Description	This command is used to disable the DHCPv6 relay global state on the Switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the DHCPv6 relay global state to disable:

```
DGS-3450:admin# disable dhcpv6_relay
Command: disable dhcpv6_relay
```

Success.

```
DGS-3450:admin#
```

debug dhcpv6_relay state

Purpose	This command is used to enable or disable DHCPv6 relay debug functions.
Syntax	debug dhcpv6_relay state [enable disable]
Description	This command is used to enable or disable DHCPv6 relay debug functions.
Parameters	<i>state</i> - See below: <i>enable</i> - Enable the DHCPv6 relay debug function <i>disable</i> - Disable the DHCPv6 relay debug function
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enabled the DHCPv6 relay debug function:

```
DGS-3450:admin# debug dhcpv6_relay state enable
Command:  debug dhcpv6_relay state enable

Success.

DGS-3450:admin#
```

debug dhcpv6_relay output

Purpose	This command is used to set the debug message to output to a buffer or a console.
Syntax	debug dhcpv6_relay output [buffer console]
Description	This command is used to set the debug message to output to a buffer or a console.
Parameters	<i>output</i> - See below: <i>buffer</i> - Let the debug message output to buffer. <i>console</i> - Let the debug message output to console.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To set debug information to output to a console:

```
DGS-3450:admin# debug dhcpv6_relay output console
Command:  debug dhcpv6_relay output console

Success.

DGS-3450:admin#
```

debug dhcpv6_relay packet

Purpose	This command is used to enable or disable the debug information flag of the DHCPv6 relay packet, including packets receiving and sending.
Syntax	debug dhcpv6_relay packet {all receiving sending} state [enable disable]
Description	This command is used to enable or disable the debug information flag of the DHCPv6 relay packet, including packets receiving and sending.
Parameters	<i>all</i> - Set packet receiving and sending debug flags. <i>receiving</i> - Set packet receiving debug flag. <i>sending</i> - Set packet sending debug flag. <i>enable</i> - Enable the designated flags. <i>disable</i> - Disable the designated flags.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enabled the DHCPv6 relay packet sending debug:


```
DGS-3450:admin# debug dhcpv6_relay packet sending state enable
Command: debug dhcpv6_relay packet sending state enable

Success.

DGS-3450:admin#
```

debug dhcpv6_relay hop_count state

Purpose	This command is used to enable or disable debug information flag about the hop count.
Syntax	debug dhcpv6_relay hop_count state [enable disable]
Description	This command is used to enable or disable debug information flag about the hop count.
Parameters	<p><i>hop_count</i> - The hop count is the number of relay agents that have to be relayed in this message. The range is 1 to 32. The default value is 4.</p> <p><i>enable</i> - Enable the hop_count state.</p> <p><i>disable</i> - Disable the hop_count state.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable debug information flag about the hop count:

```
DGS-3450:admin# debug dhcpv6_relay hop_count state enable
Command: debug dhcpv6_relay hop_count state enable

Success.

DGS-3450:admin#
```

DHCPV6 SERVER COMMANDS

The DHCPV6 Server commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameters
create dhcpv6 pool	<pool_name 12>
delete dhcpv6 pool	[<pool_name 12> all]
show dhcpv6 pool	{<pool_name 12>}
config dhcpv6 pool ipv6network_addr	<pool_name 12> begin < ipv6networkaddr> end <ipv6networkaddr>
config dhcpv6 pool domain_name	<pool_name 12> <domain_name 255>
config dhcpv6 pool dns_server	<pool_name 12> <ipv6addr> {<ipv6addr>}
config dhcpv6 pool lifetime	<pool_name 12> preferred_lifetime <sec 60-4294967295> valid_lifetime <sec 60-4294967295>
config dhcpv6 pool manual_binding	<pool_name 12> [add <ipv6addr > client_duid <string 28> delete [<ipv6addr > all]]
show dhcpv6 manual_binding	{<pool_name 12>}
show dhcpv6 binding	{<pool_name 12>}
clear dhcpv6 binding	{<pool_name 12>}
enable dhcpv6_server	
disable dhcpv6_server	
show dhcpv6_server	
config dhcpv6 pool excluded_address	<pool_name 12> [add begin < ipv6addr> end < ipv6addr > delete [begin < ipv6addr> end < ipv6addr> all]]
show dhcpv6 excluded_address	{<pool_name 12>}
config dhcpv6_server ipif	<ipif_name 12> state [enable disable]
debug dhcpv6_server state	[enable disable]
debug dhcpv6_server packet	{all receiving sending} state [enable disable]

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

create dhcpv6 pool

Purpose	This command is used to create a DHCPV6 pool.
Syntax	create dhcpv6 pool <pool_name 12>
Description	This command is used to create a DHCPV6 pool for the DHCPV6 server.
Parameters	<pool_name 12> - Enter a name of up to 12 alphanumeric characters to identify the pool to be created with this command.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create a DHCPV6 pool pool1:

```
DGS-3450:admin# create dhcpv6 pool pool1
Command : create dhcpv6 pool pool1

success

DGS-3450:admin#
```

delete dhcpv6 pool

Purpose	This command is used to delete one or all DHCPv6 pools.
Syntax	delete dhcpv6 pool [<pool_name 12> all]
Description	This command will delete a DHCPv6 pool that was created with the create dhcpv6 pool command.
Parameters	<i>pool <pool_name 12></i> - Enter a name of up to 12 alphanumeric characters to identify the pool to be deleted with this command. <i>all</i> - If specify this parameter, all DHCPv6 pools on the Switch will be deleted.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete the DHCPv6 pool by specifying the pool name pool1:

```
DGS-3450:admin# delete dhcpv6 pool pool1
Command: delete dhcpv6 pool pool1

Success.

DGS-3450:admin#
```

show dhcpv6 pool

Purpose	This command is used to display one or all DHCPv6 pools configuration.
Syntax	show dhcpv6 pool {<pool_name 12>}
Description	This command will show one or all DHCPv6 pools configuration that were created with the create dhcpv6 pool command.
Parameters	<i>pool <pool_name 12></i> - Enter the name of the DHCPv6 pool for which to view the pool information. Entering this command without the pool name will display all pools information of the DHCPv6 server.
Restrictions	None.

Example usage:

To show the DHCPv6 pool by specifying the pool name pool1:

```
DGS-3450:admin# show dhcpv6 pool pool1
```

```
Command: show dhcpv6 pool pool1
```

```
Pool Name           : pool1
Begin Network Address : 2000::1/64
End Network Address  : 2000::200/64
Domain Name          : domain.com
DNS Server Address   : 2000::ff
                    : 2000::fe
Preferred Lifetime   : 604800 (sec)
Valid Lifetime       : 2592000 (sec)
```

```
Total Pool Entry: 1
```

```
DGS-3450:admin#
```

config dhcpv6 pool ipv6networkaddr

Purpose	This command is used to configure the range of ipv6network address for the DHCPv6 pool
Syntax	config dhcpv6 pool ipv6network_addr <pool_name 12> begin < ipv6networkaddr> end <ipv6networkaddr>
Description	<p>Specify the range of ipv6network address for the DHCPv6 pool. The IPv6 addresses in the range are free to be assigned to the DHCPv6 client.</p> <p>When the DHCPv6 server receives a request from the client, the server will automatically find an available pool to allocate an IPv6 address.</p> <p>The begin_networkaddr and end_networkaddr must observe some rules as followed:</p> <ol style="list-style-type: none"> 1. The prefix of the begin_networkaddr and end_networkaddr are not consistent, otherwise, the switch will print an error message: The prefix of begin_networkaddr and end_networkaddr must be consistent.(e.g.: the begin_networkaddr is 2000::1/64, and the end_networkaddr is 3000::100/64) 2. The begin address must not be larger than end address, otherwise, the switch will print an error message: The begin IPv6 address must be lower than or equal to the end IPv6 address.(e.g.: the begin_networkaddr is 2000::200/64, and the end_networkaddr is 2000::100/64) 3. There must not be intersection between the IPv6 address ranges of two pools, otherwise, the Switch will print an error message: IPv6network address collision. (e.g.: pool1: 2000::1/64 --- 2000::100/64, pool2: 2000::50/64 --- 2000::200/64) 4. The IPv6 network address can't be Link-local address and Multicast address, otherwise, the Switch will print an error message: "The IPv6 network address can't be Link-local address or Multicast address." (e.g.: pool1: FE80::1/64 --- FE80::100/64, pool2: FE80::200/64 --- FE80::300/64)
Parameters	<p><i>pool <pool_name 12></i> - Enter the previously created pool name for which to set the network address.</p> <p><i>begin <ipv6networkaddr></i> - The begin IPv6network address of the DHCPv6 pool.</p> <p><i>end < ipv6networkaddr></i> - The end IPv6 network address of the DHCPv6 pool.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the range of ipv6network address for the DHCPv6 pool pool1:

```
DGS-3450:admin# config dhcpv6 pool ipv6networkaddr pool1 begin 2000::1/64 end 2000::32/64
Command: config dhcpv6 pool ipv6networkaddr pool1 begin 2000::1/64 end 2000::32/64

success

DGS-3450:admin#
```

config dhcpv6 pool domain_name

Purpose	This command is used to configure the domain name for the DHCPv6 pool of the Switch.
Syntax	config dhcpv6 pool domain_name <pool_name 12> <domain_name 255>
Description	The domain name configured here will be used as the default domain name by the client. By default, the domain name is empty. If domain name is empty, the domain name information will not be provided to the client.
Parameters	<i>pool <pool_name 12></i> - Enter the pool name for which to set the domain name. <i>domain_name <domain_name 255></i> - The domain name is used by client when resolving hostnames with DNS.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the domain name for the DHCPv6 pool pool1:

```
DGS-3450:admin# config dhcpv6 pool domain_name pool1 d_link.com
Command: config dhcpv6 pool domain_name pool1 d_link.com

Success.

DGS-3450:admin#
```

config dhcpv6 pool dns_server

Purpose	This command is used to configure the DNS server's IPv6 addresses for a specific DHCPv6 pool.
Syntax	config dhcpv6 pool dns_server <pool_name 12> <ipv6addr> {<ipv6addr>}
Description	This command is used to configure the DNS server IPv6 addresses for a specific DHCPv6 pool. Users may add up to two DNS Server addresses. If DNS server is not specified, the DNS server information will not be provided to the client. Users could delete a DNS server address in the method of setting the DNS server address to zero. For example, users first add two DNS server address: 2000::200, 2000::201, and then delete the DNS server address 2000::200. The procedure is as followed: Command: config dhcpv6 pool dns_server pool1 2000::200 2000::201 config dhcpv6 pool dns_server pool1 ::
Parameters	<i><pool_name 12></i> - Enter the pool name for which to add one or two DNS server addresses. <i><ipv6addr></i> - Enter the DNS server IPv6 address for this pool. Users may specify up to two DNS server addresses.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the DNS server address for a DHCPv6 pool:

```
DGS-3450:admin# config dhcpv6 pool dns_server pool1 2000::200 2000::201
Command: config dhcpv6 pool dns_server pool1 2000::200 2000::201

Success.

DGS-3450:admin#
```

config dhcpv6 pool lifetime

Purpose	This command is used to configure the preferred-lifetime and valid-lifetime of IPv6 address within a DHCPv6 pool.
Syntax	config dhcpv6 pool lifetime <pool_name 12> preferred_lifetime <sec 60-4294967295> valid_lifetime <sec 60-4294967295>
Description	within a DHCPv6 pool. preferred lifetime - the length of time that a valid address is preferred (i.e., the time until deprecation). When the preferred lifetime expires, the address becomes deprecated. valid lifetime - the length of time an address remains in the valid state (i.e., the time until invalidation). When the valid lifetime expires, the address becomes invalid. The valid lifetime must be greater than or equal to the preferred lifetime.
Parameters	<i>pool <pool_name 12></i> - Enter the previously created pool name for which to set the preferred-lifetime and valid-lifetime of IPv6 address. <i>preferred_lifetime <sec 60-4294967295></i> - The amount of time (in seconds) that the IPv6 address, based on the specified pool, remains in preferred state. <i>valid_lifetime <sec 60-4294967295></i> - The amount of time (in seconds) that the IPv6 address, based on the specified pool, remains in valid state.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the preferred-lifetime and valid-lifetime for the DHCPv6 pool:

```
DGS-3450:admin# config dhcpv6 pool lifetime pool1 preferred_lifetime 80 valid_lifetime 100
Command: config dhcpv6 pool lifetime pool1 preferred_lifetime 80 valid_lifetime 100

Success.

DGS-3450:admin#
```

config dhcpv6 pool manual_binding

Purpose	This command is used to configure a DHCPv6 pool manual binding entry.
Syntax	config dhcpv6 pool manual_binding <pool_name 12> [add <ipv6addr > client_aid <string 28> delete [<ipv6addr > all]]
Description	An address binding is a mapping between the IPv6 address and DUID (A DHCPv6 Unique Identifier for a DHCPv6 participant) of a client. The IPv6 address specified in the manual binding entry must be in the range of the DHCPv6 pool. If the user specifies a conflict IPv6 address, error message (#9) will be returned.
Parameters	<i>pool <pool_name 12></i> - Enter the name of the previously created pool that will contain the manual binding entry.

config dhcpv6 pool manual_binding

add <ipv6addr> - Enter the IPv6 address to be statically bound to a device.
client_ duid <string 28> - Enter the DUID of the device to be statically bound to the IPv6 address entered in the previous field. The DUID string must be '0--9', 'a--f' or 'A--F'.
delete - To delete the manual binding entry.
 <ipv6addr> - Enter the IPv6 address of the manual binding entry to be deleted.
all - Enter this command to delete all manual binding entries for the given pool.

Restrictions

Only Administrator and Operator-level users can issue this command.

Example usage:

To add a manual binding DHCPv6 entry:

```
DGS-3450:admin# create dhcpv6 pool manual_binding pool1 add 2000::3 client_ duid
00010006124dd5840021918d4d9f
Command: create dhcpv6 pool manual_binding pool1 add 2000::3 client_ duid
00010006124dd5840021918d4d9f
```

success

```
DGS-3450:admin#
```

show dhcpv6 manual_binding

Purpose	This command is used to display the manual binding settings.
Syntax	show dhcpv6 manual_binding {<pool_name 12>}
Description	This command will display the manual binding entries for the selected or all DHCPv6 pools.
Parameters	<i>pool</i> <pool_name 12> - Enter the name of the DHCPv6 pool for which to view manual binding entries. Entering this command without the pool name will display all manual binding entries of the DHCPv6 server.
Restrictions	None.

Example usage:

To display the manual binding entries of the DHCPv6 pool pool1:

```
DGS-3450:admin# show dhcpv6 manual_binding
Command: show dhcpv6 manual_binding

Pool Name: pool1
Entry 1
  IPv6 Address : 3000::21
  DUID         : 00010006124dd584002191454d33

Entry 2
  IPv6 Address : 3000::28
  DUID         : 000300060022d7e50900

Pool Name: pool2
Entry 1
  IPv6 Address : 8000:1000:1000:1000:1000:1000:1000:2000
  DUID         : 00010006124dd584002191454d37

Total Entries: 3

DGS-3450:admin#
```

show dhcpv6 binding

Purpose	This command is used to show the DHCPv6 dynamic binding information.
Syntax	show dhcpv6 binding {<pool_name 12>}
Description	This command is used to display the DHCPv6 dynamic binding information. Entering the command without the pool name will display all information regarding DHCPv6 dynamic binding on the switch. This command only displays the dynamic binding information, not including manual binding information.
Parameters	<pool_name 12> - Enter the name of the DHCPv6 pool for which to view dynamic binding information. Entering this command without the pool name will display all dynamic binding entries of the DHCPv6 server.
Restrictions	None.

Example usage:

To display the DHCPv6 dynamic binding information on the Switch:

```
DGS-3450:admin# show dhcpv6 binding
Command: show dhcpv6 binding

Pool Name: pool1      Ipv6 Address : 2000::3
                     DUID         : 00010006124dd5840021918d4d9f
                     Preferred(s) : 604800           Valid(s): 2592000

Pool Name: pool1      Ipv6 Address : 2000::1
                     DUID         : 00010006124dd5840021918d8865
                     Preferred(s) : 620              Valid(s): 800

Total Entries : 2

DGS-3450:admin#
```


clear dhcpv6 binding

Purpose	This command is used to clear the DHCPv6 dynamic binding information.
Syntax	clear dhcpv6 binding {<pool_name 12>}
Description	This command is used to clear the DHCPv6 dynamic binding information, not including manual binding information. Users could use command (4-1-8) to delete the manual binding information.
Parameters	<pool_name 12> - Enter the name of the DHCPv6 pool for which to clear the dynamic binding information. If not specify the parameter, it will delete all dynamic binding entries of the DHCPv6 server.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To clear the DHCPv6 dynamic binding information on the Switch:

```
DGS-3450:admin# clear dhcpv6 binding
Command: clear dhcpv6 binding

Success.

DGS-3450:admin#
```

enable dhcpv6_server

Purpose	This command is used to enable the DHCPv6 server function on the Switch.
Syntax	enable dhcpv6_server
Description	This command is used to enable the DHCPv6 server global state on the Switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the DHCPv6 server global state to enable:

```
DGS-3450:admin# enable dhcpv6_server
Command: enable dhcpv6_server

Success.

DGS-3450:admin#
```

disable dhcpv6_server

Purpose	This command is used to disable the DHCPv6 server function on the Switch.
Syntax	disable dhcpv6_server
Description	This command is used to disable the DHCPv6 server global state on the Switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the DHCPv6 server global state to disable:

```
DGS-3450:admin# disable dhcpv6_server
Command: disable dhcpv6_server

Success.

DGS-3450:admin#
```

show dhcpv6_server

Purpose	This command is used to display the DHCPv6 server setting.
Syntax	show dhcpv6_server
Description	This command will display the DHCPv6 server settings.
Parameters	None.
Restrictions	None.

Example usage:

To display the DHCPv6 server setting:

```
DGS-3450:admin# show dhcpv6_server
Command: show dhcpv6_server

DHCPv6 Server Global State: Disabled
-----
IP Interface           : System
DHCPv6 Server State   : Enabled

IP Interface           : ipif1
DHCPv6 Server State   : Enabled

Total Entries        : 2

DGS-3450:admin#
```

config dhcpv6 pool excluded_address

Purpose	This command is used to configure the reserved IPv6 addresses on the DHCPv6 server
Syntax	config dhcpv6 pool excluded_address <pool_name 12> [add begin < ipv6addr> end < ipv6addr > delete [begin < ipv6addr> end < ipv6addr> all]]
Description	This command will configure the IPv6 addresses range that the DHCPv6 server should not assign to DHCPv6 client. The excluded address range must be the subset of the specified pool.
Parameters	<p><i>pool <pool_name 12></i> - Enter the name of the DHCPv6 pool for which to add/delete the excluded address information.</p> <p><i>add</i> - Add an excluded address range for a specified pool.</p> <p><i>delete</i> - Delete one or all excluded address ranges of a specified pool.</p> <p><i>begin <ipv6addr></i> - Enter the beginning IPv6 address of the range of IPv6 addresses to be excluded from the DHCPv6 pool.</p> <p><i>end <ipv6addr></i> - Enter the ending IPv6 address of the range of IPv6 addresses to be excluded from the DHCPv6 pool.</p>

config dhcpv6 pool excluded_address

all - Delete all excluded address ranges of a specified pool.

Restrictions

Only Administrator and Operator-level users can issue this command.

Example usage:

To add the IPv6 addresses range that DHCPv6 server should not assign to clients:

```
DGS-3450:admin# config dhcpv6 pool excluded_address pool1 add begin 2000::3 end 2000::8
Command: config dhcpv6 pool excluded_address pool1 add begin 2000::3 end 2000::8
```

Success.

```
DGS-3450:admin#
```

show dhcpv6 excluded_address

Purpose This command is used to display the groups of IPv6 addresses which are excluded from the legal assigned IPv6 address

Syntax **show dhcpv6 excluded_address {<pool_name 12>}**

Description This command will display the groups of IPv6 addresses which are excluded from the legal assigned IPv6 address.

Parameters <pool_name 12> - Enter the name of the DHCPv6 pool for which to display the excluded address information.

If not specify the pool name, It will display all pool's excluded address information.

Restrictions

None.

Example usage:

To display the excluded address information:

```
DGS-3450:admin# show dhcpv6 excluded_address
Command: show dhcpv6 excluded_address

Pool name: Pool1
Range 1
Begin Address: 2000::2
End Address   : 2000::5

Range 2
Begin Address: 2000::8
End Address   : 2000::8

Pool name: Pool2
Range 1
Begin Address: 3000::2
End Address   : 3000::5
Range 2
Begin Address: 3000::8
End Address   : 3000::8
Range 3
Begin Address: 3000::18
End Address   : 3000::20

Total Entries : 5

DGS-3450:admin#
```

config dhcpv6_server ipif

Purpose	This command is used to configure the DHCPv6 Server state per interface
Syntax	config dhcpv6_server ipif <ipif_name 12> state [enable disable]
Description	This command configures the DHCPv6 Server state on the IP interface.
Parameters	<i>ipif <ipif_name 12></i> - The name of the IP interface. <i>state</i> - See below: <i>enable</i> - Enable the dhcpv6 server state for a specified interface. <i>disable</i> - Disable the dhcpv6 server state for a specified interface.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the DHCPv6 Server state of System Interface to enable:

```
DGS-3450:admin# config dhcpv6_server ipif System state enable
Command: config dhcpv6_server ipif System state enable

Success.

DGS-3450:admin#
```

debug dhcpv6_server state

Purpose	This command is used to enable or disable DHCPv6 server debug functions.
Syntax	debug dhcpv6_server state [enable disable]

debug dhcpv6_server state

Description	This command is used to enable or disable DHCPv6 server debug functions.
Parameters	<i>state</i> - See below: <i>enable</i> - Enable the DHCPv6 server debug function <i>disable</i> - Disable the DHCPv6 server debug function
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enabled the DHCPv6 server debug function:

```
DGS-3450:admin# debug dhcpv6_server state enable
```

```
Command: debug dhcpv6_server state enable
```

```
Success.
```

```
DGS-3450:admin#
```

debug dhcpv6_server packet

Purpose	This command is used to enable or disable the debug information flag of the DHCPv6 server packet, including packets receiving and sending.
Syntax	debug dhcpv6_server packet {all receiving sending} state [enable disable]
Description	This command is used to enable or disable the debug information flag of the DHCPv6 server packet, including packets receiving and sending.
Parameters	<i>all</i> - Set packet receiving and sending debug flags. <i>receiving</i> - Set packet receiving debug flag. <i>sending</i> - Set packet sending debug flag. <i>enable</i> - Enable the designated flags. <i>disable</i> - Disable the designated flags.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enabled the DHCPv6 server packet sending debug:

```
DGS-3450:admin# debug dhcpv6_server packet sending state enable
```

```
Command: debug dhcpv6_server packet sending state enable
```

```
Success.
```

```
DGS-3450:admin#
```

DIGITAL DIAGNOSTIC MONITORING (DDM) COMMANDS

This DDM UI specification describes the Digital Diagnostic Monitoring functionality and specifications based on SFF-8472 standard. Functions of this software module apply on L2 and L3 Ethernet switches, which contain SFP interface.

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

Command	Parameters
config ddm ports	[<portlist> all] temperature_threshold { high_alarm < float > low_alarm < float > high_warning < float > low_warning < float >} (1)
config ddm ports	[<portlist> all] voltage_threshold { high_alarm < float > low_alarm < float > high_warning < float > low_warning < float >} (1)
config ddm ports	[<portlist> all] bias_current_threshold { high_alarm < float > low_alarm < float > high_warning < float > low_warning < float >} (1)
config ddm ports	[<portlist> all] tx_power_threshold { high_alarm < float > low_alarm < float > high_warning < float > low_warning < float >} (1)
config ddm ports	[<portlist> all] rx_power_threshold { high_alarm < float > low_alarm < float > high_warning < float > low_warning < float >} (1)
config ddm ports	[<portlist> all] { state [enable disable] shutdown [alarm warning none]} (1)
config ddm log	[enable disable]
config ddm trap	[enable disable]
show ddm ports	{<portlist>} status
show ddm ports	{<portlist>} configuration
show ddm	

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

config ddm ports temperature_threshold

Purpose	To configure the thresholds of temperature of the specified ports.
Syntax	config ddm ports [<portlist> all] temperature_threshold { high_alarm < float > low_alarm < float > high_warning < float > low_warning < float >} (1)
Description	The command configures the temperature thresholds of the specified ports.
Parameters	<p><i>portlist</i> - Specified a range of ports to be configured. (UnitID: port number).</p> <p><i>all</i> - If 'all' parameter is chosen, all SFP ports' operating parameters will be configured.</p> <p><i>temperature_threshold</i> - Specifies the threshold of SFP module's temperature.</p> <p><i>high_alarm</i> - High threshold for alarm. When the operating parameter rises above this value, action associated with alarm is taken. The range of this parameter is -128 to 127.996 Celsius degrees.</p> <p><i>low_alarm</i> - Low threshold for alarm. When the operating parameter falls below this value, action associated with alarm is taken. The range of this parameter is -128 to 127.996 Celsius degrees.</p> <p><i>high_warning</i> - High threshold for warning. When the operating parameter rises above this value, action associated with warning is taken. The range of this parameter is -128 to 127.996 Celsius degrees.</p> <p><i>low_warning</i> - Low threshold for warning. When the operating parameter falls below this value, action associated with warning is taken. The range of this parameter is -128 to</p>

config ddm ports temperature_threshold

127.996 Celsius degrees.

Restrictions

Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the port 9's temperature threshold:

```
DGS-3450:admin# config ddm ports 9 temperature_threshold high_alarm 84.9555 low_alarm -10
high_warning 70 low_warning 2.2525
Command: config ddm ports 9 temperature_threshold high_alarm 84.9555 low_alarm -10
high_warning 70 low_warning 2.2525
```

According to the DDM precision definition, closest value 84.9531 and 2.25 are chosen.

Success.

DGS-3450:admin#

config ddm ports voltage_threshold

Purpose

To configure the thresholds of voltage of the specified ports.

Syntax

config ddm ports [<portlist> | all] **voltage_threshold** { **high_alarm** < float > | **low_alarm** < float > | **high_warning** < float > | **low_warning** < float >} (1)

Description

The command configures the voltage thresholds of the specified ports.

Parameters

portlist - Specified a range of ports to be configured. (UnitID: port number).

all - If 'all' parameter is chosen, all SFP ports' operating parameters will be configured.

voltage_threshold - Specifies the threshold of SFP module's voltage.

high_alarm - High threshold for alarm. When the operating parameter rises above this value, action associated with alarm is taken. The range of this parameter is 0 to 6.55 voltages.

low_alarm - Low threshold for alarm. When the operating parameter falls below this value, action associated with alarm is taken. The range of this parameter is 0 to 6.55 voltages.

high_warning - High threshold for warning. When the operating parameter rises above this value, action associated with warning is taken. The range of this parameter is 0 to 6.55 voltages.

low_warning - Low threshold for warning. When the operating parameter falls below this value, action associated with warning is taken. The range of this parameter is 0 to 6.55 voltages.

Restrictions

Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the port 9's voltage threshold:

```
DGS-3450:admin# config ddm ports 9 voltage_threshold high_alarm 4.25 low_alarm 2.5 high_warning 3.5 low_warning 3
Command: config ddm ports 9 voltage_threshold high_alarm 4.25 low_alarm 2.5 high_warning 3.5 low_warning 3
```

Success.

DGS-3450:admin#

config ddm ports bias_current_threshold

Purpose	To configure the thresholds of bias current of the specified ports
Syntax	config ddm ports [<portlist> all] bias_current_threshold { high_alarm < float > low_alarm < float > high_warning < float > low_warning < float >} (1)
Description	The command configures the bias current thresholds of the specified ports.
Parameters	<p><i>portlist</i> - Specified a range of ports to be configured. (UnitID: port number).</p> <p><i>all</i> - If 'all' parameter is chosen, all SFP ports' operating parameters will be configured.</p> <p><i>bias_current_threshold</i> - Specifies the threshold of SFP module's bias current.</p> <p><i>high_alarm</i> - High threshold for alarm. When the operating parameter rises above this value, action associated with alarm is taken. The range of this parameter is 0 to 131 mA.</p> <p><i>low_alarm</i> - Low threshold for alarm. When the operating parameter falls below this value, action associated with alarm is taken. The range of this parameter is 0 to 131 mA</p> <p><i>high_warning</i> - High threshold for warning. When the operating parameter rises above this value, action associated with warning is taken. The range of this parameter is 0 to 131 mA</p> <p><i>low_warning</i> - Low threshold for warning. When the operating parameter falls below this value, action associated with warning is taken. The range of this parameter is 0 to 131 mA</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the port 9's bias current threshold:

```
DGS-3450:admin# config ddm ports 9 bias_current_threshold high_alarm 7.25 low_alarm 0.004
high_warning 0.5 low_warning 0.008
Command: config ddm ports 9 bias_current_threshold high_alarm 7.25 low_alarm 0.004
high_warning 0.5 low_warning 0.008

Success.

DGS-3450:admin#
```

config ddm ports tx_power_threshold

Purpose	To configure the thresholds of output power of the specified ports.
Syntax	config ddm ports [<portlist> all] tx_power_threshold { high_alarm < float > low_alarm < float > high_warning < float > low_warning < float >} (1)
Description	The command configures the output power thresholds of the specified ports.
Parameters	<p><i>portlist</i> - Specified a range of ports to be configured. (UnitID: port number).</p> <p><i>all</i> - If 'all' parameter is chosen, all SFP ports' operating parameters will be configured.</p> <p><i>tx_power_threshold</i> - Specifies the threshold of SFP module's output power.</p> <p><i>high_alarm</i> - High threshold for alarm. When the operating parameter rises above this value, action associated with alarm is taken. The range of this parameter is 0 to 6.5535 mW.</p> <p><i>low_alarm</i> - Low threshold for alarm. When the operating parameter falls below this value, action associated with alarm is taken. The range of this parameter is 0 to 6.5535 mW.</p> <p><i>high_warning</i> - High threshold for warning. When the operating parameter rises above this value, action associated with warning is taken. The range of this parameter is 0 to 6.5535 mW.</p> <p><i>low_warning</i> - Low threshold for warning. When the operating parameter falls below this value, action associated with warning is taken. The range of this parameter is 0 to 6.5535 mW.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the port 9's transmit power threshold:

```
DGS-3450:admin# config ddm ports 9 tx_power_threshold high_alarm 0.625 low_alarm 0.006
high_warning 0.55 low_warning 0.008
Command: config ddm ports 9 tx_power_threshold high_alarm 0.625 low_alarm 0.006 hi
gh_warning 0.55 low_warning 0.008

Success.

DGS-3450:admin#
```

config ddm ports rx_power_threshold

Purpose	To configure the thresholds of received power of the specified ports.
Syntax	config ddm ports [<portlist> all] rx_power_threshold { high_alarm <float > low_alarm <float > high_warning <float > low_warning <float >} (1)
Description	The command configures the output power thresholds of the specified ports.
Parameters	<p><i>portlist</i> - Specified a range of ports to be configured. (UnitID: port number).</p> <p><i>all</i> - If 'all' parameter is chosen, all SFP ports' operating parameters will be configured.</p> <p><i>rx_power_threshold</i> - Specifies the threshold of SFP module's received power.</p> <p><i>high_alarm</i> - High threshold for alarm. When the operating parameter rises above this value, action associated with alarm is taken. The range of this parameter is 0 to 6.5535 mW.</p> <p><i>low_alarm</i> - Low threshold for alarm. When the operating parameter falls below this value, action associated with alarm is taken. The range of this parameter is 0 to 6.5535 mW.</p> <p><i>high_warning</i> - High threshold for warning. When the operating parameter rises above this value, action associated with warning is taken. The range of this parameter is 0 to 6.5535 mW.</p> <p><i>low_warning</i> - Low threshold for warning. When the operating parameter falls below this value, action associated with warning is taken. The range of this parameter is 0 to 6.5535 mW.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the port 9's receive power threshold:

```
DGS-3450:admin# :config ddm ports 9 rx_power_threshold high_alarm 4.55 low_alarm 0.01
high_warning 3.5 low_warning 0.03
Command: config ddm ports 9 rx_power_threshold high_alarm 4.55 low_alarm 0.01 high
_warning 3.5 low_warning 0.03

Success.

DGS-3450:admin#
```

config ddm ports state

Purpose	To configure the DDM state or/and DDM shutdown action when encounter an exceeding alarm or warning thresholds event.
Syntax	config ddm ports [<portlist> all] { state [enable disable] shutdown [alarm warning none]} (1)
Description	The command configures the DDM state or (and) DDM shutdown action when encounter an exceeding alarm or warning thresholds event

config ddm ports state

Parameters	<p><i>portlist</i> - Specified a range of ports to be configured. (UnitID: port number).</p> <p><i>all</i> - If 'all' parameter is chosen, all SFP ports' operating parameters will be configured.</p> <p><i>state</i> - Specifies the DDM state, if the state is disabled, no DDM action will take effect.</p> <p><i>shutdown</i> - Specifies whether or not to shutdown the port, on which the operating parameter exceeds the corresponding alarm threshold or warning threshold.</p> <p>Note: The port being shutdown cannot recover to normal operation automatically, using "config ports x state enable" command to recover the port.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the port 11's actions associate with alarm:

```
DGS-3450:admin# config ddm ports 11 state enable shutdown alarm
Command: config ddm ports 11 state enable shutdown alarm

Success.

DGS-3450:admin#
```

config ddm log

Purpose	Enable or disable log action when the SFP exceed its DDM threshold.
Syntax	config ddm log [enable disable]
Description	The command configures the DDM log action when encounter an exceeding alarm or warning thresholds event
Parameters	<i>log</i> - Specifies whether or not to send log, when the operating parameter exceeds the corresponding threshold.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the port 11's log state to enable:

```
DGS-3450:admin# config ddm log enable
Command: config ddm log enable

Success.

DGS-3450:admin#
```

config ddm trap

Purpose	Enable or disable trap action when the SFP exceed its DDM threshold.
Syntax	config ddm trap [enable disable]
Description	The command configures the DDM trap action when encounter an exceeding alarm or warning thresholds event.
Parameters	<i>trap</i> - Specifies whether or not to send trap, when the operating parameter exceeds the corresponding threshold.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the port 11's trap state to enable:

```
DGS-3450:admin# config ddm trap enable
Command: config ddm trap enable

Success.

DGS-3450:admin#
```

show ddm ports status

Purpose	Used to show the current operating DDM parameters values of the SFP module of the specified ports.
Syntax	show ddm ports {<portlist> } status
Description	The command displays the current operating parameters of the SFP modules.
Parameters	<i>portlist</i> - Specified a range of ports to be displayed. (UnitID:port number). If 'all' parameter is chosen, all SFP ports' operating parameters will be displayed.
Restrictions	None.

Example usage:

To show the port 10-12's operating parameters:

```
DGS-3450:admin# show ddm ports 10-12 status
Command: show ddm ports 10-12 status
```

Port	Temperature (in Celsius)	Voltage (V)	Bias Current (mA)	TX Power (mW)	RX Power (mW)
10	-	-	-	-	-
11	21.5	2.5	50	3	4
12	-	-	-	-	-

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

show ddm ports configuration

Purpose	Used to display the current configurations of the digital diagnostics monitoring function
Syntax	show ddm ports {<portlist>} configuration
Description	The command displays the current configurations of the SFP modules. There are two types of threshold, the administrative configuration and the operation configuration threshold. For the SFP port, when a particular threshold was configured by user, it will be shown on this command with a tag indicate that it is a threshold that user configured, else it would be the threshold read from the SFP module that is being inserted.
Parameters	<i>portlist</i> - Specified a range of ports to be displayed. (UnitID: port number). If 'all' parameter is chosen, all SFP ports' operating parameters will be displayed
Restrictions	None.

Example usage:

To show the port 11's configuration:

```
DGS-3450:admin# show ddm ports 11 configuration
Command: show ddm ports 11 configuration

Port 11
-----
DDM state : Enabled
Shutdown  : Alarm

Threshold      Temperature Voltage Bias-Current TX-Power RX-Power
              (in Celsius) (V)      (mA)      (mW)      (mW)
-----
High Alarm    85(A)      6.55     7.25(A)   0.625     4.5
Low Alarm     -10         2.5      0.004     0.006(A)  0.01
High Warning  70(A)      3.5(A)   6         0.5       3.5(A)
Low Warning   0          3        0.006(A) 0.008     0.03

A means that the threshold is administratively configured.

DGS-3450:admin#
```

show ddm

Purpose	Used to display the DDM global setting.
Syntax	show ddm
Description	The command displays the DDM global setting.
Parameters	None.
Restrictions	None.

Example usage:

To display the global DDM setting:

```
DGS-3450:admin# show ddm
Command: show ddm

DDM Log      : Enabled
DDM Trap     : Enabled

DGS-3450:admin#
```

D-LINK SINGLE IP MANAGEMENT COMMANDS

Simply put, D-Link Single IP Management is a concept that will stack switches together over Ethernet instead of using stacking ports or modules. Switches using D-Link Single IP Management (labeled here as SIM) must conform to the following rules:

SIM is an optional feature on the Switch and can easily be enabled or disabled. SIM grouping has no effect on the normal operation of the Switch in the user's network.

There are three classifications for switches using SIM. The Commander Switch(CS), which is the master switch of the group, Member Switch(MS), which is a switch that is recognized by the CS as a member of a SIM group, and a Candidate Switch (CaS), which is a switch that has a physical link to the SIM group but has not been recognized by the CS as a member of the SIM group.

A SIM group can only have one Commander Switch(CS). All switches in a particular SIM group must be in the same IP subnet (broadcast domain). Members of a SIM group cannot cross a router. A SIM group accepts up to 33 switches (numbered 0-32), including the Commander Switch (numbered 0). There is no limit to the number of SIM groups in the same IP subnet (broadcast domain), however a single switch can only belong to one group. If multiple VLANs are configured, the SIM group will only utilize the management VLAN on any switch. SIM allows intermediate devices that do not support SIM. This enables the user to manage a switch that are more than one hop away from the CS.

The SIM group is a group of switches that are managed as a single entity. The DGS-3400 Series may take on three different roles:

1. **Commander Switch (CS)** – This is a switch that has been manually configured as the controlling device for a group, and takes on the following characteristics:
 - a. It has an IP Address.
 - b. It is not a Commander Switch or Member Switch of another Single IP group.
 - c. It is connected to the Member Switches through its management VLAN.
2. **Member Switch (MS)** – This is a switch that has joined a single IP group and is accessible from the CS, and it takes on the following characteristics:
 - a. It is not a CS or MS of another IP group.
 - b. It is connected to the CS through the CS management VLAN.
3. **Candidate Switch (CaS)** – This is a switch that is ready to join a SIM group but is not yet a member of the SIM group. The Candidate Switch may join the SIM group through an automatic function of the DGS-3400, or by manually configuring it to be a MS of a SIM group. A switch configured as a CaS is not a member of a SIM group and will take on the following characteristics:
 - a. It is not a CS or MS of another Single IP group.
 - b. It is connected to the CS through the CS management VLAN.

The following rules also apply to the above roles:

1. Each device begins in the Candidate state.
2. CS's must change their role to CaS and then to MS, to become a MS of a SIM group. Thus the CS cannot directly be converted to a MS.
3. The user can manually configure a CS to become a CaS.
4. A MS can become a CaS by:
 - a. Being configured as a CaS through the CS.
 - b. If report packets from the CS to the MS time out.
5. The user can manually configure a CaS to become a CS
6. The CaS can be configured through the CS to become a MS.

After configuring one switch to operate as the CS of a SIM group, additional xStack® DGS-3400 series switches may join the group by either an automatic method or by manually configuring the Switch to be a MS. The CS will then serve as the in band entry point for access to the MS. The CS's IP address will become the path to all MS's of the group and the CS's Administrator's password, and/or authentication will control access to all MS's of the SIM group.

With SIM enabled, the applications in the CS will redirect the packet instead of executing the packets. The applications will decode the packet from the administrator, modify some data, then send it to the MS. After execution, the CS may receive a response packet from the MS, which it will encode and send back to the administrator.

When a CS becomes a MS, it automatically becomes a member of the first SNMP community (include read/write and read only) to which the CS belongs. However if a MS has its own IP address, it can belong to SNMP communities to which other switches in the group, including the CS, do not belong.

The Upgrade to v1.6

To better improve SIM management, the xStack® DGS-3400 Series switches have been upgraded to version 1.6 in this release. Many improvements have been made, including:

The Commander Switch (CS) now has the capability to automatically rediscover member switches that have left the SIM group, either through a reboot or web malfunction. This feature is accomplished through the use of Discover packets and Maintain packets that previously set SIM members will emit after a reboot. Once a MS has had its MAC address and password saved to the CS's database, if a reboot occurs in the MS, the CS will keep this MS information in its database and when a MS has been rediscovered, it will add the MS back into the SIM tree automatically. No configuration will be necessary to rediscover these switches. There are some instances where pre-saved MS switches cannot be rediscovered. For example, if the Switch is still powered down, if it has become the member of another group, or if it has been configured to be a Commander Switch, the rediscovery process cannot occur.

This version will support multiple switch upload and downloads for firmware, configuration files and log files, as follows:

- Firmware – The switch now supports MS firmware downloads from a TFTP server.
- Configuration Files – This switch now supports downloading and uploading of configuration files both to (for configuration restoration) and from (for configuration backup) MS's, using a TFTP server..
- Log – The switch now supports uploading MS log files to a TFTP server.



NOTE: For more details regarding improvements made in SIMv1.6, please refer to the Single IP Management White Paper located on the D-Link website.

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

Command	Parameters
enable sim	
disable sim	
show sim	{[candidates {<candidate_id 1-100>} members {<member_id 1-32>} group {commander_mac <macaddr>} neighbor]}
reconfig	{member_id <value 1-32> exit}
config sim_group	[add <candidate_id 1-100> {<password>} delete <member_id 1-32>]
config sim	[[commander {group_name <groupname 64>} candidate] dp_interval <sec 30-90> hold_time <sec 100-255>]
download sim_ms	[firmware_from_tftp configuration_from_tftp] <ipaddr> <path_filename> {[members <mclist 1-32> all]}
upload sim_ms	[configuration_to_tftp log_to_tftp] <ipaddr> <path_filename> {[members <mclist> all]}

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

enable sim

Purpose	Used to enable Single IP Management (SIM) on the Switch
Syntax	enable sim
Description	This command will enable SIM globally on the Switch. SIM features and functions will not function properly unless this function is enabled.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable SIM on the Switch:

```
DGS-3450:admin# enable sim
Command: enable sim
```

Success.

```
DGS-3450:admin#
```

disable sim

Purpose	Used to disable Single IP Management (SIM) on the Switch.
Syntax	disable sim
Description	This command will disable SIM globally on the Switch.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To disable SIM on the Switch:

```
DGS-3450:admin# disable sim
Command: disable sim

Success.

DGS-3450:admin#
```

show sim

Purpose	Used to view the current information regarding the SIM group on the Switch.
Syntax	show sim {[candidates {<candidate_id 1-100>} members {<member_id 1-32>} group { commander_mac <macaddr>} neighbor]}
Description	<p>This command will display the current information regarding the SIM group on the Switch, including the following:</p> <p>SIM Version – Displays the current Single IP Management version on the Switch.</p> <p>Firmware Version – Displays the current Firmware version on the Switch.</p> <p>Device Name – Displays the user-defined device name on the Switch.</p> <p>MAC Address – Displays the MAC Address of the Switch.</p> <p>Capabilities – Displays the type of switch, be it Layer 2 (L2) or Layer 3 (L3).</p> <p>Platform – Switch Description including name and model number.</p> <p>SIM State – Displays the current Single IP Management State of the Switch, whether it be enabled or disabled.</p> <p>Role State – Displays the current role the Switch is taking, including Commander, Member or Candidate. A Stand-alone switch will always have the commander role.</p> <p>Discovery Interval – Time in seconds the Switch will send discovery packets out over the network.</p> <p>Hold time – Displays the time in seconds the Switch will hold discovery results before dropping it or utilizing it.</p>
Parameters	<p><i>candidates</i> <candidate_id 1-100> – Entering this parameter will display information concerning candidates of the SIM group. To view a specific candidate, include that candidate's ID number, listed from 1 to 100.</p> <p><i>members</i> <member_id 1-32> – Entering this parameter will display information concerning members of the SIM group. To view a specific member, include that member's id number, listed from 1 to 32.</p> <p><i>group</i> {<i>commander_mac</i> <macaddr>} – Entering this parameter will display information concerning the SIM group. To view a specific group, include the commander's MAC address of the group.</p> <p><i>neighbor</i> – Entering this parameter will display neighboring devices of the Switch. A SIM neighbor is defined as a switch that is physically connected to the Switch but is not part of the SIM group. This screen will produce the following results:</p> <ul style="list-style-type: none"> • Port – Displays the physical port number of the commander switch where the uplink to the neighbor switch is located. • MAC Address – Displays the MAC Address of the neighbor switch. • Role – Displays the role(CS, CaS, MS) of the neighbor switch.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To show the SIM information in detail:


```
DGS-3450:admin# show sim
Command: show sim

SIM Version       : VER-1.61
Firmware Version  : 2.70.B56
Device Name       :
MAC Address       : 00-19-5B-F5-26-C0
Capabilities      : L3
Platform          : DGS-3450 L3 Switch
SIM State         : Disabled
Role State        : Candidate
Discovery Interval : 30 sec
Holdtime          : 100 sec

DGS-3450:admin#
```

To show the candidate information in summary, if the candidate ID is specified:

```
DGS-3450:admin# show sim candidates
Command: show sim candidates

ID   MAC Address           Platform /           Hold   Firmware   Device Name
   MAC Address           Capability           Time   Version
---  -
2    00-55-55-00-55-00    DGS-3450 L3 Switch  140    2.70.B56   default master

Total Entries: 2

DGS-3450:admin#
```

To show the member information in summary, if the member ID is specified:

```
DGS-3450:admin# show sim member 1
Command: show sim member 1

ID   MAC Address           Platform /           Hold   Firmware   Device Name
   MAC Address           Capability           Time   Version
---  -
1    00-01-02-03-04-00    DGS-3450 L3 Switch  40     2.70.B56   The Man

Total Entries: 2

DGS-3450:admin#
```

To show other groups information in summary:

```
DGS-3450:admin# show sim group
```

```
Command: show sim group
```

```
SIM Group Name : default
```

ID	MAC Address	Platform / Capability	Hold Time	Firmware Version	Device Name
*1	00-01-02-03-04-00	DGS-3450 L3 Switch	40	2.70.B56	Tiberius

```
SIM Group Name : SIM2
```

ID	MAC Address	Platform / Capability	Hold Time	Firmware Version	Device Name
*1	00-01-02-03-04-00	DGS-3450 L3 Switch	40	2.70.B56	Neo

```
`*' means commander switch.
```

```
DGS-3450:admin#
```

Example usage:

To view SIM neighbors:

```
DGS-3450:admin# show sim neighbor
```

```
Command: show sim neighbor
```

```
Neighbor Info Table
```

Port	MAC Address	Role
23	00-35-26-00-11-99	Commander
23	00-35-26-00-11-91	Member
24	00-35-26-00-11-90	Candidate

```
Total Entries: 3
```

```
DGS-3450:admin#
```

reconfig

Purpose	Used to connect to a member switch, through the commander switch, using telnet.
Syntax	reconfig {member_id <value 1-32> exit}
Description	This command is used to reconnect to a member switch using Telnet.
Parameters	<i>member_id</i> <value 1-32> – Select the ID number of the member switch the user desires to configure. <i>exit</i> – This command is used to exit from managing the member switch and will return to managing the commander switch.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To connect to the MS, with member ID 2, through the CS, using the command line interface:

```
DGS-3450:admin# reconfig member_id 2
Command: reconfig member_id 2

DGS-3450:admin#
Login:
```

config sim_group

Purpose	Used to add candidates and delete members from the SIM group.
Syntax	config sim [add <candidate_id 1-100> {<password>} delete <member_id 1-32>]
Description	This command is used to add candidates and delete members from the SIM group by ID number.
Parameters	<p><i>add <candidate_id 1-100> <password></i> – Use this parameter to change a candidate switch (CaS) to a member switch (MS) of a SIM group. The CaS may be defined by its ID number and a password (if necessary).</p> <p><i>delete <member_id 1-32></i> – Use this parameter to delete a member switch of a SIM group. The member switch should be defined by ID number.</p>
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To add a member:

```
DGS-3450:admin# config sim_group add 2
Command: config sim_group add 2

Please wait for ACK!!!
SIM Config Success !!!

Success.

DGS-3450:admin#
```

To delete a member:

```
DGS-3450:admin# config sim_group delete 1
Command: config sim_group delete 1

Please wait for ACK!!!
SIM Config Success!!!

Success.

DGS-3450:admin#
```

config sim

Purpose	Used to configure role parameters for the SIM protocol on the Switch.
Syntax	config sim [[commander {group_name <groupname 64>} candidate] dp_interval <sec 30-90> hold_time <sec 100-255>]}
Description	This command is used to configure parameters of switches of the SIM.
Parameters	<i>commander</i> – Use this parameter to configure the commander switch(CS) for the following parameters:

config sim

- *group_name <groupname 64>* – Used to update the name of the group. Enter an alphanumeric string of up to 64 characters to rename the SIM group.
 - *dp_interval <30-90>* – The user may set the discovery protocol interval, in seconds that the Switch will send out discovery packets. Returning information to the CS will include information about other switches connected to it. (Ex. MS, CaS). The user may set the *dp_interval* from 30 to 90 seconds.
 - *hold time <sec 100-255>* – Using this parameter, the user may set the time, in seconds, the CS will hold information sent to it from other switches, utilizing the discovery interval protocol. The user may set the hold time from 100 to 255 seconds.
- candidate* – Used to change the role of a CS (commander) to a CaS (candidate).
- *dp_interval <30-90>* – The user may set the discovery protocol interval, in seconds that the Switch will send out discovery packets. Returning information to the CS will include information about other switches connected to it. (Ex. MS, CaS). The user may set the *dp_interval* from 30 to 90 seconds.
 - *hold time <100-255>* – Using this parameter, the user may set the time, in seconds, the Switch will hold information sent to it from other switches, utilizing the discovery interval protocol. The user may set the hold time from 100 to 255 seconds.

Restrictions

Only Administrator-level users can issue this command.

To change the time interval of the discovery protocol:

```
DGS-3450:admin# config sim commander dp_interval 40
Command: config sim commander dp_interval 40

Success.

DGS-3450:admin#
```

To change the hold time of the discovery protocol:

```
DGS-3450:admin# config sim hold_time 120
Command: config sim hold_time 120

Success.

DGS-3450:admin#
```

To transfer the CS (commander) to be a CaS (candidate):

```
DGS-3450:admin# config sim candidate
Command: config sim candidate

Success.

DGS-3450:admin#
```

To transfer the Switch to be a CS:

```
DGS-3450:admin# config sim commander
Command: config sim commander

Success.

DGS-3450:admin#
```

To update the name of a group:

```
DGS-3450:admin# config sim commander group_name Demetrius
Command: config sim commander group_name Demetrius

Success.

DGS-3450:admin#
```

download sim_ms

Purpose	Used to download firmware or configuration file to an indicated device.
Syntax	download sim_ms [firmware_from_tftp configuration_from_tftp] <ipaddr> <path_filename> {[members <mslist 1-32> all]}
Description	This command will download a firmware file or configuration file to a specified device from a TFTP server.
Parameters	<p><i>firmware_from_tftp</i> – Specify this parameter to download firmware to members of a SIM group.</p> <p><i>configuration_from_tftp</i> – Specify this parameter to download a switch configuration to members of a SIM group.</p> <p><i><ipaddr></i> – Enter the IP address of the TFTP server.</p> <p><i><path_filename></i> – Enter the path and the filename of the firmware or switch on the TFTP server.</p> <p><i>members</i> – Enter this parameter to specify the members the user prefers to download firmware or switch configuration files to. The user may specify a member or members by adding one of the following:</p> <ul style="list-style-type: none"> ▪ <i><mslist 1-32></i> – Enter a value, or values to specify which members of the SIM group will receive the firmware or switch configuration. ▪ <i>all</i> – Add this parameter to specify all members of the SIM group will receive the firmware or switch configuration.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To download firmware:

```
DGS-3450:admin# download sim_ms firmware_from_tftp 10.53.13.94 c:/dgs3450.had all
Command: download sim_ms firmware_from_tftp 10.53.13.94 c:/dgs3450.had all
```

This device is updating firmware. Please wait...

Download Status :

ID	MAC Address	Result
1	00-01-02-03-04-00	Success
2	00-07-06-05-04-03	Success
3	00-07-06-05-04-03	Success

```
DGS-3450:admin#
```

To download configuration files:

```
DGS-3450:admin# download sim_ms configuration_from_tftp 10.53.13.94 c:/dgs3450.txt all
Command: download sim_ms configuration_from_tftp 10.53.13.94 c:/dgs3450.txt all
```

This device is updating configuration. Please wait...

Download Status :

ID	MAC Address	Result
1	00-01-02-03-04-00	Success
2	00-07-06-05-04-03	Success
3	00-07-06-05-04-03	Success

```
DGS-3450:admin#
```

upload sim_ms

Purpose	User to upload a configuration file to a TFTP server from a specified member of a SIM group.
Syntax	upload sim_ms [configuration_to_tftp log_to_tftp] <ipaddr> <path_filename> {[members <mclist> all]}
Description	This command will upload a configuration file to a TFTP server from a specified member of a SIM group.
Parameters	<p><i>configuration_to_tftp</i> – Specify this parameter if the user wishes to upload a switch configuration to members of a SIM group.</p> <p><i>log_to_tftp</i> – Specify this parameter to download a switch log to members of a SIM group.</p> <p><i><ipaddr></i> – Enter the IP address of the TFTP server to upload a configuration file to.</p> <p><i><path_filename></i> – Enter a user-defined path and file name on the TFTP server to which to upload configuration files.</p> <p><i>members</i> – Enter this parameter to specify the members the user prefers to upload switch configuration or log files to. The user may specify a member or members by adding one of the following:</p> <ul style="list-style-type: none"> ▪ <i><mclist></i> – Enter a value, or values to specify which members of the SIM group will receive the switch configuration or log files. ▪ <i>all</i> – Add this parameter to specify all members of the SIM group will receive the switch configuration or log files.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To upload configuration files to a TFTP server:

```
DGS-3450:admin# upload sim_ms configuration 10.55.47.1 D:\configuration.txt 1  
Command: upload sim_ms configuration 10.55.47.1 D:\configuration.txt 1
```

```
Success.
```

```
DGS-3450:admin#
```

D-LINK UNIDIRECTIONAL LINK DETECTION (DULD) COMMANDS

The D-Link Unidirectional Link Detection (DULD) Resolver commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameters
config duld ports	[<portlist> all] {state [enable disable] mode [shutdown normal] discovery_time <sec 5-65535>}(1)
show duld ports	{<portlist>}

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

config duld ports

Purpose	Used to configure unidirectional link detection on port
Syntax	config duld ports [<portlist> all] {state [enable disable] mode [shutdown normal] discovery_time <sec 5-65535>}(1)
Description	The command used to configure unidirectional link detection on ports. Unidirectional link detection provides discovery mechanism based on 802.3ah to discover its neighbor. If the OAM discovery can complete in configured discovery time, it concludes the link is bidirectional. Otherwise, it starts detecting task to detect the link status.
Parameters	<p><portlist> - Specify a range of ports.</p> <p>state - Specifies these ports unidirectional link detection status. The default state is disabled.</p> <p>mode - See below:</p> <p style="padding-left: 20px;"><i>shutdown</i> - If any unidirectional link is detected, disable the port and log an event.</p> <p style="padding-left: 20px;"><i>normal</i> - Only log an event when a unidirectional link is detected.</p> <p>discovery_time - Specifies these ports neighbor discovery time. If the discovery is timeout, the unidirectional link detection will start. The default discovery time is 5 seconds.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable unidirectional link detection on port 1:

```
DGS-3450:admin# config duld ports 1 state enable
```

```
Commands: config duld ports 1 state enable
```

Success

```
DGS-3450:admin#
```

show duld

Purpose	Used to show unidirectional link detection information
Syntax	show duld ports {<portlist>}
Description	The command used to show ports unidirectional link information including: Admin state: port's unidirectional link detection configuration state. Discovery Time: the neighbor discovery timer. Link Status: port's link detection result. It maybe

show duld

1. Unknown: either local or remote do not support OAM or unidirectional detection.
2. Bidirectional
3. TX Fault
4. RX Fault
5. Link Down

Oper Status: indicates the detection is operational or not.

1. Enabled: the port supports OAM and unidirectional detection and discover remote peer supporting this detection capability.
2. Disabled: either local or remote do not support OAM or unidirectional detection.

So we should enable OAM when we need to detect the unidirectional link.

Parameters

<portlist> - Specify a range of ports to display.

If no port specified, all ports will be displayed.

Restrictions

Only Administrator and Operator-level users can issue this command.

Example usage:

To show ports 1-4 unidirectional link detection information:

```
DGS-3450:admin# config duld ports 1,2,4 state enable
```

```
Commands: config duld ports 1,2,4 state enable
```

Success

```
DGS-3450:admin# show duld ports 1-4
```

```
Commands: show duld ports 1-4
```

port	Admin State	Oper Status	Mode	Link Status	Discovery Time(Sec)
1	Enabled	Enabled	Shutdown	Bidirectional	5
2	Enabled	Enabled	Normal	RX Fault	5
3	Enabled	Enabled	Normal	TX Fault	5
4	Disabled	Disabled	Normal	Unknown	5
5	Enabled	Enabled	Normal	Link Down	5

```
DGS-3450:admin#
```

DOMAIN NAME SERVER (DNS) RESOLVER COMMANDS

The Domain Name Server (DNS) Resolver commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameters
config name_server	[[add delete] <ipaddr> {primary} timeout <second 1-60>]
show name_server	
create host_name	<name 255> <ipaddr>
delete host_name	[<name 255> all]
show host_name	{static dynamic}
enable dns_resolver	
disable dns_resolver	

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

config name_server

Purpose	Used to configure the DNS Resolver name server of the switch.
Syntax	config name_server [[add delete] <ipaddr> {primary} timeout <second 1-60>]
Description	<p>The config name_server command is used to configure the DNS Resolver name server of the switch. Note that only when add a name server, the parameter “primary” will be resolved. Other conditions won’t resolve the parameter “primary”. It means that when delete a name server, just check the IP address. If the IP address is the same to the name server’s, the name server will be deleted, don’t check the priority parameter.</p> <p>When adding a name server, if one primary name server exists in the static name server table, then add a new primary name server, the existing primary name server will be changed to a normal name server. If the added primary name server’s IP address is the same to an existed normal name server’s IP address, the existing normal name server will be changed to a primary name server, but won’t add new name server. When no primary name server is specified, the first configured name server will auto change to primary name server.. If the deleted name server’s IP address equals to one of the existing name servers’ IP addresses, regardless whether a normal name server or primary name server, the name server will be deleted.</p>
Parameters	<p><i>add</i> - Add DNS Resolver name server</p> <p><i>delete</i> - Delete DNS Resolver name server</p> <p><i>ipaddr</i> - The DNS Resolver name server IP address</p> <p><i>timeout</i> - The maximum time waiting for a response from a specified name server.</p> <p><i>primary</i> - Specify the name server is a primary name server.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To add DNS Resolver primary name server 10.10.10.10:

```
DGS-3450:admin# config name_server add 10.10.10.10 primary
Command: config name_server add 10.10.10.10 primary

Success.

DGS-3450:admin#
```

To delete DNS Resolver name server 10.10.10.1:

```
DGS-3450:admin# config name_server delete 10.10.10.10
Command: config name_server delete 10.10.10.10

Success.

DGS-3450:admin#
```

To configure DNS Resolver name server time out to 10 seconds:

```
DGS-3450:admin# config name_server timeout 10
Command: config name_server timeout 10

Success.

DGS-3450:admin#
```

show name_server

Purpose	Used to display the current DNS Resolver name servers and name server time out on the switch.
Syntax	show name_server
Description	The show name_server command is used to display the current DNS Resolver name servers and name server time out on the switch.
Parameters	None.
Restrictions	None.

Example usage:

To display the current DNS Resolver name servers and name server time out:

```
DGS-3450:admin# show name_server
```

```
Command: show name_server
```

```
Name Server Timeout: 3 seconds
```

```
Static Name Server Table:
```

```
Server IP Address      Priority
-----
20.20.20.20           Secondary
10.1.1.1              Primary
```

```
Dynamic Name Server Table:
```

```
Server IP Address      Priority
-----
10.48.74.122         Primary
```

```
DGS-3450:admin#
```

create host_name

Purpose	Used to create the static host name entry of the switch.
Syntax	create host_name <name 255> <ipaddr>
Description	The create host name command is used to create the static host name entry of the switch. If the created host name entry exists in the dynamic host name table, the existing dynamic host name entry will be deleted, and then add the created host name entry is added into the static host name table and a log for duplicate is recorded.
Parameters	<name 255> - The host's host name <ipaddr> - The host's IP address
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create static host name "www.example.com":

```
DGS-3450:admin# create host_name www.example.com 10.10.10.10
```

```
Command: create host_name www.example.com 10.10.10.10
```

```
Success.
```

```
DGS-3450:admin#
```

delete host_name

Purpose	Used to delete the static or dynamic host name entries of the switch.
Syntax	delete host_name [<name 255> all]
Description	The delete host_name command is used to delete the static or dynamic host name entries of the switch.
Parameters	<name 255> - The host's host name. all - All of the static and dynamic host name entries.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete the static host name entry “www.example.com”:

```
DGS-3450:admin# delete host_name www.example.com
Command: delete host_name www.example.com

Success.

DGS-3450:admin#
```

show host_name

Purpose	Used to display the current host name.
Syntax	show host_name {static dynamic}
Description	The show host_name command is used to display the current host name entries. If the parameters for “static” and “dynamic” are not specified, both static and dynamic host name entries will be displayed.
Parameters	<i>static</i> - Display the static host name entries <i>dynamic</i> - Display the dynamic host name entries
Restrictions	None.

Example usage:

To display the static and dynamic host name entries:

```
DGS-3450:admin# show host_name
Command: show host_name

Static Host Name Table
Host Name                IP Address
-----
www.example.com          10.10.10.10
www.exampla.com          20.20.20.20

Total Static Entries: 2

Dynamic Host Name Table
Host Name                IP Address      TTL
-----
www.examplc.com          30.30.30.30    60 minutes
www.exampld.com          40.40.40.40    10 minutes

Total Dynamic Entries: 2

DGS-3450:admin#
```

enable dns_resolver

Purpose	Used to configure the DNS Resolver state of the switch to enabled.
Syntax	enable dns_resolver
Description	The enable dns_resolver command is used to configure the switch’s DNS Resolver state.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the DNS Resolver state to enabled:

```
DGS-3450:admin# enable dns_resolver
Command: enable dns_resolver

Success.

DGS-3450:admin#
```

disable dns_resolver

Purpose	Used to configure the DNS Resolver state of the switch to disabled.
Syntax	disable dns_resolver
Description	The disable dns_resolver command is used to configure the switch's DNS Resolver state to disabled.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the DNS Resolver state to disabled:

```
DGS-3450:admin# disable dns_resolver
Command: disable dns_resolver

Success.

DGS-3450:admin#
```

DOMAIN NAME SERVER (DNS) RELAY COMMANDS

The Domain Name Server (DNS) relay commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameters
config dnsr	[[primary secondary] nameserver <ipaddr> [add delete] static <domain_name 32> <ipaddr>]
enable dnsr	{[cache static]}
disable dnsr	{[cache static]}
show dnsr	{static}

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

config dnsr

Purpose	Used to configure the DNS relay function.
Syntax	config dnsr [[primary secondary] nameserver <ipaddr> [add delete] static <domain_name 32> <ipaddr>]
Description	This command is used to configure the DNS relay function on the Switch.
Parameters	<p><i>primary</i> – Indicates that the IP address below is the address of the primary DNS server.</p> <p><i>secondary</i> – Indicates that the IP address below is the address of the secondary DNS server.</p> <p><i>nameserver <ipaddr></i> – The IP address of the DNS nameserver.</p> <p><i>[add delete]</i> – Indicates whether to add or delete the DNS relay function.</p> <p><i><domain_name 32></i> – The domain name of the entry.</p> <p><i><ipaddr></i> – The IP address of the entry.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To set IP address 10.43.21.12 of primary.

```
DGS-3450:admin# config dnsr primary nameserver 10.43.21.12
Command: config dnsr primary nameserver 10.43.21.12

Success

DGS-3450:admin#
```

Example usage:

To add an entry domain name dns1, IP address 10.43.21.12 to DNS static table:

```
DGS-3450:admin# config dnsr add static dns1 10.43.21.12
Command: config dnsr add static dns1 10.43.21.12

Success.

DGS-3450:admin#
```

Example usage:

To delete an entry domain name dns1, IP address 10.43.21.12 from DNS static table.

```
DGS-3450:admin# config dnsr delete static dns1 10.43.21.12
Command: config dnsr delete static dns1 10.43.21.12

Success.

DGS-3450:admin#
```

enable dnsr

Purpose	Used to enable DNS relay.
Syntax	enable dnsr {[cache static]}
Description	This command is used, in combination with the disable dnsr command below, to enable and disable DNS Relay on the Switch.
Parameters	<i>cache</i> – This parameter will allow the user to enable the cache lookup for the DNS relay on the Switch. <i>static</i> – This parameter will allow the user to enable the static table lookup for the DNS relay on the Switch.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable status of DNS relay:

```
DGS-3450:admin# enable dnsr
Command: enable dnsr

Success.

DGS-3450:admin#
```

Example usage:

To enable cache lookup for DNS relay.

```
DGS-3450:admin# enable dnsr cache
Command: enable dnsr cache

Success.

DGS-3450:admin#
```

Example usage:

To enable static table lookup for DNS relay.


```
DGS-3450:admin# enable dnsr static
Command: enable dnsr static

Success.

DGS-3450:admin#
```

disable dnsr

Purpose	Used to disable DNS relay on the Switch.
Syntax	disable dnsr {[cache static]}
Description	This command is used, in combination with the enable dnsr command above, to enable and disable DNS Relay on the Switch.
Parameters	<i>cache</i> – This parameter will allow the user to disable the cache lookup for the DNS relay on the Switch. <i>static</i> – This parameter will allow the user to disable the static table lookup for the DNS relay on the Switch.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable status of DNS relay.

```
DGS-3450:admin# disable dnsr
Command: disable dnsr

Success.

DGS-3450:admin#
```

Example usage:

To disable cache lookup for DNS relay.

```
DGS-3450:admin# disable dnsr cache
Command: disable dnsr cache

Success.

DGS-3450:admin#
```

Example usage:

To disable static table lookup for DNS relay.

```
DGS-3450:admin# disable dnsr static
Command: disable dnsr static

Success.

DGS-3450:admin#
```

show dnsr

Purpose	Used to display the current DNS relay status.
---------	---

show dnsr

Syntax	show dnsr {static}
Description	This command is used to display the current DNS relay status.
Parameters	<i>static</i> – Allows the display of only the static entries into the DNS relay table. If this parameter is omitted, the entire DNS relay table will be displayed.
Restrictions	None.

Example usage:

To display DNS relay status:

```
DGS-3450:admin# show dnsr
Command: show dnsr
DNSR Status           : Disabled
Primary Name Server   : 0.0.0.0
Secondary Name Server : 0.0.0.0
DNSR Cache Status     : Disabled
DNSR Static Table Status : Disabled

DNS Relay Static Table

Domain Name           IP Address
-----
www.123.com.tw       10.12.12.123

Total Entries: 1

DGS-3450:admin#
```

ETHERNET RING PROTECTION SWITCHING (ERPS) COMMANDS

ITU-T G.8032 Ethernet Ring protection switching (ERPS) is used to provide a reliable mechanism of malfunction recovery in an Ethernet ring topology network.

The Ethernet Ring Protection Switching (ERPS) Resolver commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameters
enable erps	
disable erps	
create erps raps_vlan	<vlanid>
delete erps raps_vlan	<vlanid>
config erps raps_vlan	<vlanid> ring mel <value 0-7>
config erps raps_vlan	<vlanid> ring_port [west [<port> virtual_channel] east [<port> virtual_channel]]
config erps raps_vlan	<vlanid> [rpl_port [west east none] rpl_owner [enable disable]]
config erps raps_vlan	<vlanid> protected_vlan [add delete] vlanid <vidlist>
config erps raps_vlan	<vlanid> timer { holdoff_time <value 0-10000> guard_time <value 10-2000> wtr_time <min 5-12>} (1)
config erps log	[enable disable]
show erps	{raps_vlan <vlanid> {sub_ring}}
config erps trap	[enable disable]
config erps raps_vlan	<vlanid> state [enable disable]
config erps raps_vlan	<vlanid> [add delete] sub_ring raps_vlan <vlanid>
config erps raps_vlan	<vlanid> sub_ring raps_vlan <vlanid> tc_propagation state [enable disable]

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

enable erps

Purpose	Used to enable the global ERPS function on a switch.
Syntax	enable erps
Description	<p>This command is used to enable the global ERPS function on a switch. When both the global state and the specified ring ERPS state are enabled, the specified ring will be activated.</p> <p>The global ERPS function cannot be enabled, when any ERPS ring on the device is enabled and the integrity of any ring parameter is not available. For each ring with the ring state enabled when ERPS is enabled, the following integrity will be checked:</p> <ol style="list-style-type: none"> 1. R-APS VLAN is created. 2. The Ring port is a tagged member port of the R-APS VLAN. 3. The RPL port is specified if the RPL owner is enabled. <p>The default state is disabled.</p>
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable ERPS:

```
DGS-3450:admin# enable erps
Command: enable erps

Success.

DGS-3450:admin#
```

disable erps

Purpose	Used to disable the global ERPS function on a switch.
Syntax	disable erps
Description	This command is used to disable the global ERPS function on a switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable ERPS:

```
DGS-3450:admin# disable erps
Command: disable erps

Success.

DGS-3450:admin#
```

create erps raps_vlan

Purpose	Used to create an R-APS VLAN on a switch.
Syntax	create erps raps_vlan <vlanid>
Description	This command is used to create an R-APS VLAN on a switch. Only one R-APS VLAN should be used to transfer R-APS messages. Note: The R-APS VLAN must already have been created by the create vlan command.
Parameters	<i>raps_vlan</i> - Specifies the VLAN which will be the R-APS VLAN.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create and ERPS R-APS VLAN:

```
DGS-3450:admin# create erps raps_vlan 4094
Command: create erps raps_vlan 4094

Success.

DGS-3450:admin#
```

delete erps raps_vlan

Purpose	Used to delete an R-APS VLAN on a switch.
Syntax	delete erps raps_vlan <vlanid>
Description	This command is used to delete an R-APS VLAN on a switch. When an R-APS VLAN is deleted, all parameters related to this R-APS VLAN will also be deleted. This command can only be issued when the ring is not active.
Parameters	<i>raps_vlan</i> - Specifies the VLAN which will be the R-APS VLAN.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete an ERPS R-APS VLAN:

```
DGS-3450:admin# delete erps raps_vlan 4094
Command: delete erps raps_vlan 4094
Success.

DGS-3450:admin#
```

config erps ring_mel

Purpose	Used to configure the MEL of the ERPS ring for a specific R-APS VLAN.
Syntax	config erps raps_vlan <vlanid> ring mel <value 0-7>
Description	This command is used to configure the ring MEL for a R-APS VLAN. The ring MEL is one field in the R-APS PDU. Note: If CFM (Connectivity Fault Management) and ERPS are used at the same time, the R-APS PDU is one of a suite of Ethernet OAM PDU. The behavior for forwarding of R-APS PDU should follow the Ethernet OAM. If the MEL of R-APS PDU is not higher than the level of the MEP with the same VLAN on the ring ports, the R-APS PDU cannot be forwarded on the ring.
Parameters	<i>ring mel</i> - Specifies the ring MEL of the R-APS function. The default ring MEL is 1.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure a MEL of the ERPS ring:

```
DGS-3450:admin# config erps raps_vlan 4094 ring mel 2
Command: config erps raps_vlan 4094 ring mel 2

Success.

DGS-3450:admin#
```

config erps raps_vlan ring_port

Purpose	Used to configure the ports of the ERPS ring for a specific R-APS VLAN.
Syntax	config erps raps_vlan <vlanid> ring_port [west [<port> virtual_channel] east [<port> virtual_channel]]
Description	This command is used to configure the port that participates in the ERPS ring. Restrictions apply for ports that are included in a link aggregation group. A link aggregation group can be

config erps raps_vlan ring_port

configured as a ring port by specifying the master port of the link aggregation port. Only the master port can be specified as a ring port. If the specified link aggregation group is eliminated, the master port retains its ring port status. If the ring port configured on virtual channel, the ring which the port connects to will be considered as a sub-ring.

Note: The ring ports cannot be modified when ERPS is enabled.

Parameters

west <port> - Specifies the port as the west ring port.

virtual_channel - Specifies the port as west port on virtual channel.

east <port> - Specifies the port as the east ring port.

virtual_channel - Specifies the port as east port on virtual channel.

Restrictions

Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the ports of an ERPS ring for a specific R-APS VLAN:

```
DGS-3450:admin# config erps raps_vlan 4094 ring_port west 5 east 7
```

```
Command: config erps raps_vlan 4094 ring_port west 5 east 7
```

Success.

```
DGS-3450:admin#
```

config erps raps_vlan rpl

Purpose

Used to configure the RPL port or the RPL owner for a specific R-APS VLAN.

Syntax

```
config erps raps_vlan <vlanid> [ rpl_port [west | east | none] | rpl_owner [enable | disable] ]
```

Description

This command is used to configure the RPL port and the RPL owner.

RPL port: Specifies one of the R-APS VLAN ring ports as the RPL port. To remove an RPL port from an R-APS VLAN, use the none designation for rpl_port.

RPL owner: Specifies the node as the RPL owner.

Note: The RPL port and RPL owner cannot be modified when ERPS is enabled; and the virtual channel cannot be configured as RPL. For example, if a ring port is configured on the virtual channel and the ring port is configured as an RPL port, an error message will be display and the configuration will fail.

Parameters

port - See below.

west - Specifies the west ring port as the RPL port.

east - Specifies the east ring port as the RPL port.

none - No RPL port on this node. By default, the node has no RPL port.

owner - See below.

enable - Specifies the device as an RPL owner node.

disable - This node is not an RPL owner. By default, the RPS owner is disabled.

Restrictions

Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the RPL port or the RPL owner for a specific R-APS VLAN:

```
DGS-3450:admin# config erps raps_vlan 4094 rpl port west owner enable
Command: config erps raps_vlan 4094 rpl port west owner enable

Success.

DGS-3450:admin#
```

config erps raps_vlan protected_vlan

Purpose	Used to configure the protected VLAN for a specific R-APS VLAN.
Syntax	config erps raps_vlan <vlanid> protected_vlan [add delete] vlanid <vidlist>
Description	This command is used to configure the VLANs that are protected by the ERPS function. The R-APS VLAN cannot be the protected VLAN. The protected VLAN can be one that has already been created, or it can be used for a VLAN that has not yet been created.
Parameters	<i>protected_vlan</i> - See below: <i>add</i> - Add VLANs to the protected VLAN group. <i>delete</i> - Delete VLANs from the protected VLAN group.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the protected VLAN for a specific R-APS VLAN:

```
DGS-3450:admin# config erps raps_vlan 4094 protected_vlan add vlanid 10-20
Command: config erps raps_vlan 4094 protected_vlan add vlanid 10-20

Success.

DGS-3450:admin#
```

config erps raps_vlan timer

Purpose	Used to configure the ERPS timers for a specific R-APS VLAN.
Syntax	config erps raps_vlan <vlanid> timer { holdoff_time <value 0-10000> guard_time <value 10-2000> wtr_time <min 5-12>} (1)
Description	This command is used to configure the protocol timers. Holdoff timer: The Holdoff timer is used to filter out intermittent link faults when link failures occur during the protection switching process. When a ring node detects a link failure, it will start the holdoff timer and report the link failure event (R-APS BPDU with SF flag) after the link failure is confirmed within period of time specified. Guard timer: Guard timer is used to prevent ring nodes from receiving outdated R-APS messages. This timer is used during the protection switching process after the link failure recovers. When the link node detects the recovery of the link, it will report the link failure recovery event (R-APS PDU with NR flag) and start the guard timer. Before the guard timer expires, all received R-APS messages are ignored by this ring node, except in the case where a burst of three R-APS event messages that indicates the topology of a sub-ring has changed and the node needs to flush FDB are received on the node. In this case the recovered link does not go into a blocking state. The Guard Timer should be greater than the maximum expected forwarding delay for which one R-APS message circles around the ring. WTR timer: WTR timer is used to prevent frequent operation of the protection switch due to an intermittent defect. This timer is used during the protection switching process when a link failure recovers. It is only used by the RPL owner. When the RPL owner in protection state receives R-APS PDU with an NR flag, it will start the WTR timer. The RPL owner will block

config erps raps_vlan timer

	the original unblocked RPL port and start to send R-APS PDU with an RB flag after the link recovery is confirmed within this period of time.
Parameters	<p><i>holdoff_time</i> - Specifies the holdoff time of the R-APS function. The default holdoff time is 0 milliseconds.</p> <p><i>guard_time</i> - Specifies the guard time of the R-APS function. The default guard time is 500 milliseconds.</p> <p><i>wtr_time</i> - Specifies the WTR time of the R-APS function. The range is from 5 to 12 minutes. The default WTR time is 5 minutes.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the ERPS timers for a specific R-APS VLAN:

```
DGS-3450:admin# config erps raps_vlan 4094 holdoff_time 100 guard_time 1000 wtr_time 10
Command: config erps raps_vlan 4094 holdoff_time 100 guard_time 1000 wtr_time 10
```

Success.

```
DGS-3450:admin#
```

config erps log

Purpose	Used to configure the ERPS log state.
Syntax	config erps log [enable disable]
Description	This command is used to configure the log state of ERPS events.
Parameters	<i>log</i> - Enable or disable the log state. The default value is disabled.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the ERPS log state:

```
DGS-3450:admin# config erps log enable
Command: config erps log enable
```

Success.

```
DGS-3450:admin#
```

show erps

Purpose	Used to display ERPS information.
Syntax	show erps {raps_vlan <vlanid> {sub_ring}}
Description	<p>This command is used to display ERPS configuration and operation information.</p> <p>The port state of the ring port may be as "Forwarding", "Blocking", "Signal Fail". "Forwarding" indicates that traffic is able to be forwarded. "Blocking" indicates that traffic is blocked by ERPS and a signal failure is not detected on the port. "Signal Fail" indicates that a signal failure is detected on the port and traffic is blocked by ERPS.</p> <p>The RPL owner administrative state could be configured to "Enabled" or "Disabled". But the RPL owner operational state may be different from the RPL owner administrative state, for</p>

show erps

example, the RPL owner conflict occurs. "Active" is used to indicate that the RPL owner administrative state is enabled and the device is operated as the active RPL owner. "Inactive" is used to indicate that the RPL owner administrative state is enabled, but the device is operated as the inactive RPL owner.

Parameters *raps_vlan* <vlanid> - Specifies the R-APS VLAN.
 sub_ring - Display sub-ring configuration information.

Restrictions None.

Example usage:

To display ERPS information:

```

DGS-3450:admin# show erps
Command: show erps

ERPS Information
Global Status      : Enabled
Log Status         : Disabled
Trap Status       : Disabled
-----
R-APS VLAN        : 4092
Ring Status       : Enabled
West Port         : 5 (Blocking)
East Port         : 7 (Forwarding)
RPL Port         : West Port
RPL Owner         : Enabled (Active)
Protected VLANs   : 100-300, 4093, 4094
Ring MEL          : 2
Holdoff Time      : 0 milliseconds
Guard Time       : 500 milliseconds
WTR Time         : 5 minutes
Current Ring State : Idle
-----
R-APS VLAN        : 4093
Ring Status       : Enabled
West Port         : Virtual Channel
East Port         : 10 (Forwarding)
RPL Port         : None
RPL Owner         : Disabled
Protected VLANs   : 200-220
Ring MEL          : 2
Holdoff Time      : 0 milliseconds
Guard Time       : 500 milliseconds
WTR Time         : 5 minutes
Current Ring State : Idle
-----
R-APS VLAN        : 4094
Ring Status       : Enabled
West Port         : Virtual Channel
East Port         : 12 (Forwarding)
RPL Port         : None
RPL Owner         : Disabled
Protected VLANs   : 250-300
Ring MEL          : 2
Holdoff Time      : 0 milliseconds
Guard Time       : 500 milliseconds
WTR Time         : 5 minutes
Current Ring State : Idle
-----
Total Ring: 3

DGS-3450:admin#

```

config erps trap

Purpose	Used to configure the trap state of the ERPS.
Syntax	config erps trap [enable disable]
Description	This command is used to configure trap state of ERPS events.
Parameters	<i>trap</i> - Enable or disable trap state. The default value is disabled.

config erps trap

Restrictions	Only Administrator and Operator-level users can issue this command.
--------------	---

Example usage:

To configure the trap state of the ERPS:

```
DGS-3450:admin# config erps trap enable
Command: config erps trap enable

Success.

DGS-3450:admin#
```

config erps raps_vlan state

Purpose	Used to configure the state of the specified ring.
Syntax	config erps raps_vlan <vlanid> state [enable disable]
Description	<p>This command is used to configure ring state of the specified ring. When both the global state and the specified ring ERPS state are enabled, the specified ring will be activated. STP and LBD should be disabled on the ring ports before the specified ring is activated.</p> <p>The ring cannot be enabled before the R-APS VLAN is created, and ring ports, RPL port, RPL owner, are configured. Note that these parameters cannot be changed when the ring is activated.</p> <p>In order to guarantee correct operation, the following integrity will be checked when the ring is enabled and the global ERPS state is enabled.</p> <ol style="list-style-type: none"> 1. R-APS VLAN is created. 2. The Ring port is the tagged member port of the R-APS VLAN. 3. The RPL port is specified if RPL owner is enabled. <p>The default state of the ring is disabled.</p>
Parameters	<p><i>state</i> - See below:</p> <ul style="list-style-type: none"> <i>enable</i> - Enable the state of the specified ring. <i>disable</i> - Disable the state of the specified ring. <p>The default value is disabled.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the ring state of the ERPS:

```
DGS-3450:admin# config erps raps_vlan state enable
Command: config erps raps_vlan state enable

Success.

DGS-3450:admin#
```

config erps raps_vlan sub_ring

Purpose	Used to configure a sub-ring connected to another ring.
Syntax	config erps raps_vlan <vlanid> [add delete] sub_ring raps_vlan <vlanid>

config erps raps_vlan sub_ring

Description	This command is used to configure a sub-ring connected to another ring. This command is applied on the interconnection node.
Parameters	<i>raps_vlan</i> <vlanid> - Specifies the R-APS VLAN. <i>add</i> - Connect the sub-ring to another ring. <i>delete</i> - Disconnect the sub-ring from the connected ring.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure a sub-ring connected to another ring:

```
DGS-3450:admin# config erps raps_vlan 4094 add sub_ring raps_vlan 4093
Command: config erps raps_vlan 4094 add sub_ring raps_vlan 4093

Success.

DGS-3450:admin#
```

config erps raps_vlan tc_propagation

Purpose	Used to configure the state of topology change propagation for the sub-ring.
Syntax	config erps raps_vlan <vlanid> sub_ring raps_vlan <vlanid> tc_propagation state [enable disable]
Description	This command is used to configure the state of topology change propagation for the sub-ring. This command is applied on the interconnection node.
Parameters	<i>raps_vlan</i> <vlanid> - Specifies the R-APS VLAN. <i>state</i> - See below: <i>enable</i> - Enable the propagation state of topology change for the sub-ring. <i>disable</i> - Disable the propagation state of topology change for the sub-ring. The default value is disabled.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the state of topology change propagation:

```
DGS-3450:admin# config erps raps_vlan 4094 sub_ring raps_vlan 4093 tc_propagation state enable
Command: config erps raps_vlan 4094 sub_ring raps_vlan 4093 tc_propagation state enable

Success.

DGS-3450:admin#
```

FILTER DATABASE (FDB) COMMANDS

This section describes the Filter Database functionality and specifications based on IEEE 802.1d 2001 standard and IEEE 802.1Q-2003 standard. Functions of this software module apply on L2 and L3 Ethernet switches.

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

Command	Parameters
create fdb	<vlan_name 32> <macaddr> port <port>
create multicast_fdb	<vlan_name 32> <macaddr>
config multicast_fdb	<vlan_name 32> <macaddr> [add delete] <portlist>
config fdb aging_time	<sec 10-1000000>
config multicast filtering_mode	[vlan <vlan_name 32> all][forward_all_groups forward_unregistered_groups filter_unregistered_groups]
delete fdb	<vlan_name 32> <macaddr>
clear fdb	[vlan <vlan_name 32> port <port> all]
show multicast_fdb	{[vlan <vlan_name 32> vlanid <vidlist >]} mac_address <macaddr>}
show fdb	{port <port> [vlan <vlan_name 32> vlanid <vidlist>] mac_address <macaddr> static aging_time}
show multicast filtering_mode	{vlan <vlan_name 32>}

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

create fdb

Purpose	Used 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 places an entry into the switch's unicast MAC address forwarding database
Parameters	<i>vlan_name</i> - Specifies a VLAN name associated with a MAC address. <i>macaddr</i> - The MAC address to be added to the static forwarding table. <i>port</i> - 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 and Operator-level users can issue this command.

Example usage:

To create a unicast MAC forwarding:

```
DGS-3450:admin# create fdb default 00-00-00-00-01-02 port 2:5
Command: create fdb default 00-00-00-00-01-02 port 2:5
```

Success.

```
DGS-3450:admin#
```

create multicast_fdb

Purpose	Used to create a static entry in the multicast MAC address forwarding table (database).
Syntax	create multicast_fdb <vlan_name 32> <macaddr>
Description	The create multicast_fdb is used to make an entry in the switch's multicast MAC address forwarding database.
Parameters	<i>vlan_name</i> - The name of the VLAN on which the MAC address resides. The maximum length is 32. <i>macaddr</i> - The multicast MAC address to be added to the static forwarding table.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create multicast MAC forwarding:

```
DGS-3450:admin# create multicast_fdb default 01-00-00-00-00-00
Command: create multicast_fdb default 01-00-00-00-00-00

Success.

DGS-3450:admin#
```

config multicast_fdb

Purpose	Used to configure the switch's multicast MAC address forwarding database.
Syntax	config multicast_fdb <vlan_name 32> <macaddr> [add delete] <portlist>
Description	The config multicast_fdb command is used to configure the multicast MAC address forwarding table.
Parameters	<i>vlan_name</i> - The name of the VLAN on which the MAC address resides. The maximum name length is 32. <i>macaddr</i> - The MAC address that will be added or deleted to the forwarding table. <i>portlist</i> - Specifies a range of ports to be configured. (UnitID: port number).
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To add multicast MAC forwarding:

```
DGS-3450:admin# config multicast_fdb default 01-00-00-00-00-00 add 1:1-1:5
Command: config multicast_fdb default 01-00-00-00-00-00 add 1:1-1:5

Success.

DGS-3450:admin#
```

config fdb aging_time

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

config fdb aging_time

Parameters	<i>aging_time</i> - Specifies the time, in seconds, that a dynamically learned MAC address will remain in the switch's MAC address forwarding table, without being accessed, before being dropped from the database. The range of the value is 10 to 1000000.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the MAC address aging time:

```
DGS-3450:admin# config fdb aging_time 300
```

```
Command: config fdb aging_time 300
```

```
Success.
```

```
DGS-3450:admin#
```

config multicast filtering_mode

Purpose	Used to configure the multicast packet filtering mode for VLANs.
Syntax	config multicast filtering_mode [<vlan_name 32> all] [forward_all_groups forward_unregistered_groups filter_unregistered_groups]
Description	The config multicast_fdb command configures the multicast packet filtering mode for VLANs. This switch support vlan filtering mode.
Parameters	<i>vlan_name</i> - Specifies the name of the VLAN. <i>forward_all_groups</i> - All multicast groups forwarded based on VLAN. <i>forward_unregistered_groups</i> - The registered group forwarded based on register table. The un-register group forwarded based on VLAN. <i>filter_unregistered_groups</i> - The registered group forwarded based on register table. The un-register group filtered.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the multicast packet filtering mode for VLANs:

```
DGS-3450:admin# config multicast filtering_mode 200 forward_all_groups
```

```
Command: config multicast filtering_mode 200 forward_all_groups
```

```
Success.
```

```
DGS-3450:admin#
```

delete fdb

Purpose	Used to delete an entry from the switch's forwarding database.
Syntax	delete fdb <vlan_name 32> <macaddr>
Description	The delete fdb deletes a permanent FDB entry.
Parameters	<i>vlan_name</i> - The name of the VLAN on which the MAC address resides. The maximum length is 32 characters. <i>macaddr</i> - The multicast MAC address to be deleted from the static forwarding table.

delete fdb

Restrictions	Only Administrator and Operator-level users can issue this command.
--------------	---

Example usage:

To delete a permanent FDB entry:

```
DGS-3450:admin# delete fdb default 00-00-00-00-01-02
Command: delete fdb default 00-00-00-00-01-02

Success.

DGS-3450:admin#
```

clear fdb

Purpose	Used to clear the switch's forwarding database of all dynamically learned MAC addresses.
Syntax	clear fdb [vlan <vlan_name 32> port <port> all]
Description	The clear fdb command clears all dynamically learned MAC addresses from the switch's forwarding database..
Parameters	<i>vlan_name</i> - The name of the VLAN on which the MAC address resides. The maximum length is 32 characters. <i>port</i> - 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 and Operator-level users can issue this command.

Example usage:

To clear all FDB dynamic entries:

```
DGS-3450:admin# clear fdb all
Command: clear fdb all

Success.

DGS-3450:admin#
```

show multicast_fdb

Purpose	Used to display the contents of the switch's multicast forwarding database.
Syntax	show multicast_fdb {[vlan <vlan_name 32> vlanid <vidlist >] mac_address <macaddr>}
Description	The show multicast_fdb command displays the entries of the switch's multicast forwarding database.
Parameters	<i>vlan_name</i> - The name of the VLAN on which the MAC address resides. The maximum length is 32 characters. <i>vlanid</i> - Display the entries for the VLANs indicated by VID list. <i>macaddr</i> - Specifies a MAC address, for which FDB entries will be displayed. If no parameter is specified, all multicast FDB entries will be displayed.
Restrictions	None.

Example usage:

To display the multicast MAC address table:

```
DGS-3450:admin# show multicast_fdb
Command: show multicast_fdb

VLAN Name      : default
MAC Address     : 01-00-00-00-00-01
Egress Ports   : 1:1-1:5,1:26,2:26
Mode           : Static

Total Entries : 1
```

show fdb

Purpose	Used to display the current unicast MAC address forwarding database.
Syntax	show fdb { port <port> [vlan <vlan_name 32> vlanid <vidlist>] mac_address <macaddr> static aging_time}
Description	The show fdb command displays the current unicast MAC address forwarding database.
Parameters	<p><i>port</i> - Displays the entries for one port.</p> <p><i>vlan_name</i> - Displays the entries for a specific VLAN.</p> <p><i>vlanid</i> - Display the entries for the VLANs indicated by VID list.</p> <p><i>static</i> - Displays all permanent entries.</p> <p><i>aging_time</i> - Displays the unicast MAC address aging time.</p> <p>If no parameter is specified, system will display the unicast address table.</p>
Restrictions	None.

Example usage:

To display the FDB table:

DGS-3450:admin# show fdb

Command: show fdb

Unicast MAC Address Aging Time = 300

VID	VLAN Name	MAC Address	Port	Type
1	default	00-00-00-00-01-02	2:5	Permanent
1	default	00-01-02-03-04-00	CPU	Self
2	VLAN_2	00-00-01-02-03-04	-	Permanently Drop
1	default	00-00-00-00-00-07	1:3	Permanent
1	default	00-00-00-00-00-08	1:4	BlockByAddrBind
1	default	00-00-00-00-00-09	1:4	UnblockByAddrBind
1	default	00-00-00-00-00-10	1:5	BlockByMBA
1	default	00-00-00-00-00-11	1:5	UnBlockByMBA
1	default	00-00-00-00-00-12	1:6	BlockBySecurity
1	default	00-00-00-00-00-13	1:6	UnBlockBySecurity
1	default	00-00-00-00-00-14	1:7	JWAC_Authing
1	default	00-00-00-00-10-15	1:7	JWAC_Authed
1	default	00-00-00-00-10-16	1:7	JWAC_Blocked
1	default	00-00-00-00-10-18	1:8	Asymmetric_VLAN
1	default	00-00-00-00-10-19	-	BlackHole
1	default	00-00-00-00-10-21	1:11	Del_on_Reset
1	default	00-00-00-00-10-22	1:12	Del_on_Timeout
1	default	00-00-00-00-10-23	1:13	Secured_Permanent
1	default	00-00-00-00-10-24	1:14	Del_on_Reset
1	default	00-00-00-00-10-25	1:15	SVL

Total Entries: 19

DGS-3450:admin#

show multicast filtering_mode

Purpose	Used to show the multicast packet filtering mode for VLANs.
Syntax	show multicast filtering_mode {vlan <vlan_name 32>}
Description	The show multicast vlan_filtering_mode command show the multicast packet filtering mode for VLAN.
Parameters	<i>vlan</i> – Specifies the VLAN name to be configured. If no parameter is specified, the device will show all multicast filtering settings in the device.
Restrictions	None.

Example usage:

To show the multicast filtering_mode for VLANs:

```
DGS-3450:admin# show multicast filtering_mode
```

```
Command: show multicast filtering_mode
```

VLAN Name	Multicast Filter Mode
-----	-----
default	forward_unregistered_groups
n61	forward_unregistered_groups
n101	forward_unregistered_groups
n103	forward_unregistered_groups
n172	forward_unregistered_groups
sue	forward_unregistered_groups

```
DGS-3450:admin#
```

GRATUITOUS ARP COMMANDS

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

Command	Parameters
config gratuitous_arp send ipif_status_up	[enable disable]
config gratuitous_arp send dup_ip_detected	[enable disable]
config gratuitous_arp learning	[enable disable]
config gratuitous_arp send periodically	ipif <ipif_name 12> interval <value 0-65535>
enable gratuitous_arp	{ipif <ipif_name 12>} {trap log}
disable gratuitous_arp	{ipif <ipif_name 12>} {trap log}
show gratuitous_arp	{ipif <ipif_name 12>}

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

config gratuitous_arp send ipif_status_up

Purpose	Used to enable or disable send gratuitous ARP request while IP interface status become up.
Syntax	config gratuitous_arp send ipif_status_up [enable disable]
Description	The command is used to enable/disable sending of gratuitous ARP request packet while IPIF interface become up. This is used to automatically announce the interface's IP address to other nodes. By default, the state is disabled. After enable this state, one gratuitous ARP packet will be broadcast.
Parameters	<i>enable</i> - Enable sending of gratuitous ARP when IPIF status become up. <i>disable</i> - Disable sending of gratuitous ARP when IPIF status become up.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable send gratuitous ARP request in normal situation:

```
DGS-3450:admin# config gratuitous_arp send ipif_status_up enable
Command: config gratuitous_arp send ipif_status_up enable

Success.
DGS-3450:admin#
```

config gratuitous_arp send dup_ip_detected

Purpose	Used to enable or disable sending of gratuitous ARP request while duplicate IP address is detected.
Syntax	config gratuitous_arp send dup_ip_detected [enable disable]
Description	The command is used to enable/disable sending of gratuitous ARP request packet while duplicate IP is detected. By default, the state is disabled. For this command, the duplicate IP

config gratuitous_arp send dup_ip_detected

detected means that the system received an ARP request packet that is sent by an IP address that match the system's own IP address. In this case, the system knows that some body out there uses an IP address that is conflict with the system. In order to reclaim the correct host of this IP address, the system can send out the gratuitous ARP request packet for this duplicate IP address.

Parameters	<i>enable</i> - Enable sending of gratuitous ARP when duplicate IP is detected. <i>disable</i> - Disable sending of gratuitous ARP when duplicate IP is detected.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable send gratuitous ARP request when duplicate IP is detected:

```
DGS-3450:admin# config gratuitous_arp send dup_ip_detected enable
Command: config gratuitous_arp send dup_ip_detected enable

Success.
DGS-3450:admin#
```

config gratuitous_arp learning

Purpose	Used to enable or disable learning of ARP entry in ARP cache based on the received gratuitous ARP packet.
Syntax	config gratuitous_arp learning [enable disable]
Description	Normally, the system will only learn the ARP reply packet or a normal ARP request packet that asks for the MAC address that corresponds to the system's IP address. The command is used to enable/disable learning of ARP entry in ARP cache based on the received gratuitous ARP packet. The gratuitous ARP packet is sent by a source IP address that is identical to the IP that the packet is queries for. Note that, with the gratuitous ARP learning, the system will not learn new entry but only do the update on the ARP table based on the received gratuitous ARP packet. By default, the state is disabled.
Parameters	<i>enable</i> - Enable learning of ARP entry based on the received gratuitous ARP packet. <i>disable</i> - Disable learning of ARP entry based on the received gratuitous ARP packet.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable update ARP table when Gratuitous ARP received:

```
DGS-3450:admin# config gratuitous_arp learning enable
Command: config gratuitous_arp learning enable

Success.
DGS-3450:admin#
```

config gratuitous_arp periodical_send

Purpose	Used to configure the interval for periodical sending of gratuitous ARP request packet.
Syntax	config gratuitous_arp send periodically ipif <ipif_name 12> interval <value 0-65535>
Description	The command is used to configure the interval for periodical sending of gratuitous ARP request packet. By default, the interval is 0.

config gratuitous_arp periodical_send

Parameters	<i>ipif</i> <ipif_name 12> - Interface name of L3 interface. <i>interval</i> <value 0-65535> - Periodically send gratuitous ARP interval time in seconds.0 means not send gratuitous ARP periodically.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure gratuitous ARP interval to 5 for IPIF System:

```
DGS-3450:admin# config gratuitous_arp send periodically ipif System interval 5
Command: config gratuitous_arp send periodically ipif System interval 5
```

```
Success.
DGS-3450:admin#
```

enable gratuitous_arp trap

Purpose	Used to enable gratuitous ARP trap and log state.
Syntax	enable gratuitous_arp {ipif <ipif_name 12>} {trap log}
Description	The command is used to enable gratuitous ARP trap and log state. The switch can trap and log the IP conflict event to inform the administrator. By default, trap is disabled and event log is enabled.
Parameters	<i>ipif</i> <ipif_name 12> - Interface name of L3 interface <i>trap</i> – Specify to enable traps for gratuitous ARP. <i>log</i> – Specify to enable the log for gratuitous ARP.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable system interface's gratuitous ARP log and trap:

```
DGS-3450:admin# enable gratuitous_arp ipif System trap log
Command: enable gratuitous_arp ipif System trap log
```

```
Success.
DGS-3450:admin#
```

disable gratuitous_arp trap

Purpose	Used to disable interface's gratuitous ARP log and trap.
Syntax	disable gratuitous_arp {ipif <ipif_name 12>} {trap log}
Description	The command is used to disable gratuitous ARP trap and log state.
Parameters	<i>ipif</i> <ipif_name 12> - Interface name of L3 interface <i>trap</i> – Specify to disable traps for gratuitous ARP. <i>log</i> – Specify to disable the log for gratuitous ARP.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable system interface's gratuitous ARP log and trap:

```
DGS-3450:admin# disable gratuitous_arp ipif System trap log
Command: disable gratuitous_arp ipif System trap log

Success.
DGS-3450:admin#
```

show gratuitous_arp

Purpose	Used to display gratuitous ARP configuration.
Syntax	show gratuitous_arp {ipif <ipif_name 12>}
Description	The show gratuitous_arp command is used to display gratuitous ARP configuration.
Parameters	<i>ipif <ipif_name 12></i> - Interface name of L3 interface.
Restrictions	None.

Example usage:

To display gratuitous ARP configuration:

```
DGS-3450:admin# show gratuitous_arp
Command: show gratuitous_arp

Send on IPIF status up           : Enabled
Send on Duplicate_IP_Detected    : Disabled
Gratuitous ARP Learning          : Enabled

IP Interface Name : System
Gratuitous ARP Trap           : Disabled
Gratuitous ARP Log           : Enabled
Gratuitous ARP Periodical Send Interval : 5

IP Interface Name : ip1
Gratuitous ARP Trap           : Enabled
Gratuitous ARP Log           : Disabled
Gratuitous ARP Periodical Send Interval : 6

Total Entries: 2

DGS-3450:admin#
```

IEEE 802.1Q VLAN COMMANDS

Along with normal VLAN configurations, this Switch now incorporate Double VLANs. Better known as Q-IN-Q VLANs, Double VLANs allow network providers to expand their VLAN configurations to place VLANs within a larger inclusive VLAN, which adds a new layer to the VLAN configuration. This basically lets large ISP's create L2 Virtual Private Networks and also create transparent LANs for their customers, which will connect two or more customer LAN points without over complicating configurations on the client's side. Not only will over-complication be avoided, but now the administrator has over 4000 VLANs in which over 4000 VLANs can be placed, therefore greatly expanding the VLAN network.

Implementation of this feature adds a VLAN frame to an existing VLAN frame for the ISP VLAN recognition and classification. To ensure devices notice this added VLAN frame, an Ethernet encapsulation, here known as a tpid, is also added to the frame. The device recognizes this tpid and therefore checks the VLAN tagged packet to see if a provider VLAN tag has been added. If so, the packet is then routed through this provider VLAN, which contains smaller VLANs with similar configurations to ensure speedy and guaranteed routing destination of the packet.

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

Command	Parameters
create vlan	<vlan_name 32> {tag <vlanid 2-4094> type 1q_vlan advertisement}
delete vlan	<vlan_name 32>
config vlan	<vlan_name 32> {[add [tagged untagged forbidden] delete] <portlist> advertisement [enable disable]}
config gvrp	[<portlist> all] {state [enable disable] ingress_checking [enable disable] acceptable_frame [tagged_only admit_all] pvid <vlanid 1-4094>}
enable gvrp	
disable gvrp	
show vlan	{<vlan_name 32> vlanid <vidlist> ports <portlist>}
show gvrp	{<portlist>}
enable double_vlan	
disable double_vlan	
create double_vlan	<vlan_name 32> spvid <vlanid 1-4094> {tpid <hex 0x0-0xffff>}
config double_vlan	<vlan_name> {[add [access uplink] delete] <portlist> tpid <hex 0x0-0xffff>}
delete double_vlan	<vlan_name>
show double_vlan	{<vlan_name>}
enable pvid auto_assign	
disable pvid auto_assign	
show pvid auto_assign	

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

create vlan

Purpose	Used to create a VLAN on the Switch.
Syntax	create vlan <vlan_name 32> {tag <vlanid 2-4094> type 1q_vlan advertisement}
Description	This command allows the creation of a VLAN on the Switch.
Parameters	<p><i><vlan_name 32></i> – The name of the VLAN to be created.</p> <p><i>tag <vlanid 2-4094></i> – The VLAN ID of the VLAN to be created. Allowed values = 2-4094</p> <p><i>type</i> – This parameter uses the <i>type</i> field of the packet header to determine the packet protocol and destination VLAN:</p> <p><i>1q_vlan</i> – Allows the creation of a normal 802.1Q VLAN on the Switch.</p> <p><i>advertisement</i> – Specifies that the VLAN is able to join GVRP.</p>
Restrictions	Each VLAN name can be up to 32 characters. Only Administrator and Operator-level users can issue this command.

Example usage:

To create a VLAN v1, tag 2:

```
DGS-3450:admin# create vlan v1 tag 2
Command: create vlan v1 tag 2

Success.

DGS-3450:admin#
```

delete vlan

Purpose	Used to delete a previously configured VLAN on the Switch.
Syntax	delete vlan <vlan_name 32>
Description	This command will delete a previously configured VLAN on the Switch.
Parameters	<i><vlan_name 32></i> – The VLAN name of the VLAN to delete.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To remove the VLAN "v1":

```
DGS-3450:admin# delete vlan v1
Command: delete vlan v1

Success.

DGS-3450:admin#
```

config vlan add

Purpose	Used to add additional ports to a previously configured VLAN.
Syntax	config vlan <vlan_name 32> {[add [tagged untagged forbidden] delete] <portlist> advertisement [enable disable]}
Description	This command is used to add ports to the port list of a previously configured VLAN. Additional ports may be specified as tagging, untagging, or forbidden. The default is to assign the ports as untagging.
Parameters	<p><i><vlan_name 32></i> – The name of the VLAN to add or delete ports to.</p> <p><i>add</i> – Specifies which ports to add. The user may also specify if the ports are:</p> <ul style="list-style-type: none"> • <i>tagged</i> – Specifies the additional ports as tagged. • <i>untagged</i> – Specifies the additional ports as untagged. • <i>forbidden</i> – Specifies the additional ports as forbidden. <p><i>delete</i> – Specifies which ports to delete.</p> <p><i><portlist></i> – A port or range of ports to add to the VLAN. The beginning and end of the port list range are separated by a dash.</p> <p><i>advertisement [enable disable]</i> – Enables or disables GVRP on the specified VLAN.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

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

```
DGS-3450:admin# config vlan v1 add tagged 1:4-1:8
Command: config vlan v1 add tagged 1:4-1:8
```

Success.

```
DGS-3450:admin#
```

config gvrp

Purpose	Used to configure GVRP on the Switch.
Syntax	config gvrp [<portlist> all] {state [enable disable] ingress_checking [enable disable] acceptable_frame [tagged_only admit_all] pvid <vlanid 1-4094>}
Description	This command is used to configure the GARP VLAN Registration Protocol on the Switch. Configurable settings include ingress checking, the sending and receiving of GVRP information, and the Port VLAN ID (PVID).
Parameters	<p><i><portlist></i> – A port or range of ports for which to configure GVRP. The beginning and end of the port list range are separated by a dash.</p> <p><i>all</i> – Specifies all of the ports on the Switch.</p> <p><i>state [enable disable]</i> – Enables or disables GVRP for the ports specified in the port list.</p> <p><i>ingress_checking [enable disable]</i> – Enables or disables ingress checking for the specified port list.</p> <p><i>acceptable_frame [tagged_only admit_all]</i> – This parameter states the frame type that will be accepted by the Switch for this function. <i>tagged_only</i> implies that only VLAN tagged frames will be accepted, while <i>admit_all</i> implies tagged and untagged frames will be accepted by the Switch.</p> <p><i>pvid</i> – Specifies the default VLAN ID associated with the port.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

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

```
DGS-3450:admin# config gvrp 1:1-1:4 state enable ingress_checking enable acceptable_frame
tagged_only pvid 2
Command: config gvrp 1:1-1:4 state enable ingress_checking enable acceptable_frame
tagged_only pvid 2

Success.

DGS-3450:admin#
```



NOTE: When the PVID Auto Assign function is disabled, users must manually configure the PVID for untagged ports or the host may not connect to the Switch correctly.

enable gvrp

Purpose	Used to enable GVRP on the Switch.
Syntax	enable gvrp
Description	This command, along with disable gvrp below, is used to enable and disable GVRP globally on the Switch, without changing the GVRP configuration on the Switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable the generic VLAN Registration Protocol (GVRP):

```
DGS-3450:admin# enable gvrp
Command: enable gvrp

Success.

DGS-3450:admin#
```

disable gvrp

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

Example usage:

To disable the Generic VLAN Registration Protocol (GVRP):

```
DGS-3450:admin# disable gvrp
Command: disable gvrp

Success.

DGS-3450:admin#
```

show vlan

Purpose	Used to display the current VLAN configuration on the Switch.
Syntax	show vlan {[<vlan_name 32> vlanid <vidlist>] ports <portlist>}
Description	This command displays summary information about each VLAN including the VLAN ID, VLAN name, the Tagging/Untagging status, and the Member/Non-member/Forbidden status of each port that is a member of the VLAN.
Parameters	<vlan_name 32> – The VLAN name of the VLAN for which to display a summary of settings. vlanid <vidlist> – Users may alternately choose the VLAN to be displayed by entering the VLAN ID. ports <portlist> – Users may also view VLANs by designated port.
Restrictions	None.

Example usage:

To display the Switch's current VLAN settings:

```
DGS-3450:admin# show vlan
Command: show vlan

VID          : 1          VLAN Name    : default
VLAN Type    : Static    Advertisement : Enabled
Member Ports : 1:1-1:25
Static Ports : 1:1-1:25
Current Tagged Ports :
Current Untagged Ports: 1:1-1:25
Static Tagged Ports :
Static Untagged Ports : 1:1-1:25
Forbidden Ports :

VID          : 4094      VLAN Name    : v1
VLAN Type    : Static    Advertisement : Disabled
Member Ports : 1:4,1:8
Static Ports : 1:4,1:8
Current Tagged Ports : 1:4,1:8
Current Untagged Ports:
Static Tagged Ports : 1:4,1:8
Static Untagged Ports :
Forbidden Ports :

Total Entries: 2

DGS-3450:admin#
```

show gvrp

Purpose	Used to display the GVRP status for a port list on the Switch.
Syntax	show gvrp {<portlist>}
Description	This command displays the GVRP status for a port list on the Switch.
Parameters	<portlist> – Specifies a range of ports for which the GVRP status is to be displayed. The beginning and end of the port list range are separated by a dash. Non-contiguous portlist entries are separated by a comma. (ex: 1-3,7-9)
Restrictions	None.

Example usage:

To display GVRP port status:

```
DGS-3450:admin# show gvrp
```

```
Command: show gvrp
```

```
Global GVRP : Disabled
```

Port	PVID	GVRP	Ingress Checking	Acceptable Frame Type
1:1	1	Disabled	Enabled	All Frames
1:2	1	Disabled	Enabled	All Frames
1:3	1	Disabled	Enabled	All Frames
1:4	1	Disabled	Enabled	All Frames
1:5	1	Disabled	Enabled	All Frames
1:6	1	Disabled	Enabled	All Frames
1:7	1	Disabled	Enabled	All Frames
1:8	1	Disabled	Enabled	All Frames
1:9	1	Disabled	Enabled	All Frames
1:10	1	Disabled	Enabled	All Frames
1:11	1	Disabled	Enabled	All Frames
1:12	1	Disabled	Enabled	All Frames
1:13	1	Disabled	Enabled	All Frames
1:14	1	Disabled	Enabled	All Frames
1:15	1	Disabled	Enabled	All Frames
1:16	1	Disabled	Enabled	All Frames
1:17	1	Disabled	Enabled	All Frames
1:18	1	Disabled	Enabled	All Frames

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

enable double_vlan

Purpose	Used to enable the Double VLAN feature on the Switch.
Syntax	enable double_vlan
Description	This command, along with the disable double_vlan command, enables and disables the Double Tag VLAN. When Double VLANs are enabled, the system configurations for VLANs will return to the default setting, except IP address, log, user accounts and banner setting, in order to enable the Double VLAN mode. In the Double VLAN mode, normal VLANs and GVRP functions are disabled. The Double VLAN default setting is disabled.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable the Double VLAN feature on the Switch, thus disabling normal VLANs and GVRP.

```
DGS-3450:admin# enable double_vlan
Command: enable double_vlan
Current Double VLAN mode : Disabled
Enable Double VLAN need to reset system config. Are you sure?(y/n)y

Success.

DGS-3450:admin#
```

disable double_vlan

Purpose	Used to disable the Double VLAN feature on the Switch.
Syntax	disable double_vlan
Description	This command, along with the enable double_vlan command, enables and disables the Double Tag VLAN. When Double VLANs are enabled, the system configurations for VLANs will return to the default setting, except IP address, log, user accounts, and banner setting, in order to enable the Double VLAN mode. In the Double VLAN mode, normal VLANs and GVRP functions are disabled. The Double VLAN default setting is disabled.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable the Double VLAN feature on the Switch

```
DGS-3450:admin# disable double_vlan
Command: disable double_vlan
Current Double VLAN mode : Enabled
Disable Double VLAN need to reset system config. Are you sure?(y/n)y

Success.

DGS-3450:admin#
```

create double_vlan

Purpose	Used to create a Double VLAN on the Switch.
Syntax	create double_vlan <vlan_name 32> spvid <vlanid 1-4094> {tpid <hex 0x0-0xffff>}
Description	This command is used to create a Double VLAN (service provider VLAN) on the Switch.
Parameters	<p><i>vlan <vlan_name 32></i> – The name of the Double VLAN to be created. The user is to enter an alphanumeric string of up to 32 characters to identify this VLAN.</p> <p><i>spvid <vlanid 1-4094></i> – The VLAN ID of the service provider VLAN. The user is to identify this VLAN with a number between 1 and 4094.</p> <p><i>tpid <hex 0x0-0xffff></i> – The tag protocol ID. This ID, identified here in hex form, will help identify packets to devices as Double VLAN tagged packets. The default setting is 0x8100.</p>
Restrictions	Only Administrator and Operator-level users can issue this command. Users must have the Switch enabled for Double VLANs.

Example usage:

To create a Double VLAN on the Switch

```
DGS-3450:admin# create double_vlan RG spvid 2 tpid 0x9100
Command: create double_vlan RG spvid 2 tpid 0x9100

Success.

DGS-3450:admin#
```

config double_vlan

Purpose	Used to config the parameters for a previously created Double VLAN on the Switch.
Syntax	config double_vlan <vlan_name> [[[add [access uplink] delete] <portlist> tpid <hex 0x0-0xffff>]]
Description	This command is used to configure a Double VLAN (service provider VLAN) on the Switch.
Parameters	<p><i>vlan</i> <vlan_name 32> – The name of the Double VLAN to be configured. The user is to enter an alphanumeric string of up to 32 characters to identify this VLAN.</p> <p><i>add</i> – Specify this parameter to add ports configured in the <portlist> as one of the two following types of ports.</p> <ul style="list-style-type: none"> <i>uplink</i> – Add this parameter to configure these ports as uplink ports. Uplink ports are for connecting Switch VLANs to the Provider VLANs on a remote source. Only gigabit ports can be configured as uplink ports. <i>access</i> – Add this parameter to configure these ports as access ports. Access ports are for connecting Switch VLANs to customer VLANs. <i>portlist</i> – Enter a list of ports to be added to this VLAN. The beginning and end of the port list range are separated by a dash. Non-contiguous portlist entries are separated by a comma. (ex: 1-3,7-9) <p><i>delete</i> – Specify this parameter to delete ports configured in the <portlist> from this VLAN.</p> <ul style="list-style-type: none"> <i>portlist</i> – Enter a list of ports to be deleted from this VLAN. The beginning and end of the port list range are separated by a dash. Non-contiguous portlist entries are separated by a comma. (ex: 1-3,7-9) <p><i>tpid</i> <hex 0x0-0xffff> – The tag protocol ID. This ID, identified here in hex form, will help identify packets to devices as Double VLAN tagged packets. The default setting is 0x8100.</p>
Restrictions	Only Administrator and Operator-level users can issue this command. Users must have the Switch enabled for Double VLANs.

Example usage:

To add ports 4 through 8 as access ports to the Double VLAN “RG”:

```
DGS-3450:admin# config double_vlan RG add access 1:4-1:8
Command: config double_vlan RG add access 1:4-1:8

Success.

DGS-3450:admin#
```

Example usage:

To delete ports 4 through 8 on the Double VLAN “RG”:

```
DGS-3450:admin# config double_vlan Drazen delete 1:4-1:8
Command: config double_vlan Drazen delete 1:4-1:8

Success.

DGS-3450:admin#
```

show double_vlan

Purpose	Used to display the Double VLAN settings on the Switch.
Syntax	show double_vlan {<vlan_name>}
Description	This command will display the current double VLAN parameters configured on the Switch.
Parameters	<i>vlan_name</i> – Enter the name of a previously created VLAN for which to display the settings.
Restrictions	None.

Example usage:

To display parameters for the Double VLAN “RG”:

```
DGS-3450:admin# show double_vlan RG
Command: show double_vlan RG

Global Double VLAN : Enabled
=====
SPVID           : 2
VLAN Name       : RG
TPID            : 0x9100
Uplink Ports    :
Access Ports    : 1:4-1:8
Unknow Ports    :
-----
Total Entries   : 1
DGS-3450:admin#
```

enable pvid auto_assign

Purpose	Used to enable auto assignment of PVID.
Syntax	enable pvid auto_assign
Description	If “Auto-assign PVID” is enabled, PVID will be possibly changed by PVID or VLAN configuration. When a user configures a port to VLAN X’s untagged membership, this port’s PVID will be updated with VLAN X. In the form of VLAN list command, PVID is updated with the last item of the VLAN list. When a user removes a port from the untagged membership of the PVID’s VLAN, the port’s PVID will be assigned with “default VLAN”. The default setting is enabled.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable the auto-assign PVID:


```
DGS-3450:admin# enable pvid auto_assign
Command: enable pvid auto_assign

Success.

DGS-3450:admin#
```

disable pvid auto_assign

Purpose	Used to disable auto assignment of PVID.
Syntax	disable pvid auto_assign
Description	If “auto-assign PVID” is disabled, PVID can only be changed by PVID configuration (user changes explicitly). The VLAN configuration will not automatically change PVID. The default setting is enabled.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable the auto-assign PVID:

```
DGS-3450:admin# disable pvid auto_assign
Command: disable pvid auto_assign

Success.

DGS-3450:admin#
```

show pvid auto_assign

Purpose	Used to display the PVID auto-assign status.
Syntax	show pvid auto_assign
Description	The show pvid auto_assign command displays the PVID auto assignment state.
Parameters	None.
Restrictions	None.

Example usage:

To display the PVID auto assignment state:

```
DGS-3450:admin# show pvid auto_assign
Command: show pvid auto_assign

PVID Auto-assignment: Enabled

DGS-3450:admin#
```

IEEE 802.1QINQ COMMANDS

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

Command	Parameters
enable qinq	
disable qinq	
show qinq	
config qinq ports	[<portlist> all] {role [nni uni] missdrop [enable disable] [outer_ tpid tpid]<hex 0x1 - 0xffff> use_inner_priority [enable disable]}(1)
show qinq ports	{<portlist>}
delete vlan_translation ports	[<portlist> all] { cvid <vidlist>}
show vlan_translation	ports <portlist>
create vlan_translation ports	[<portlist> all] cvid <vidlist> [add replace] svid <vlanid 1-4094> {priority <value 0-7>}

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

enable qinq

Purpose	Used to enable QinQ.
Syntax	enable qinq
Description	When QinQ is enabled, all network port roles will be NNI port and outer TPID will be set to 0x88A8; All existed static VLAN will run as S-VLAN; All dynamic learned L2 address will be cleared; All dynamic registered VLAN entries will be cleared, and GVRP will be disabled. If need to run GVRP on the switch, administrator should enable GVRP manually. In QinQ mode, GVRP protocol will employ reserve address 01-80-C2-00-00-0D. The default setting of QinQ is disabled.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable qinq:

```
DGS-3450:admin# enable qinq
Command: enable qinq

Success.

DGS-3450:admin#
```

disable qinq

Purpose	Used to disable the QinQ.
Syntax	disable qinq

disable qinq

Description	When QinQ is disabled, all dynamic learned L2 address will be cleared, all dynamic registered VLAN entries will be cleared, and GVRP will be disabled. If need to run GVRP on the switch, administrator should enable GVRP manually.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable qinq:

```
DGS-3450:admin# disable qinq
Command: disable qinq

Success.

DGS-3450:admin#
```

show qinq

Purpose	Used to show global QinQ status.
Syntax	show qinq
Description	Use this command to display the global QinQ status.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To show qinq:

```
DGS-3450:admin# show qinq
Command: show qinq

Qinq Status: Enable

Success.

DGS-3450:admin#
```

config qinq ports

Purpose	Used to configure QinQ ports parameters.
Syntax	config qinq ports [<portlist> all] {role [nni uni] missdrop [enable disable] [outer_ tpid tpid]<hex 0x1 - 0xffff> use_inner_priority [enable disable]}(1)
Description	The command used to configure QinQ port parameters, include: <ul style="list-style-type: none"> • Role of a port. • Missdrop of a port. • Use inner-priority of a port.
Parameters	<i>ports</i> - A range of ports to configure.

config qinq ports

role - Port role in QinQ mode

UNI - Port is connecting to customer network.

NNI - Port is connecting to service provider network.

outer_ tpid | tpid - Outer-TPID of a port.

use_inner_priority - Specify whether to use the priority in the C-VLAN tag as the priority in the S-VLAN tag. By default, the setting is disabled.

missdrop - Enable/disable miss drop of port.

Restrictions

Only Administrator and Operator-level users can issue this command.

Example usage:

To config port list 1-4 as NNI port, set TPID to 0x88A8:

```
DGS-3450:admin# config qinq ports 1-4 role nni outer_tpid 0x88a8
```

```
Command: config qinq ports 1-4 role nni outer_tpid 0x88a8
```

Success.

```
DGS-3450:admin#
```

show qinq ports

Purpose Used to show qinq configuration of ports.

Syntax **show qinq ports {<portlist>}**

Description The command used to show qinq configuration of ports, include:

- Role of port.
- Outer-TPID of port.
- Miss drop state of port.
- Use inner-priority of a port.

Parameters *portlist* - Specifies a range of ports to be displayed. (Unit ID: port number).
If no parameter specified, system will display all ports information.

Restrictions Only Administrator and Operator-level users can issue this command.

Example usage:

To show QinQ mode for ports 1-4 of unit 1:

```
DGS-3450:admin# show qinq ports 1:1-1:4
```

```
Command: show qinq ports 1:1-1:4
```

Port	Role	Missdrop	TPID	Use Inner Priority
1:1	Normal	Disabled	0x8100	Disabled
1:2	Normal	Disabled	0x8100	Disabled
1:3	Normal	Disabled	0x8100	Disabled
1:4	Normal	Disabled	0x8100	Disabled

```
DGS-3450:admin#
```

delete vlan_translation ports

Purpose	Used to delete existed VLAN translation rules.
Syntax	delete vlan_translation ports [<portlist> all] { cvid <vidlist> }
Description	The delete vlan_translation command is used to delete translation relationship between C-VLAN and S-VLAN.
Parameters	<i>ports</i> - The translation rule for the specified ports. <i>cvid</i> - The rules for the specified CVIDs. If CVID is not specified, all rules configured for the port will be deleted.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete VLAN translation rule on ports 1-4:

```
DGS-3450:admin# delete vlan_translation ports 1-4
Command: delete vlan_translation ports 1-4

Success.

DGS-3450:admin#
```

show vlan_translation

Purpose	Used to show existed C-VLAN based VLAN translation rules.
Syntax	show vlan_translation ports <portlist>
Description	Used to show existed C-VLAN based VLAN translation rules.
Parameters	<i>ports</i> - The C-VLAN based VLAN translation rule of the ports.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To show C-VLAN based VLAN translation rules in the system:

```
DGS-3450:admin# show vlan_translation
Commands: show vlan_translation
Port      CVID    SVID    Action  Priority
-----
1         10      100     Add     4
1         20      100     Add     5
1         30      200     Add     6
2         10      100     Add     7
2         20      100     Add     1

Total Entries: 5

DGS-3450:admin#
```

create vlan_translation ports

Purpose	Use this command to create the CVID VLAN translation rules.
Syntax	create vlan_translation ports [<portlist> all] cvid <vidlist> [add replace] svid <vlanid>

create vlan_translation ports

	1-4094> {priority <value 0-7>}
Description	Use this command to create the CVID VLAN translation rules.
Parameters	<i>portlist</i> - A range of ports on which the S-VLAN will be translated to C-VLAN <i>add</i> - The action indicates to add a tag for the assigned S-VLAN before the C-VLAN tag. <i>replace</i> - The action indicates to replace the C-VLAN tag with the SP VLAN. <i>cvid</i> - Specify the C-VLAN ID to match. <i>svid</i> - Specify the S-VLAN ID.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create vlan translation rule which assign to add S-VLAN 100 to C-VLAN 1-10 on ports 1-4:

```
DGS-3450:admin# create vlan_translation add cvid 10 svid 100
Command: create vlan_translation add cvid 10 svid 100

Success.

DGS-3450:admin#
```

IGMP AND MLD SNOOPING COMMANDS

The Internet Group Management Protocol (IGMP) is a Layer 4 protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. IGMP snooping, as implied by the name, is a feature that allows a Layer 2 switch to "listen in" on the IGMP conversation between hosts and routers by processing the Layer 4 IGMP packets sent in a multicast network.

The Multicast Listener Discovery (MLD) is protocol used by an IPv6 router to discover the presence of multicast listeners (that is, nodes wishing to receive multicast packets) on its directly attached links, and to discover specifically which multicast addresses are of interest to those neighboring nodes.

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

Command	Parameters
config igmp_snooping	[vlan <vlan_name 32> all] {host_timeout <sec 1-16711450> router_timeout <sec 1-16711450> leave_timer <sec 1-16711450> state [enable disable] fast_leave [enable disable] report_suppression [enable disable]}(1)
config igmp_snooping querier	[vlan <vlan_name 32> all]{ query_interval <sec 1-65535> max_response_time <sec 1-25> robustness_variable <value 1-255> last_member_query_interval <sec 1-25> state [enable disable]} version <value 1-3> }
config router_ports	<vlan_name 32> [add delete] <portlist>
config router_ports_forbidden	<vlan_name 32> [add delete] <portlist>
enable igmp_snooping	{forward_mcrouter_only}
disable igmp_snooping	{forward_mcrouter_only}
create igmp_snooping static_group	[vlan<vlan_name 32> vlanid <vlanid_list>] <ipaddr>
delete igmp_snooping static_group	[vlan<vlan_name 32> vlanid <vlanid_list>] <ipaddr>
config igmp_snooping static_group	[vlan <vlan_name 32> vlanid <vlanid_list>] < ipaddr > [add delete] <portlist>
show igmp_snooping static_group	{[vlan <vlan_name 32> vlanid <vlanid_list>] < ipaddr >}
show igmp_snooping group	{vlan <vlan_name 32>} {data_driven}
show router_ports	{vlan <vlan_name 32>} {[static dynamic forbidden]}
config mld_snooping	[vlan <vlan_name 32> all] {node_timeout <sec 1-16711450> router_timeout <sec 1-16711450> done_timer <sec 1-16711450> state [enable disable] fast_done [enable disable]}
config mld_snooping querier	[vlan <vlan_name 32> all] {query_interval <sec 1-65535> max_response_time <sec 1-25> robustness_variable <value 1-255> last_listener_query_interval <sec 1-25> state [enable disable] version <value 1-2> }(1)
config mld_snooping mrouter_ports	<vlan_name 32> [add delete] <portlist>
config mld_snooping mrouter_ports_forbidden	<vlan_name 32> [add delete] <portlist>
enable mld_snooping	{forward_mcrouter_only}
disable mld_snooping	{forward_mcrouter_only}
show mld_snooping	{vlan <vlan_name 32>}
show mld_snooping group	{vlan <vlan_name 32>} {data_driven}
show mld_snooping mrouter_ports	vlan <vlan_name 32> {[static dynamic forbidden]}
config igmp_snooping data_driven_learning	[vlan_name <vlan_name> vlanid <vlanid_list> all] {state [enable disable] aged_out [enable disable] expiry_time <sec 1-65535>}(1)
config igmp_snooping data_driven_learning max_learned_entry	config igmp_snooping data_driven_learning max_learned_entry <value 1-960>
config mld_snooping data_driven_learning	[vlan_name <vlan_name> vlanid <vlanid_list> all] {state [enable disable] aged_out [enable disable] expiry_time <sec 1-65535>}(1)
config mld_snooping data_driven_learning max_learned_entry	<value 1-511>

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

config igmp_snooping

Purpose	Used to configure IGMP snooping on the switch.
Syntax	config igmp_snooping [vlan <vlan_name 32> all] {host_timeout <sec 1-16711450> router_timeout <sec 1-16711450> leave_timer <sec 1-16711450> state [enable disable] fast_leave [enable disable] report_suppression [enable disable]}(1)
Description	The config igmp_snooping command configures IGMP snooping on the switch. Note: A fast leave enabled switch can not be attached to another report suppression enabled switch's downstream interface. That is, if switch A is attached to switch B's downstream interface, you can not enable the fast leave feature on switch A and enable report suppression on switch B simultaneously.
Parameters	<i>vlan</i> - Specify the name of the VLAN for which IGMP snooping is to be configured. All indicates all VLANs. <i>host_timeout</i> – Specify the host time-out value here. <i>router_timeout</i> – Specify the router time-out value here. <i>leave_timer</i> – Specify the leave timer value here. <i>state</i> - Enable or disable IGMP snooping for the chosen VLAN. <i>fast_leave</i> - Enable or disable the IGMP snooping fast leave function. If enabled, the membership is immediately removed when the system receives the IGMP leave message. <i>report_suppression</i> - When IGMP report suppression is enabled (the default), the switch sends the first IGMP report from all hosts for a group to all the multicast routers. The switch does not send the remaining IGMP reports for the group to the multicast routers. If the multicast router query includes requests only for IGMPv1 and IGMPv2 reports, the switch forwards only the first IGMPv1 or IGMPv2 report from all hosts for a group to all the multicast routers. If the multicast router query also includes requests for IGMPv3 reports, the switch forwards all IGMPv3 reports for a group to the multicast devices.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure IGMP snooping:

```
DGS-3450:admin# config igmp_snooping vlan default state enable
Command: config igmp_snooping vlan default state enable

Success.

DGS-3450:admin#
```

config igmp_snooping querier

Purpose	Used to configure the time in seconds between general query transmissions, the maximum time in seconds to wait for reports from members, and the permitted packet loss that guarantees IGMP snooping.
Syntax	config igmp_snooping querier [vlan <vlan_name 32> all]{ query_interval <sec 1-65535> max_response_time <sec 1-25> robustness_variable <value 1-255> last_member_query_interval <sec 1-25> state [enable disable]} version <value 1-3> }
Description	This command configures the IGMP snooping querier.
Parameters	<i>vlan</i> - Specify the name of the VLAN for which IGMP snooping querier is to be configured. <i>query_interval</i> - Specify the amount of time in seconds between general query transmissions. The default setting is 125 seconds. <i>max_reponse_time</i> - Specify the maximum time in seconds to wait for reports from members.

config igmp_snooping querier

The default setting is 10 seconds.

robustness_variable - Provides fine-tuning to allow for expected packet loss on a subnet. The value of the robustness variable is used in calculating the following IGMP message intervals:

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

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

On receiving a leave message, the router will assume there are no local members on the interface if there are no reports received after the response time (which is last member query interval * robustness variable)

state - If the state is enabled, it allows the switch to be selected as an IGMP Querier (sends IGMP query packets). If the state is disabled, then the switch cannot play the role as a querier.

Note: If the I3 router connected to the switch provide only the IGMP proxy function but does not provide the multicast routing function, then this state must be configured as disabled. Otherwise, if the I3 router is not selected as the querier, it will not send the IGMP query packet. Since it will not send the multicast-routing protocol packet, the port will be timed out as a router port.

version - Specify the version of IGMP packet that will be sent by this port. If an IGMP packet received by the interface has a version higher than the specified version, this packet will be dropped.

Restrictions

Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the IGMP snooping querier:

```
DGS-3450:admin# config igmp_snooping querier vlan default query_interval 125 state enable
Command: config igmp_snooping querier vlan default query_interval 125 state enable
```

Success.

```
DGS-3450:admin#
```

config router_ports

Purpose	Used to configure ports as router ports.
Syntax	config router_ports <vlan_name 32> [add delete] <portlist>
Description	This command allows you to designate a range of ports as being connected to multicast-

config router_ports

	enabled routers. This will ensure that all packets with such a router as its destination will reach the multicast-enabled router, regardless of protocol, etc.
Parameters	<i>vlan</i> - Specify the name of the VLAN on which the router port resides. <i>add delete</i> - Specify to add or delete the router ports. <i>portlist</i> - Specify a range of ports to be configured. (UnitID:port number)
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To set up static router ports:

```
DGS-3450:admin# config router_ports default add 2:1-2:10
```

```
Command: config router_ports default add 2:1-2:10
```

Success.

```
DGS-3450:admin#
```

config router_ports_forbidden

Purpose	Used to configure ports as forbidden router ports.
Syntax	config router_ports_forbidden <vlan_name 32> [add delete] <portlist>
Description	This command allows you to designate a range of ports as being not connected to multicast-enabled routers. This ensures that the forbidden router port will not propagate routing packets out.
Parameters	<i>vlan</i> - Specify the name of the VLAN on which the router port resides. <i>add delete</i> - Specify to add or delete the router ports. <i>portlist</i> - Specify a range of ports to be configured. (UnitID:port number)
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To set up port range 1-10 to forbidden router ports of default VLAN:

```
DGS-3450:admin# config router_ports_forbidden default add 1-10
```

```
Command: config router_ports_forbidden default add 1-10
```

Success.

```
DGS-3450:admin#
```

enable igmp_snooping

Purpose	Used to enable IGMP snooping on the switch.
Syntax	enable igmp_snooping {forward_mcrouter_only}
Description	This command allows you to enable IGMP snooping on the switch. The forward mcrouter only function is disabled by default. The enable the IGMP snooping forward mcrouter only command will enable the IGMP snooping function and the forward multicast router only function. If the forward multicast router only is enabled, the switch will forward all multicast traffic to the multicast router only. Otherwise, the switch forwards all multicast traffic to any IP router.

enable igmp_snooping

Parameters	<p><i>forward_mcrouter_only</i> - If specified, the switch will learn the router port based on identification of the multicast routing protocol packet and IGMP control packet.</p> <p>If not specified, the switch will learn the router port based on identification of the unicast routing protocol packet, the multicast routing protocol packet, and the IGMP control packet.</p> <p>When the switch receives an IGMP report packet from a port, this port will be learned as a member port of the multicast group that the port is reported, and the router will be a default member of this multicast group. The multicast packet destined for this multicast group will be forwarded to all the members of this multicast group.</p> <p>The identification of a router port will also affect the forwarding of the IGMP control packet. When the switch receives the IGMP report packet from the client member, it will forward the packet to the router port. If the switch receives the IGMP query packet from the router port, it will forward the packet to the client member port. (If the switch itself is the querier, then it will issue the query packet to the client member port.)</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable IGMP snooping on the switch:

```
DGS-3450:admin# enable igmp_snooping
Command: enable igmp_snooping

Success.

DGS-3450:admin#
```

disable igmp_snooping

Purpose	Used to disable IGMP snooping on the switch.
Syntax	disable igmp_snooping {forward_mcrouter_only}
Description	<p>This command disables IGMP snooping on the switch. Disabling the IGMP snooping allows all IGMP and IP multicast traffic to flood within a given IP interface. Note that disabling IGMP snooping will also disable the forward multicast router only function.</p> <p>The disable mld_snooping forward_mcrouter_only command will only disable the forward multicast router only function.</p>
Parameters	<p><i>forward_mcrouter_only</i> - If specified, the switch will learn the router port based on identification of the multicast routing protocol packet and IGMP control packet.</p> <p>If not specified, the switch will learn the router port based on identification of the unicast routing protocol packet, the multicast routing protocol packet, and the IGMP control packet.</p> <p>When the switch receives an IGMP report packet from a port, this port will be learned as a member port of the multicast group that the port is reported, and the router will be a default member of this multicast group. The multicast packet destined for this multicast group will be forwarded to all the members of this multicast group.</p> <p>The identification of a router port will also affect the forwarding of the IGMP control packet. When the switch receives the IGMP report packet from the client member, it will forward the packet to the router port. If the switch receives the IGMP query packet from the router port, it will forward the packet to the client member port. (If the switch itself is the querier, then it will issue the query packet to the client member port.)</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable IGMP snooping on the switch:

```
DGS-3450:admin# disable igmp_snooping
Command: disable igmp_snooping

Success.

DGS-3450:admin#
```

create igmp_snooping static_group

Purpose	Used to configure an IGMP snooping multicast static group.
Syntax	create igmp_snooping static_group [vlan<vlan_name 32> vlanid <vlanid_list>] <ipaddr >
Description	<p>This command allows you to create an IGMP snooping static group. Member ports can be added to the static group. The static member and the dynamic member port form the member ports of a group.</p> <p>The static group will only take effect when IGMP snooping is enabled on the VLAN. For those static member ports, the device needs to emulate the IGMP protocol operation to the querier, and forward the traffic destined to the multicast group to the member ports.</p> <p>For a layer 3 device, the device is also responsible to route the packet destined for this specific group to static member ports.</p> <p>The static member port will only affect V2 IGMP operation. The Reserved IP multicast address 224.0.0.X must be excluded from the configured group. The VLAN must be created first before a static group can be created.</p>
Parameters	<p><i>vlan_name</i> - Specify the name of the VLAN on which the router port resides.</p> <p><i>ipaddr</i> - Specify the multicast group IP address (for Layer 3 switch).</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create an IGMP snooping static group for VLAN 1, group 239.1.1.1:

```
DGS-3450:admin# create igmp_snooping static_group vlan vlan1 239.1.1.1
Command: create igmp_snooping static_group vlan vlan1 239.1.1.1
Success.

DGS-3450:admin#
```

delete igmp_snooping static_group

Purpose	Used to delete a IGMP snooping multicast static group.
Syntax	delete igmp_snooping static_group [vlan<vlan_name 32> vlanid <vlanid_list>] <ipaddr>
Description	The deletion of an IGMP snooping static group will not affect the IGMP snooping dynamic member ports for a group.
Parameters	<p><i>vlan</i> - Specify the name of the VLAN on which the router port resides.</p> <p><i>vlanid</i> - Specify the ID of the VLAN on which the router port resides.</p> <p><i>ipaddr</i> - Specify the multicast group IP address (for Layer 3 switch).</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete an IGMP snooping static group for VLAN 1, group 239.1.1.1:

```
DGS-3450:admin# delete igmp_snooping_static_group vlan vlan1 239.1.1.1
Command: delete igmp_snooping_static_group vlan vlan1 239.1.1.1

Success.

DGS-3450:admin#
```

config igmp_snooping_static_group

Purpose	Used to configure an IGMP snooping multicast group static member port.
Syntax	config igmp_snooping_static_group [vlan <vlan_name 32> vlanid <vlanid_list>] <ipaddr > [add delete] <portlist>
Description	When a port is configured as a static member port, the IGMP protocol will not operate on this port. For example, suppose that a port is a dynamic member port learned by IGMP. If this port is configured as a static member later, then the IGMP protocol will stop operating on this port. The IGMP protocol will resume once this port is removed from static member ports. The static member port will only affect V2 IGMP operation.
Parameters	<i>vlan</i> - Specify the name of the VLAN on which the static group resides. <i>vlanid</i> - Specify the ID of the VLAN on which the static group resides. <i>ipaddr</i> - Specify the multicast group IP address (for Layer 3 switch). <i>add delete</i> - Specify to add or delete the member ports. <i>portlist</i> - Specify a range of ports to be configured.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To unset port range 9-10 from IGMP snooping static member ports for group 239.1.1.1 on default VLAN:

```
DGS-3450:admin# config igmp_snooping_static_group vlan default 239.1.1.1 delete 9-10
Command: create igmp_snooping_static_group vlan default 239.1.1.1 delete 9-10

Success.

DGS-3450:admin#
```

show igmp_snooping_static_group

Purpose	Used to display an IGMP Snooping multicast group static member port.
Syntax	show igmp_snooping_static_group {[vlan <vlan_name 32> vlanid <vlanid_list>] <ipaddr >}
Description	This command is used to display the IGMP snooping multicast group static members.
Parameters	<i>vlan</i> - Specify the name of the VLAN on which the static group resides. <i>vlanid</i> - Specify the ID of the VLAN on which the static group resides. <i>ipaddr</i> - Specify the multicast group IP address (for Layer 3 switch).
Restrictions	None.

Example usage:

To display all the IGMP snooping static groups:

```
DGS-3450:admin# show igmp_snooping static_group
```

```
Command: show igmp_snooping static_group
```

VLAN ID/Name	IP Address	Static Member Ports
1 / Default	239.1.1.1	2:9-2:10

```
Total Entries : 1
```

```
DGS-3450:admin#
```

show igmp_snooping group

Purpose	Used to display the current IGMP snooping group configuration on the switch.
Syntax	show igmp_snooping group {vlan <vlan_name 32>} {data_driven}
Description	This command displays the current IGMP snooping group configuration on the switch.
Parameters	<i>vlan</i> - Specify the name of the VLAN for which you want to view IGMP snooping group information. <i>data_driven</i> - Specify to display the dynamic data learning groups.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To show IGMP snooping groups when IGMP v3 is supported:

The first item means that for ports 1-2, the data from the 10.0.0.2/225.0.0.2 will be forwarded.

The second item means that for port 3, the data from the 10.0.0.2/225.0.0.3 must not be forwarded.

The third item means that for ports 4-5, the data from 225.0.0.5 will be forwarded, IGMP v2 group. The source address does not matter.

The fourth item is a data-driven learned entry. If the member port list is empty, the multicast packets will be forwarded to the router ports. If the router port list is empty, the packets will be dropped.

```

DGS-3450:admin# show igmp_snooping group
Command: show igmp_snooping group
Source/Group   : 10.0.0.2 / 225.0.0.2
VLAN Name/VID  : n172/172
Port Member    : 1-2
Mode           : INCLUDE

Source/Group   : 10.0.0.2 / 225.0.0.3
VLAN Name/VID  : n172/172
Port Member    : 3
Mode           : EXCLUDE

Source/Group   : NULL / 225.0.0.5
VLAN Name/VID  : n172/172
Port Member    : 4-5
Mode           : EXCLUDE

Source/Group   : NULL / 239.255.255.250
VLAN Name/VID  : n172/172
Port Member    : 2:22
Mode           : EXCLUDE

Total Entries : 4

DGS-3450:admin# show igmp_snooping group data_driven
Command: show igmp_snooping group data_driven

Source/Group   : NULL/225.0.0.5
VLAN Name/VID  : default/1
Port Member    :
Router Ports   : 24
Mode           : EXCLUDE

Total Entries : 1

DGS-3450:admin#

```

show router_ports

Purpose	Used to display the currently configured router ports on the switch.
Syntax	show router_ports {vlan <vlan_name 32>} {[static dynamic forbidden]}
Description	This command displays the currently configured router ports on the switch.
Parameters	<p><i>vlan</i> - Specify the name of the VLAN on which the router port resides.</p> <p><i>static</i> - Displays router ports that have been statically configured.</p> <p><i>dynamic</i> - Displays router ports that have been dynamically configured.</p> <p><i>forbidden</i> - Displays forbidden router ports that have been statically configured.</p> <p>If no parameter is specified, the system will display all currently configured router ports on the switch.</p>
Restrictions	None.

Example usage:

To display router ports:


```
DGS-3450:admin# show router_ports
```

```
Command: show router_ports
```

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

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

```
Total Entries : 2
```

```
DGS-3450:admin#
```

config mld_snooping

Purpose	Used to configure MLD snooping on the switch.
Syntax	config mld_snooping [vlan <vlan_name 32> all] {node_timeout <sec 1-16711450> router_timeout <sec 1-16711450> done_timer <sec 1-16711450> state [enable disable] fast_done [enable disable]}
Description	This command is used to configure MLD snooping on the switch.
Parameters	<p><i>vlan</i> - Specify the name of the VLAN for which MLD snooping is to be configured.</p> <p><i>all</i> - Specify all VLANs for which MLD snooping is to be configured.</p> <p><i>node_timeout</i> – Specify the node time-out value here.</p> <p><i>router_timeout</i> – Specify the router time-out value here.</p> <p><i>done_timer</i> – Specify the done timer here.</p> <p><i>state</i> - Enable or disable MLD snooping for the chosen VLAN.</p> <p><i>fast_done</i> - Enable or disable MLD snooping fast_leave function.</p> <p>If enable, the membership is immediately removed when the system receive the MLD leave message.</p> <p>If the multicast router query includes requests only for MLDv1 reports, the switch forwards only the first MLDv1 report from all hosts for a group to all the multicast routers.</p> <p>If the multicast router query also includes requests for MLDv2 reports, the switch forwards all MLDv2 reports for a group to the multicast devices.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure MLD snooping:

```
DGS-3450:admin# config mld_snooping vlan default state enable
```

```
Command: config mld_snooping vlan default state enable
```

```
Success.
```

```
DGS-3450:admin#
```

config mld_snooping querier

Purpose	Used to configure the time in seconds between general query transmissions, the maximum time in seconds to wait for reports from members, and the permitted packet loss that
---------	---

config mld_snooping querier

	guarantees MLD snooping.
Syntax	config mld_snooping querier [vlan <vlan_name 32> all] {query_interval <sec 1-65535> max_response_time <sec 1-25> robustness_variable <value 1-255> last_listener_query_interval <sec 1-25> state [enable disable] version <value 1-2>}(1)
Description	This command configures the timer in seconds between general query transmissions, the maximum time in seconds to wait for reports from listeners, and the permitted packet loss that is guaranteed by MLD snooping.
Parameters	<p><i>vlan</i> - Specify the name of the VLAN for which MLD snooping querier is to be configured.</p> <p><i>all</i> - Specify all VLANs for which MLD snooping querier is to be configured.</p> <p><i>query_interval</i> - Specify the amount of time in seconds between general query transmissions. The default setting is 125 seconds..</p> <p><i>max_reponse_time</i> - Specify the maximum time in seconds to wait for reports from listeners. The default setting is 10 seconds.</p> <p><i>robustness_variable</i> - Provides fine-tuning to allow for expected packet loss on a subnet. The value of the robustness variable is used in calculating the following MLD message intervals:</p> <ul style="list-style-type: none"> • Group listener interval - Amount of time that must pass before a multicast router decides there are no more listeners of a group on a network. This interval is calculated as follows: (robustness variable * query interval) + (1 * query response interval). • Other querier present interval - Amount of time that must pass before a multicast router decides that there is no longer another multicast router that is the querier. This interval is calculated as follows: (robustness variable * query interval) + (0.5 * query response interval). • Last listener query count - Number of group-specific queries sent before the router assumes there are no local listeners of a group. The default number is the value of the robustness variable. • By default, the robustness variable is set to 2. You might want to increase this value if you expect a subnet to be loosely. <p><i>last_listener_query_interval</i> - Specify the maximum amount of time between group-specific query messages, including those sent in response to done-group messages. You might lower this interval to reduce the amount of time it takes a router to detect the loss of the last listener of a group.</p> <p><i>state</i> - This allows the switch to be specified as an MLD Querier (sends MLD query packets) or a Non-Querier (does not send MLD query packets). Set to enable or disable.</p> <p><i>version <value 1-2></i> - Specify the version of MLD packet that will be sent by this port. If a MLD packet received by the interface has a version higher than the specified version, this packet will be dropped.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the MLD snooping querier:

```
DGS-3450:admin# config mld_snooping querier vlan default query_interval 125 state enable
Command: config mld_snooping querier vlan default query_interval 125 state enable

Success.

DGS-3450:admin#
```

config mld_snooping mrouter_ports

Purpose	Used to configure ports as router ports.
---------	--

config mld_snooping mrouter_ports

Syntax	config mld_snooping mrouter_ports <vlan_name 32> [add delete] <portlist>
Description	This command allows you to designate a range of ports as being connected to multicast-enabled routers. This will ensure that all packets with such a router as its destination will reach the multicast-enabled router, regardless of protocol, etc.
Parameters	<i>add delete</i> - Specify to add or delete the router ports. <i>portlist</i> - Specify a range of ports to be configured. (UnitID:port number)
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To set up static router ports:

```
DGS-3450:admin# config mld_snooping mrouter_ports default add 2:1-2:10
```

```
Command: config mld_snooping mrouter_ports default add 2:1-2:10
```

Success.

```
DGS-3450:admin#
```

config mld_snooping mrouter_ports_forbidden

Purpose	Used to configure ports as forbidden router ports.
Syntax	config mld_snooping mrouter_ports_forbidden <vlan_name 32> [add delete] <portlist>
Description	This command allows you to designate a range of ports as being not connected to multicast-enabled routers. This ensures that the forbidden router port will not propagate routing packets out.
Parameters	<i>add delete</i> - Specify to add or delete the router ports. <i>portlist</i> - Specify a range of ports to be configured. (UnitID:port number)
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To set up port range 1-10 to forbidden router ports of the default VLAN:

```
DGS-3450:admin# config mld_snooping mrouter_ports_forbidden default add 1-10
```

```
Command: config mld_snooping mrouter_ports_forbidden default add 1-10
```

Success.

```
DGS-3450:admin#
```

enable mld_snooping

Purpose	Used to enable MLD snooping on the switch.
Syntax	enable mld_snooping {forward_mcrouter_only}
Description	This command allows you to enable MLD snooping on the switch. The <i>forward_mcrouter_only</i> function is disabled by default. The <i>enable mld_snooping forward_mcrouter_only</i> command will enable the MLD snooping function and the forward multicast router only function. If forward multicast router only is enabled, the switch will forward all multicast traffic to the

enable mld_snooping

Parameters	<p>multicast router, only. Otherwise, the switch forwards all multicast traffic to any IP router.</p> <p><i>forward_mcrouter_only</i> - If specified, the switch will learn the router port based on identification of the multicast routing protocol packet and MLD control packet.</p> <p>If not specified, the switch will learn the router port based on identification of the unicast routing protocol packet, the multicast routing protocol packet, and the MLD control packet.</p> <p>When the switch receives an MLD report packet from a port, this port will be learned as a member port of the multicast group that the port is reported, and the router will be a default member of this multicast group. The multicast packet destined for this multicast group will be forwarded to all the members of this multicast group.</p> <p>The identification of a router port will also affect the forwarding of the MLD control packet. When the switch receives the MLD report packet from the client member, it will forward the packet to the router port. If the switch receives the MLD query packet from the router port, it will forward the packet to the client member port. (If the switch itself is the querier, then it will issue the query packet to the client member port.)</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable MLD snooping on the switch:

```
DGS-3450:admin# enable mld_snooping
Command: enable mld_snooping

Success.

DGS-3450:admin#
```

disable mld_snooping

Purpose	Used to disable MLD snooping on the switch.
Syntax	disable mld_snooping {forward_mcrouter_only}
Description	<p>This command disables MLD snooping on the switch. Disabling MLD snooping allows all MLD and IP multicast traffic to flood within a given IP interface. Note that disabling MLD snooping will also disable the forward multicast router only function.</p> <p>The disable mld_snooping forward_mcrouter_only command will only disable the forward multicast router only function.</p>
Parameters	<p><i>forward_mcrouter_only</i> - If specified, the switch will learn the router port based on identification of the multicast routing protocol packet and MLD control packet.</p> <p>If not specified, the switch will learn the router port based on identification of the unicast routing protocol packet, the multicast routing protocol packet, and the MLD control packet.</p> <p>When the switch receives an MLD report packet from a port, this port will be learned as a member port of the multicast group that the port is reported, and the router will be a default member of this multicast group. The multicast packet destined for this multicast group will be forwarded to all the members of this multicast group.</p> <p>The identification of a router port will also affect the forwarding of the MLD control packet. When the switch receives the MLD report packet from the client member, it will forward the packet to the router port. If the switch receives the MLD query packet from the router port, it will forward the packet to the client member port. (If the switch itself is the querier, then it will issue the query packet to the client member port.)</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable MLD snooping on the switch:

```
DGS-3450:admin# disable mld_snooping
Command: disable mld_snooping

Success.

DGS-3450:admin#
```

show mld_snooping

Purpose	Used to show the current status of MLD snooping on the switch.
Syntax	show mld_snooping {vlan <vlan_name 32>}
Description	This command will display the current MLD snooping configuration on the switch.
Parameters	<i>vlan</i> - Specify the name of the VLAN for which you want to view the IGMP snooping configuration. If VLAN is not specified, the system will display all current MLD snooping configurations.
Restrictions	None.

Example usage:

To show MLD snooping:

```
DGS-3450:admin# show mld_snooping
Command: show mld_snooping

MLD Snooping Global State      : Disabled
Multicast router Only          : Disabled
Data Driven Learning Max Entries : 56

VLAN Name                      : default
Query Interval                  : 125
Max Response Time               : 10
Robustness Value                : 2
Last Listener Query Interval    : 1
Node Timeout                    : 260
Router Timeout                  : 260
Done Timer                      : 2
Querier State                   : Enabled
Querier Router Behavior         : Non-Querier
State                           : Disabled
Fast Done                       : Disabled
Version                         : 2
Data Driven Learning State      : Enabled
Data Driven Learning Aged Out   : Disabled
Data Driven Group Expiry Time   : 260

DGS-3450:admin#
```

show mld_snooping group

Purpose	Used to display the current MLD snooping group information on the switch.
Syntax	show mld_snooping group {vlan <vlan_name 32>} {data_driven}

show mld_snooping group

Description	This command displays the current MLD snooping group information on the switch.
Parameters	<i>vlan</i> - Specify the name of the VLAN for which you want to view MLD snooping group information. If VLAN and ports and IP address are not specified, the system will display all current IGMP snooping group information.
Restrictions	None.

Example usage:

To show an MLD snooping group when MLD v2 is supported:

The first item means that for ports 1-2, the data from the 2001::1/FE1E::1 will be forwarded.

The second item means that for port 3, the data from the 2002::2/FE1E::1 must not be forwarded.

The third item means that for ports 4-5, the data from FE1E::2 will be forwarded, MLD v1 group doesn't care about the source address.

The fourth item is a data-driven learned entry. The member port list is empty. The multicast packets will be forwarded to the router ports. If the router port list is empty, the packet will be dropped.

```

DGS-3450:admin# show mld_snooping group
Command: show mld_snooping group
Source/Group           : 2001::1/FE1E::1
VLAN Name/VID          : default/1
Reports                : 1
Member Ports           : 1-2
Router Ports           : 24
UP Time                : 26
Expiry Time            : 258
Filter Mode             : INCLUDE

Source/Group           : 2002::2/FE1E::1
VLAN Name/VID          : default/1
Reports                : 1
Member Ports           : 3
Router Ports           : 24
UP Time                : 29
Expiry Time            : 247
Filter Mode             : EXCLUDE

Source/Group           : NULL/FE1E::2
VLAN Name/VID          : default/1
Reports                : 1
Member Ports           : 4-5
Router Ports           : 24
UP Time                : 40
Expiry Time            : 205
Filter Mode             : EXCLUDE

Source/Group           : NULL/FF1E::5
VLAN Name/VID          : default/1
Reports                : 0
Member Ports           :
Router Ports           : 24
UP Time                : 100
Expiry Time            : 200
Filter Mode             : EXCLUDE

Total Entries : 4

DGS-3450:admin# show mld_snooping group data_driven
Command: show mld_snooping group data_driven

Source/Group           : NULL/FF1E::5
VLAN Name/VID          : default/1
Port Member            :
Router Ports           : 24
Mode                   : EXCLUDE

Total Entries : 1

DGS-3450:admin#

```

show mld_snooping mrouter_ports

Purpose	Used to display the currently configured router ports on the switch.
Syntax	show mld_snooping mrouter_ports {vlan <vlan_name 32>} {[static dynamic forbidden]}

show mld_snooping mrouter_ports

Description	This command displays the currently configured router ports on the switch.
Parameters	<p><i>vlan</i> - Specify the name of the VLAN on which the router port resides.</p> <p><i>static</i> - Displays router ports that have been statically configured.</p> <p><i>dynamic</i> - Displays router ports that have been dynamically configured.</p> <p><i>forbidden</i> - Displays forbidden router ports that have been statically configured.</p> <p>If no parameter is specified, the system will display all currently configured router ports on the switch.</p>
Restrictions	None.

Example usage:

To display the mld_snooping router ports:

```
DGS-3450:admin# show mld_snooping mrouter_ports
Command: show mld_snooping router_ports

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

Total Entries : 1

DGS-3450:admin#
```

config igmp_snooping data_driven_learning

Purpose	This command is used to enable or disable the data driven learning of an IGMP snooping group.
Syntax	config igmp_snooping data_driven_learning [vlan_name <vlan_name> vlanid <vlanid_list> all] {state [enable disable] aged_out [enable disable] expiry_time <sec 1-65535>}(1)
Description	<p>This command is used to enable or disable the data driven learning of an IGMP snooping group.</p> <p>When data-driven learning is enabled for the VLAN, when the switch receives the IP multicast traffic on this VLAN, an IGMP snooping group will be created. That is, the learning of an entry is not activated by IGMP membership registration, but activated by the traffic. For an ordinary IGMP snooping entry, the IGMP protocol will take care of the aging out of the entry. For a data-driven entry, the entry can be specified not to be aged out or to be aged out by the aged timer.</p> <p>When data driven learning is enabled, and the data driven table is not full, the multicast filtering mode for all ports is ignored. That is, the multicast packets will be forwarded to router ports. If the data driven learning table is full, the multicast packets will be forwarded according to the multicast filtering mode.</p> <p>Note that if a data-driven group is created and IGMP member ports are learned later, the entry will become an ordinary IGMP snooping entry. That is, the aging out mechanism will follow the ordinary IGMP snooping entry.</p>
Parameters	<p><i>vlan_name</i> - Specify the VLAN name to be configured.</p> <p><i><vlan_name></i> - Enter the VLAN name here.</p> <p><i>vlanid</i> - Specify the VLAN ID to be configured.</p>

config igmp_snooping data_driven_learning

<vlanid_list> - Enter the VLAN ID here.
all - Specify all VLANs to be configured.
state - (Optional) Specify to enable or disable the data driven learning of an IGMP snooping group.
enable - Enter enable to enable the data driven learning option. By default, the state is enabled.
disable - Enter disable to disable the data driven learning option.
aged_out - (Optional) Enable or disable the aging out of the entry.
enable - Enter enable to enable the aging out of the entry.
disable - Enter disable to disable the aging out of the entry. By default, the state is disabled state.
expiry_time - (Optional) Specify the data driven group lifetime in seconds. This parameter is valid only when *aged_out* is enabled.
<sec 1-65535> - Enter the expiry time here. This value must be between 1 and 65535 seconds.

Restrictions Only Administrator and Operator-level users can issue this command.

Example usage:

To enable the data driven learning of an IGMP snooping group on the default VLAN:

```
Prompt# config igmp_snooping data_driven_learning vlan default state enable
Command: config igmp_snooping data_driven_learning vlan default state enable

Success.

Prompt#
```

config igmp_snooping data_driven_learning max_learned_entry

Purpose	Used to configure the maximum number of groups that can be learned by data driven.
Syntax	config igmp_snooping data_driven_learning max_learned_entry <value 1-n>
Description	Used to configure the maximum number of groups that can be learned by data driven. When the table is full, the system will stop the learning of the new data-driven groups. Traffic for the new groups will be dropped.
Parameters	<i>max_learned_entry</i> - Specify the maximum number of groups that can be learned by data driven. The suggested default setting is 56. This default setting may vary depending on projects. <i><value 1-n></i> - Enter the maximum learning entry value here. This value must be between 1 and n.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To set the maximum number of groups that can be learned by data driven:

```
Prompt# config igmp_snooping data_driven_learning max_learned_entry 50
Command: config igmp_snooping data_driven_learning max_learned_entry 50

Success.

Prompt#
```

config mld_snooping data_driven_learning

Purpose	This command is used to enable or disable the data-driven learning of an MLD snooping group.
Syntax	config mld_snooping data_driven_learning [vlan_name <vlan_name> vlanid <vlanid_list > all] {state [enable disable] aged_out [enable disable] expiry_time <sec 1-65535>}(1)
Description	<p>This command is used to enable or disable the data-driven learning of an MLD snooping group.</p> <p>When data-driven learning is enabled for the VLAN, when the switch receives the IP multicast traffic, on this VLAN, an MLD snooping group will be created. That is, the learning of an entry is not activated by MLD membership registration, but activated by the traffic. For an ordinary MLD snooping entry, the MLD protocol will take care the aging out of the entry. For a data-driven entry, the entry can be specified not to be aged out or to be aged out by the aged timer.</p> <p>When the data driven learning is enabled, and the data driven table is not full, the multicast filtering mode for all ports is ignored. That is, the multicast packets will be forwarded to router ports. If the data driven learning table is full, the multicast packets will be forwarded according to the multicast filtering mode.</p> <p>Note that if a data-driven group is created and MLD member ports are learned later, the entry will become an ordinary MLD snooping entry. That is, the aging out mechanism will follow the ordinary MLD snooping entry.</p>
Parameters	<p><i>vlan_name</i> - Specify the VLAN name to be configured.</p> <p><i><vlan_name></i> - Enter the VLAN name here.</p> <p><i>vlanid</i> - Specify the VLAN ID to be configured.</p> <p><i><vlanid_list></i> - Enter the VLAN ID list here.</p> <p><i>all</i> - Specify that all VLANs are to be configured.</p> <p><i>state</i> - (Optional) Specify to enable or disable the data driven learning of MLD snooping groups. By default, the state is enabled.</p> <p><i>enable</i> - Enter enable to enable the data driven learning state.</p> <p><i>disable</i> - Enter disable to disable the data driven learning state.</p> <p><i>aged_out</i> - (Optional) Enable or disable the aging out of entries. By default, the state is disabled.</p> <p><i>enable</i> - Enter enable to enable the aged out option.</p> <p><i>disable</i> - Enter disable to disable the aged out option.</p> <p><i>expiry_time</i> - (Optional) Specify the data driven group lifetime, in seconds. This parameter is valid only when aged_out is enabled.</p> <p><i><sec 1-65535></i> - Enter the expiry time value here. This value must be between 1 and 65535 seconds.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable the data driven learning of an MLD snooping group on the default VLAN:

```
Prompt# config mld_snooping data_driven_learning vlan default state enable
Command: config mld_snooping data_driven_learning vlan default state enable

Success.

Prompt#
```

config mld_snooping data_driven_learning max_learned_entry

Purpose	This command is used to configure the maximum number of groups that can be learned by data driven.
Syntax	config mld_snooping data_driven_learning max_learned_entry <value 1-n>
Description	This command is used to configure the maximum number of groups that can be learned by data driven. When the table is full, the system will stop the learning of the new data-driven groups. Traffic for the
Parameters	<i>max_learned_entry</i> - Specify the maximum number of groups that can be learned by data driven. The suggested default setting is 56. This default setting may vary depending on project. <value 1-n> - Enter the maximum learned entry value here. This value must be between 1 and n.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To set the maximum number of groups that can be learned by data driven:

```
Prompt# config mld_snooping data_driven_learning max_learned_entry 50
Command: config mld_snooping data_driven_learning max_learned_entry 50

Success.

Prompt#
```

IP DIRECTED BROADCAST COMMANDS

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

Command	Parameters
create ipif	<ipif_name 12> <network_address> <vlan_name 32> { secondary state [enable disable] proxy_arp [enable disable] {local [enable disable]}}
config ipif	<ipif_name 12> [{ipaddress <network_address> vlan <vlan_name 32> state [enable disable] proxy_arp [enable disable] {local [enable disable]}}(1) bootp dhcp dhcp_option12 [hostname <hostname> clear_hostname state [enable disable]] ipv6 ipv6address <ipv6networkaddr> dhcpv6_client [enable disable] ip_directed_broadcast [enable disable]]

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

create ipif

Purpose	This command is used to create a layer 3 interface.
Syntax	create ipif <ipif_name 12> <network_address> <vlan_name 32> { secondary state [enable disable] proxy_arp [enable disable] {local [enable disable]}}
Description	<p>This command creates a L3 interface.</p> <p>This interface can be configured with IPv4 or IPv6 address. Currently, it has a restriction. An interface can have only one IPv4 address defined. But it can have multiple IPv6 addresses defined. Thus, the multinetting configuration of IPv4 must be done through creation of a secondary interface on the same VLAN, instead of directly configuring multiple IPv4 addresses on the same interface. Configuration of IPv6 address must be done through the command config ipif.</p> <p>Note that for an IPv6 case, the multicast routing protocol state in secondary IP interfaces must follow master IP interface's state. For example, if dvmrp state in master IP interface is enabled, the secondary IP interfaces need to be the same.</p>
Parameters	<p><i>ipif_name</i> - The name of the interface.</p> <p><i>network_address</i> - IPv4 networkaddress (xxx.xxx.xxx/xx). It specifies a host address and length of network mask.</p> <p><i>vlan_name</i> - The name of a vlan.</p> <p><i>secondary</i> - IPv4secondary interface to be created.</p> <p><i>state</i> - State of interface.</p> <p><i>proxy_arp</i> - Enable/disable of proxy ARP function. It is for IPv4 function. Default: Disabled.</p> <p><i>local</i> - This setting controls whether the system provides the proxy reply for the ARP packets destined for IP address located in the same interface as the received interface.</p> <p>When proxy ARP is enabled for an interface, the system will do the proxy reply for the ARP packets destined for IP address located in a different interface. For ARP packets destined for IP address located in the same interface, the system will check this setting to determine whether to reply.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create an IP interface called 'InterS':

```
DGS-3450:admin# create ipif Inters 192.168.69.1/24 default secondary
Command: create ipif Inters 192.168.69.1/24 default secondary

Success.

DGS-3450:admin#
```

config ipif

Purpose	This command is used to configure the IP directed-broadcast state of the interface.
Syntax	config ipif <ipif_name 12> [{ipaddress <network_address> vlan <vlan_name 32> state [enable disable] proxy_arp [enable disable] {local [enable disable]}}(1) bootp dhcp dhcp_option12 [hostname <hostname> clear_hostname state [enable disable]] ipv6 ipv6address <ipv6networkaddr> dhcpv6_client [enable disable] ip_directed_broadcast [enable disable]]
Description	<p>This command will enabled or disabled the IP directed-broadcast state of a specified interface.</p> <p>An IP directed broadcast is an IP packet whose destination address is a valid broadcast address of some IP subnet, but which originates from a node that is not a part of that destination subnet.</p> <p>The Switch that is not directly connected to its destination subnet and forwards an IP directed broadcast in the same way that it would forward unicast IP packets to a host on that subnet. When a directed broadcast packet reaches a router that is directly connected to its destination subnet, and that packet is "exploded" as a broadcast on the destination subnet. It only works on layer 3 Switch.</p>
Parameters	<p><i>ip_directed_broadcast</i> - Specifies the IP directed-broadcast state of the interface.</p> <p><i>enable</i> - Enabled the IP directed-broadcast state of the interface.</p> <p><i>disable</i> - Disabled the IP directed-broadcast state of the interface.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To set the IP Directed Broadcast state of System interface to enable:

```
DGS-3450:admin# config ipif System ip_directed_broadcast enable
Command: config ipif System ip_directed_broadcast enable

Success.

DGS-3450:admin#
```

To display the IP Directed Broadcast settings of System interface:

```
DGS-3450:admin# show ipif System
```

```
Command: show ipif System
```

```
IP Interface           : System
VLAN Name              : default
Interface Admin state : Enabled
IPv4 Address           : 10.90.90.90/8 (Manual) Primary
Proxy ARP              : Disabled (Local: Disabled)
IP Directed Broadcast : Enabled
IP MTU                 : 1580
```

```
DGS-3450:admin#
```

IP-MAC-PORT BINDING (IMPB) COMMANDS

IP-MAC-Port Binding (IMPB) is a security application found on edge switches which are usually directly connected to hosts. IMPB enables administrators to configure (or snoop) pairs of MAC and IP addresses that are allowed to access networks through the switch. IP-MAC-Port Binding (IMPB) binds together the network layer IP address, and the Ethernet link layer MAC address, and the receiving port, to allow the transmission of data between the layers.

The IP-MAC-Port Binding (IMPB) commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameters
config address_binding ip_mac ports	[<portlist> all] { state [enable {[strict loose] [ipv6 all]}] disable {[ipv6 all]}] allow_zeroip [enable disable] forward_dhcppkt [enable disable] mode [arp acl] stop_learning_threshold<int 0-500> (1)
create address_binding ip_mac ipaddress	< ipaddr > mac_address < macaddr > {ports [portlist all]
create address_binding ip_mac	[ipaddress < ipaddr > ipv6address <ipv6addr>] mac_address < macaddr > { ports [portlist all]}
delete address_binding	[ip_mac [[ipaddress < ipaddr > ipv6address <ipv6addr>] mac_address < macaddr > all] blocked [all vlan_name < vlan_name > mac_address < macaddr >]]
config address_binding ip_mac	[ipaddress < ipaddr > ipv6address <ipv6addr>] mac_address < macaddr > {ports [portlist all]}
show address_binding	[ip_mac [all [ipaddress < ipaddr > ipv6address <ipv6addr>] mac_address < macaddr >] blocked [all vlan_name <vlan_name> mac_address <macaddr>] ports {<portlist>}]
enable address_binding dhcp_snoop	{[ipv6 all]}
disable address_binding dhcp_snoop	{[ipv6 all]}
clear address_binding dhcp_snoop binding_entry ports	[<portlist> all] {[ipv6 all]}
show address_binding dhcp_snoop	{[max_entry { ports <portlist>} binding_entry {port <port>}]}
config address_binding dhcp_snoop max_entry ports	[<portlist> all] limit [<value 1-50> no_limit]
enable address_binding trap_log	
disable address_binding trap_log	
config address_binding recover_learning ports	[<portlist> all]
enable address_binding nd_snoop	
disable address_binding nd_snoop	
show address_binding nd_snoop	
show address_binding nd_snoop binding_entry	{port <port>}
clear address_binding nd_snoop binding_entry ports	[<portlist> all]
debug address_binding	[event dhcp all]
no debug address_binding	

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

config address_binding ip_mac ports

Purpose	Used to configure the state of IMPB on the switch for each port.
Syntax	config address_binding ip_mac ports [< portlist > all] {state [enable {[strict loose]} disable] allow_zeroip [enable disable] forward_dhcppt [enable disable]} (1)
Description	Used to configure the per port state of IMPB on the switch. If a port has been configured as group member of an aggregated link, then the IMPB function cannot be enabled. When the binding state is enabled for IP packets and ARP packets received by this port, the switch will check whether the IP address and MAC address matches the binding entry. If the packet does not match it will be dropped.
Parameters	<p><i>state</i> - This parameter configures the IMPB port state to be enabled or disabled. When the state is enabled, the port will perform the binding check.</p> <p><i>strict</i> - Used to implement a mode of strict control. When strict control is used, all ARP and IP broadcast packets are sent to the CPU and checked for IMPB before forwarding. Packets with MAC addresses that match IMPB entries are set to dynamic state while MAC addresses with no match are set to block. All other packets are dropped. The default mode is strict if not specified.</p> <p><i>loose</i> - Used to implement a more loose or less strict mode of control. In loose mode, ARP and IP broadcast packets are sent to the CPU for IMPB checking. Packets are forwarded unless the check finds a specified source MAC address that is blocked. Packets with MAC addresses that match IMPB entries are set to dynamic state while MAC addresses with no match are set to block. All other packets are bypassed.</p> <p><i>allow_zeroip</i> - Specify whether to allow an ARP packet with a source IP address of 0.0.0.0. If the IP address 0.0.0.0 is not configured in the binding list and this setting is enabled, ARP packets with the source IP address of 0.0.0.0 will be allowed; If the IP address 0.0.0.0 is not configured in the binding list and this setting is set to disable, ARP packets with the source IP address of 0.0.0.0 will not be allowed. This option does not affect the IMPB ACL Mode.</p> <p><i>forward_dhcppt</i> - By default, DHCP packets with a broadcast DA will be flooded. When set to disabled, the broadcast DHCP packet received by the specified port will not be forwarded. This setting is effective when DHCP Snooping is enabled, in this case DHCP packets trapped by the CPU must be forwarded by the software. This setting controls the forwarding behavior in this situation.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable IMPB on port 1:

```
DGS-3450:admin# config address_binding ip_mac ports 1 state enable
Command: config address_binding ip_mac ports 1 state enable

Success.

DGS-3450:admin#
```

config address_binding ip_mac ports

Purpose	Used to configure the state of IMPB on the switch for each port.
Syntax	config address_binding ip_mac ports [<portlist> all] { state [enable {[strict loose]

config address_binding ip_mac ports

	<pre>[ipv6 all]] disable {[ipv6 all]}] allow_zeroip [enable disable] forward_dhcpptk [enable disable] mode [arp acl] stop_learning_threshold<int 0-500>} (1)</pre>
Description	<p>Used to configure the per port state of IMPB on the switch.</p> <p>If a port has been configured as group member of an aggregated link, then the IMPB function cannot be enabled.</p> <p>When the binding check state is enabled for IP packets and ARP packets received by this port, the switch will check whether the IP address and MAC address matches the binding entry. If the packet does not match it will be dropped.</p> <p>For this function, the switch can operate in ACL mode or ARP mode. In ARP mode, only ARP packets are checked for binding. In ACL mode, both ARP packets and IP packets are checked for binding. Therefore, the ACL mode provides more strict checks for packets.</p>
Parameters	<p><i>state</i> - This parameter configures the IMPB port state to be enabled or disabled. When the state is enabled, the port will perform the binding check.</p> <p><i>ipv6</i> - For “state enable ipv6”, only the IPv6 filter table applied to the driver. For “state enable” without specifying “ipv6”, only the IPv4 filtering table is applied to driver. For “state enable all”, both IPv4 and IPv6 filtering tables are applied to the driver.</p> <p>For example, if IPv6 is enabled, but IPv4 is disabled, only the IPv6 Snooping entry is used to create a HW filtering table, if the FDB is used as the HW filtering table, and one IPv6 entry is allowed to be forwarded, all IPv4 packets get forwarded.</p> <p><i>strict</i> - Used to implement a mode of strict control. When strict control is used, all ARP and IP broadcast packets are sent to the CPU and checked for IMPB before forwarding. Packets with MAC addresses that match IMPB entries are set to dynamic state while MAC addresses with no match are set to block. All other packets are dropped.</p> <p><i>loose</i> - Used to implement a more loose or less strict mode of control.</p> <p>In loose mode, ARP and IP broadcast packets are sent to the CPU for IMPB checking. Packets are forwarded unless the check finds a specified source MAC address that is blocked. Packets with MAC addresses that match IMPB entries are set to dynamic state while MAC addresses with no match are set to block. All other packets are bypassed.</p> <p><i>allow_zeroip</i> - Specify whether to allow ARP packets with a source IP address of 0.0.0.0. If the IP address 0.0.0.0 is not configured in the binding list and this setting is enabled, ARP packets with the source IP address of 0.0.0.0 will be allowed; If the IP address 0.0.0.0 is not configured in the binding list and this setting is disabled, ARP packets with the source IP address of 0.0.0.0 will not be allowed. This option does not affect the IMPB ACL Mode.</p> <p><i>forward_dhcpptk</i> - By default, DHCP packets with a broadcast DA will be flooded. When set to disabled, the broadcast DHCP packet received by the specified port will not be forwarded.</p> <p>This setting is effective when DHCP Snooping is enabled, in this case DHCP packets trapped by the CPU must be forwarded by the software.</p> <p>This setting controls the forwarding behavior in this situation.</p> <p><i>mode</i> - When configuring the mode of the port to be ACL mode, the switch will create an ACL access entry corresponding to the entries of the port. If the port changes to ARP mode, all ACL access entries are deleted automatically. The default mode for a port is ARP mode.</p> <p><i>stop_learning_threshold</i> - When the number of blocked entries exceeds the threshold, the port will stop learning new addresses. Packets with a new address will be dropped. The range is 0-500. 0 means no limit.</p>
Restrictions	<p>Only Administrator and Operator-level users can issue this command.</p>

Example usage:

To enable IMPB on port 1:

```
DGS-3450:admin# config address_binding ip_mac ports 1 state enable
Command: config address_binding ip_mac ports 1 state enable

Success.

DGS-3450:admin#
```

create address_binding ip_mac

Purpose	Used to create an IMPB entry.
Syntax	create address_binding ip_mac ipaddress < ipaddr > mac_address < macaddr > {ports [portlist all]}
Description	Use this command to create an IMPB entry. One MAC address can map to multiple IP addresses.
Parameters	<i>ipaddr</i> - Specify the IP address used for the IMPB entry. <i>macaddr</i> - Specify the MAC address used for the IMPB entry. <i>ports</i> - Specify the portlist the entry will apply to. If no ports are specified, the settings will be applied to all ports.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create an IMPB entry:

```
DGS-3450:admin#create address_binding ip_mac ipaddress 10.1.1.1 mac_address 00-00-00-00-00-11
Command: create address_binding ip_mac ipaddress 10.1.1.1 mac_address 00-00-00-00-00-11

Success.

DGS-3450:admin#
```

create address_binding ip_mac

Purpose	Used to create an IMPB entry.
Syntax	create address_binding ip_mac [ipaddress < ipaddr > ipv6address <ipv6addr>] mac_address < macaddr > { ports [portlist all]}
Description	Use this command to create an IMPB entry. One MAC address can map to multiple IP address
Parameters	<i>ipaddr</i> - Specify the IP address used for the IMPB entry. <i>ipv6addr</i> - Specify the IPv6 address used for the IMPB entry. <i>macaddr</i> - Specify the MAC address used for the IMPB entry. <i>ports</i> - Specify the portlist the entry will apply to. If not ports are specified, the settings will be applied to all ports.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create an IMPB entry:

```
DGS-3450:admin# create address_binding ip_mac ipaddress 10.1.1.1 mac_address 00-00-00-00-00-11
Command: create address_binding ip_mac ipaddress 10.1.1.1 mac_address 00-00-00-00-00-11

Success.

DGS-3450:admin#
```

To create a static IPv6 IMPB entry:

```
DGS-3450:admin# create address_binding ip_mac ipv6address fe80::240:5ff:fe00:28
mac_address 00-00-00-00-00-11
Command: create address_binding ip_mac ipv6address fe80::240:5ff:fe00:28 mac_address 00-00-00-00-00-11

Success.

DGS-3450:admin#
```

delete address_binding

Purpose	Used to delete an IMPB entry or blocked entry.
Syntax	delete address_binding [ip_mac [[ipaddress < ipaddr > ipv6address <ipv6addr>] mac_address < macaddr > all] blocked [all vlan_name < vlan_name > mac_address < macaddr >]]
Description	Use this command to delete an IMPB entry or a blocked entry. If the ACL mode is enabled, the switch will delete the related ACL access entries automatically.
Parameters	<i>ip_mac</i> - Specify the user created IMPB database. <i>blocked</i> - Specify the address database that the system has automatically learned and blocked. <i>ipaddr</i> - Specify the learned IP address of the entry in the database. <i>ipv6addr</i> - Specify the learned IPv6 address of the entry in the database. <i>macaddr</i> - Specify the MAC address of the entry or the blocked MAC address. <i>vlan_name</i> - Specify the name of the VLAN to which the blocked MAC address belongs.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete an IMPB entry:

```
DGS-3450:admin# delete address_binding ip_mac ipaddress 10.1.1.1 mac_address 00-00-00-00-00-11
Command: delete address_binding ip_mac ipaddress 10.1.1.1 mac_address 00-00-00-00-00-11

Success.

DGS-3450:admin#
```

To delete a static ipv6 IMPB entry:

```
DGS-3450:admin# delete address_binding ip_mac ipv6address fe80::240:5ff:fe00:28
mac_address 00-00-00-00-00-11
Command: delete address_binding ip_mac ipv6address fe80::240:5ff:fe00:28 mac_address 00-
00-00-00-00-11

Success.

DGS-3450:admin#
```

To delete a blocked address:

```
DGS-3450:admin# delete address_binding blocked vlan_name v31 mac_address 00-00-00-00-00-
11
Command: delete address_binding blocked vlan_name v31 mac_address 00-00-00-00-00-11

Success.

DGS-3450:admin#
```

config address_binding ip_mac

Purpose	Used to update an IMPB entry.
Syntax	config address_binding ip_mac ipaddress <ipaddr> mac_address <macaddr > {ports [portlist all]
Description	This command is used to update an IMPB entry.
Parameters	<i>ipaddr</i> - Specify the IP address of the entry being updated. <i>macaddr</i> - Specify the MAC address of the entry being updated. <i>ports</i> - Specify which ports are used for the IMPB entry being updated. If not specified, then it is applied to all ports.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure an IMPB entry:

```
DGS-3450:admin#config address_binding ip_mac ipaddress 10.1.1.1 mac_address 00-00-00-00-
00-11
Command: config address_binding ip_mac ipaddress 10.1.1.1 mac_address 00-00-00-00-00-11

Success.

DGS-3450:admin#
```

config address_binding ip_mac

Purpose	Used to update an IMPB entry.
Syntax	config address_binding ip_mac [ipaddress < ipaddr > ipv6address <ipv6addr>] mac_address < macaddr > {ports [portlist all]}
Description	This command is used to update an IMPB entry.
Parameters	<i>ipaddr</i> - Specify the IP address of the entry being updated. <i>ipv6addr</i> - Specify the IPv6 address of the entry being updated. <i>macaddr</i> - Specify the MAC address of the entry being updated <i>ports</i> - Specify which ports are used for the IMPB entry being updated. If not specified, then it

config address_binding ip_mac

is applied to all ports.

Restrictions Only Administrator and Operator-level users can issue this command.

Example usage:

To configure an IMPB entry:

```
DGS-3450:admin# config address_binding ip_mac ipaddress 10.1.1.1 mac_address 00-00-00-00-00-11
Command: config address_binding ip_mac ipaddress 10.1.1.1 mac_address 00-00-00-00-00-11

Success.

DGS-3450:admin#
```

To configure a static IPv6 IMPB entry:

```
DGS-3450:admin#config address_binding ip_mac ipv6address fe80::240:5ff:fe00:28
mac_address 00-00-00-00-00-11
Command: config address_binding ip_mac ipv6address fe80::240:5ff:fe00:28 mac_address 00-00-00-00-00-11

Success.

DGS-3450:admin#
```

show address_binding

Purpose	Used to display the IMPB entries, blocked MAC entries and port status.
Syntax	show address_binding [ip_mac [all [ipaddress < ipaddr > ipv6address <ipv6addr>] mac_address < macaddr >] blocked [all vlan_name <vlan_name> mac_address <macaddr>] ports {<portlist>}]
Description	This command is used to show the IMPB information.
Parameters	<p><i>ip_mac</i> - Specify the user created IMPB database.</p> <p><i>blocked</i> - Specify the addresses in the database that the system has auto learned and blocked.</p> <p><i>ipaddr</i> - Specify the learned IP address of the entry in the database.</p> <p><i>ipv6addr</i> - Specify the learned IPv6 address of the entry in the database.</p> <p><i>macaddr</i> - Specify the MAC address of the entry or the blocked MAC address.</p> <p><i>vlan_name</i> - Specify the name of the VLAN to which the blocked MAC address belongs.</p> <p><i>ports</i> - Specify the ports for which the information is displayed. If not specified, all ports are displayed.</p>
Restrictions	None.

Example usage:

To show the IMPB global configuration:

```
DGS-3450:admin# show address_binding
```

```
Command: show address_binding
```

```
Trap/Log           : Enabled
DHCP Snoop(IPv4)   : Disabled
DHCP Snoop(IPv6)   : Enabled
ND Snoop           : Disabled
```

```
DGS-3450:admin#
```

To show the IMPB ports:

```
DGS-3450:admin#show address_binding ports
```

```
Command: show address_binding ports
```

Port	IPv4 State	IPv6 State	Mode	Zero IP	DHCP Packet	Stop Learning Threshold/Mode
1	Loose	Enabled	ARP	Allow	Forward	100/Stop
2	Strict	Enabled	ARP	Not Allow	Not Forward	200/Normal
3	Disabled	Enabled	ACL	Not Allow	Not Forward	200/Normal
4	Strict	Disabled	ARP	Not Allow	Not Forward	200/Normal
5	Disabled	Disabled	ACL	Not Allow	Not Forward	200/Normal
6	Strict	Disabled	ARP	Not Allow	Not Forward	200/Normal
7	Disabled	Disabled	ACL	Not Allow	Not Forward	200/Normal
8	Strict	Disabled	ARP	Not Allow	Not Forward	200/Normal
9	Disabled	Disabled	ACL	Not Allow	Not Forward	200/Normal
10	Strict	Disabled	ARP	Not Allow	Not Forward	200/Normal
11	Disabled	Disabled	ACL	Not Allow	Not Forward	200/Normal
12	Strict	Disabled	ARP	Not Allow	Not Forward	200/Normal

```
DGS-3450:admin#
```

enable address_binding dhcp_snoop

Purpose	Used to enable DHCP snooping mode.
Syntax	enable address_binding dhcp_snoop {[ipv6 all]}
Description	<p>By default, DHCP snooping is disabled.</p> <p>If a user enables DHCP sSnooping mode, all ports which have IMPB disabled will become server ports. (The switch will learn the IP addresses through server ports (by using DHCP Offer and DHCP ACK packets).</p> <p>Note that the DHCP discover packet cannot be passed thru the user ports if the allow_zeroip function is disabled on the port.</p> <p>The auto-learned IMPB entry will be mapped to a specific source port based on the MAC address learning function. This entry will be created as an ACL-mode binding entry for this specific port. Each entry is associated with a lease time. When the lease time has expires, the expired entry will be removed from the port. The auto-learned binding entry can be moved from one port to another port if the DHCP snooping function has learned that the MAC address has moved to a different port.</p> <p>If a situation occurs where a binding entry learned by DHCP snooping conflicts with a statically configured entry. The binding relation has conflicted. For example, if IP A is binded to MAC X with a static configuration and suppose that the binding entry learned by DHCP snooping is that IP A is bound to MAC Y, and then it is conflict. When the DHCP snooping learned entry binds with the static configured entry, and the DHCP snooping learned entry will not be created.</p> <p>In a situation where the same IMPB pair has been statically configured, the auto-learned entry will not be created. In a situation where the learned information is consistent with the</p>

enable address_binding dhcp_snoop

	statically configured entry the auto-learned entry will not be created. In a situation where the entry is statically configured in ARP mode the auto learned entry will not be created. In a situation where the entry is statically configured on one port and the entry is auto-learned on another port, the auto-learned entry will not be created.
Parameters	<i>ipv6</i> - Enable DHCP snooping for IPv6. <i>all</i> - Enable IPv4 and IPv6 DHCP snooping. If no parameter is specified, IPv4 snooping is enabled.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable DHCP IPv4 snooping mode:

```
DGS-3450:admin# enable address_binding dhcp_snoop
Command: enable address_binding dhcp_snoop

Success.

DGS-3450:admin#
```

To enable DHCP IPv6 snooping mode:

```
DGS-3450:admin# enable address_binding dhcp_snoop ipv6
Command: enable address_binding dhcp_snoop ipv6

Success.

DGS-3450:admin#
```

disable address_binding dhcp_snoop

Purpose	Used to disable DHCP snooping mode.
Syntax	disable address_binding dhcp_snoop {[<i>ipv6</i> <i>all</i>]}
Description	When the DHCP snooping function is disabled, all of the auto-learned binding entries will be removed.
Parameters	<i>ipv6</i> - Disable IPv6 DHCP snooping. <i>all</i> - Disable IPv4 and IPv6 DHCP snooping. If no parameter is specified, IPv4 snooping is disabled.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable DHCP IPv4 snooping mode:

```
DGS-3450:admin# disable address_binding dhcp_snoop
Command: disable address_binding dhcp_snoop

Success.

DGS-3450:admin#
```

To disable DHCP IPv6 snooping mode:

```
DGS-3450:admin# disable address_binding dhcp_snoop ipv6
Command: disable address_binding dhcp_snoop ipv6

Success.

DGS-3450:admin#
```

clear address_binding dhcp_snoop binding_entry

Purpose	Used to clear the DHCP snooping entries learned for the specified ports.
Syntax	clear address_binding dhcp_snoop binding_entry ports [<portlist> all] {[ipv6 all]}
Description	To clear the DHCP Snooping entries learned for the specified ports.
Parameters	<i>ports</i> - Specify the list of ports to clear the DHCP snooping learned entries. <i>ipv6</i> - Clear IPv6 DHCP snooping learned entries. <i>all</i> - Clear both IPv4 and IPv6 DHCP snooping learned entries.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To clear DHCP IPv4 snooping entries on ports 1-3:

```
DGS-3450:admin# clear address_binding dhcp_snoop binding_entry ports 1-3
Command: clear address_binding dhcp_snoop binding_entry ports 1-3

Success.

DGS-3450:admin#
```

To clear DHCP IPv6 snooping entries on ports 1-3:

```
DGS-3450:admin# clear address_binding dhcp_snoop binding_entry ports 1-3 ipv6
Command: clear address_binding dhcp_snoop binding_entry ports 1-3 ipv6

Success.

DGS-3450:admin#
```

show address_binding dhcp_snoop

Purpose	Used to display the DHCP snooping configuration and learning database.
Syntax	show address_binding dhcp_snoop {[max_entry { ports <portlist> } binding_entry {port <port>}]}
Description	This command is used to show all DHCP snooping configuration and learning databases.
Parameters	<i>max_entry</i> - To show the maximum number of entries per port. <i>binding_entry</i> - To show DHCP snooping binding entries on ports. If no ports specified show all binding entries. If no parameters are specified, show DHCP snooping displays the enable/disable state.
Restrictions	None.

Example usage:

To show the DHCP snooping state:


```
DGS-3450:admin# show address_binding dhcp_snoop
Command: show address_binding dhcp_snoop

DHCP Snoop(IPv4) : Enabled
DHCP Snoop(IPv6) : Enabled

DGS-3450:admin#
```

config address_binding dhcp_snoop max_entry

Purpose	Used to specify the maximum number of entries that can be learned by a specified port.
Syntax	config address_binding dhcp_snoop max_entry ports [<portlist> all] limit [<value 1-50> no_limit]
Description	By default, the maximum number of port entries is unlimited. This command specifies the maximum number of entries that can be learned by the specified ports.
Parameters	<i>portlist</i> - Specify the list of ports you would like to set the maximum number of entries that can be learned. <i>all</i> - indicates all ports on the Switch. <i>limit</i> - See below: <value 1-50> - Specify the maximum number. <i>no_limit</i> - Specifies that the maximum number of learned entries is unlimited.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To set the maximum number of DHCP IPv4 snooping entries that ports 1–3 can learned to 10:

```
DGS-3450:admin# config address_binding dhcp_snoop max_entry ports 1-3 limit 10.
Command: config address_binding dhcp_snoop max_entry ports 1-3 limit 10.

Success.

DGS-3450:admin#
```

To set the maximum number of DHCP IPv6 snooping entries that ports 1 –3 can learned to 10:

```
DGS-3450:admin# config address_binding dhcp_snoop max_entry ports 1-3 limit 10 ipv6
Command: config address_binding dhcp_snoop max_entry ports 1-3 limit 10 ipv6

Success.

DGS-3450:admin#
```

enable address_binding trap_log

Purpose	Used to enable IMPB traps and logs.
Syntax	enable address_binding trap_log
Description	This command is used to send traps and logs when the IMPB module detects an illegal IP and MAC address.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable the IMPB traps and logs:

```
DGS-3450:admin# enable address_binding trap_log
Command: enable address_binding trap_log

Success.

DGS-3450:admin#
```

disable address_binding trap_log

Purpose	Used to disable the IMPB traps and logs.
Syntax	disable address_binding trap_log
Description	This command is used to disable IMPB traps and logs.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable IMPB traps and logs:

```
DGS-3450:admin# disable address_binding trap_log
Command: disable address_binding trap_log

Success.

DGS-3450:admin#
```

config address_binding recover_learning ports

Purpose	Used to recover IMPB checking.
Syntax	config address_binding recover_learning ports [<portlist> all]
Description	Use this command to recover the IMPB check function, which was previously stopped.
Parameters	<i>ports</i> - See below: <portlist> - Specify the list of ports that need to recover the IMPB check. <i>all</i> - Indicates all the ports on the Switch.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To recover IMPB checking for ports 6 to 7:

```
DGS-3450:admin# config address_binding recover_learning ports 6-7
Command: config address_binding recover_learning ports 6-7

Success.

DGS-3450:admin#
```

enable address_binding nd_snoop

Purpose	Use to enable ND snooping on the switch.
Syntax	enable address_binding nd_snoop
Description	This command allows the user to enable ND snooping on the switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable the ND snooping function on the switch:

```
DGS-3450:admin# enable address_binding nd_snoop
Command: enable address_binding nd_snoop

Success.

DGS-3450:admin#
```

disable address_binding nd_snoop

Purpose	Use to disable ND snooping on the switch.
Syntax	disable address_binding nd_snoop
Description	This command allows the user to disable ND Snooping on switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable the DHCPv6 snooping function on the switch:

```
DGS-3450:admin# disable address_binding nd_snoop
Command: disable address_binding nd_snoop

Success.

DGS-3450:admin#
```

show address_binding nd_snoop

Purpose	Use to display the status of ND snooping on the switch.
Syntax	show address_binding nd_snoop
Description	This command allows the user to display the ND snooping state on the switch.
Parameters	None.
Restrictions	None.

Example usage:

To show ND snooping state:

```
DGS-3450:admin# show address_binding nd_snoop
Command: show address_binding nd_snoop

ND Snoop      : Enabled

DGS-3450:admin#
```

To show ND snooping maximum entry:

```
DGS-3450:admin# show address_binding nd_snoop ports 1-12
Command: show address_binding nd_snoop ports 1-12
Port          Max Entry
-----
1             10
2             10
3             10
4             No Limit
5             No Limit
6             No Limit
7             No Limit
8             No Limit
9             No Limit
10            No Limit
11            No Limit
12            No Limit

DGS-3450:admin#
```

show address_binding nd_snoop binding_entry

Purpose	Used to show binding entries of ND snooping on the switch.
Syntax	show address_binding nd_snoop binding_entry {port <port>}
Description	This command allows the user to display binding entries of ND Snooping on the switch.
Parameters	<i>port</i> - Specify port number If no parameter is specified, it will show all ND snooping binding entries.
Restrictions	None.

Example usage:

To display the ND snooping binding entry:

```
DGS-3450:admin# show address_binding nd_snoop binding_entry
Command: show address_binding nd_snoop binding_entry
S (Status) - A: Active, I: Inactive
Time - Left Time (sec)
IP Address          MAC Address          S   Time          Port
-----
2001:2222:1111:7777:5555:6666:7777:8888  00-00-00-00-00-02   I   50              5
2001::1             00-00-00-00-03-02   A  100              6

Total entries : 2
```

clear address_binding nd_snoop binding_entry

Purpose	Used to clear the ND snooping entries on specified ports.
Syntax	clear address_binding nd_snoop binding_entry ports [<portlist> all]
Description	To clear the entries learned for the specified ports.
Parameters	<i>ports</i> - Specify the list of ports that you would like to clear the ND snoop learned entry. <i>all</i> - Clear all ND snooping learned entries.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To clear ND snooping entry on ports 1-3:

```
DGS-3450:admin# clear address_binding nd_snoop binding_entry ports 1-3
Command: clear address_binding nd_snoop binding_entry ports 1-3

Success.

DGS-3450:admin#
```

debug address_binding

Purpose	Start the IMPB debug when the IMPB module receives an ARP/IP packet or a DHCP packet.
Syntax	debug address_binding [event dhcp all]
Description	Use this command to start the IMPB debug when the IMPB module receives an ARP/IP packet or a DHCP packet.
Parameters	<i>event</i> - To print out the debug messages when IMPB module receives ARP/IP packets. <i>dhcp</i> - To print out the debug messages when the IMPB module receives the DHCP packets. <i>all</i> - Print out all debug messages.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To print out all debug IMPB messages:

```
DGS-3450:admin# debug address_binding all
Command: debug address_binding all

Success.

DGS-3450:admin#
```

no debug address_binding

Purpose	Stop the IMPB debug starting when the IMPB module receives an ARP/IP packet or a DHCP packet.
Syntax	no debug address_binding
Description	Use this command to stop the IMPB debug starting when the IMPB module receives an ARP/IP packet or a DHCP packet.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To stop IMPB debug: starting when the IMPB module receives an ARP/IP or DHCP packet:

```
DGS-3450:admin# no debug address_binding
```

```
Command: no debug address_binding
```

```
Success.
```

```
DGS-3450:admin#
```

IP MULTICAST VLAN REPLICATION COMMANDS

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

Command	Parameters
enable ipmc_vlan_replication	
disable ipmc_vlan_replication	
config ipmc_vlan_replication	{ttl [decrease no_decrease] src_mac [replace no_replace]}(1)
create ipmc_vlan_replication_entry	<name 16>
config ipmc_vlan_replication_entry source	<name 16> [[vlan <vlan_name 32> vlanid <vlanid 1-4094>] group [add delete] [mcast_ip <mcast_address_list> mcast_ipv6 <mcastv6_address_list>] {[source_ip <ipaddr> source_ipv6 <ip6addr>}]
config ipmc_vlan_replication destination_entry	<name 16> [add delete] [vlan <vlan_name 32> vlanid <vidlist>] ports <portlist>
delete ipmc_vlan_replication_entry	<name 16>
show ipmc_vlan_replication	
show ipmc_vlan_replication_entry	{<name 16> hardware}

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

enable ipmc_vlan_replication

Purpose	Used to enable static IP multicast VLAN replication on the switch.
Syntax	enable ipmc_vlan_replication
Description	This command is used to enable static IP multicast VLAN replication on the switch. By default, the replication function is enabled.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable static IP multicast VLAN replication:

```
DGS-3450:admin# enable ipmc_vlan_replication
Command: enable ipmc_vlan_replication
```

```
Success.
```

```
DGS-3450:admin#
```

disable ipmc_vlan_replication

Purpose	Used to disable static IP multicast VLAN replication on the switch.
Syntax	disable ipmc_vlan_replication
Description	This command is used to disable static IP multicast VLAN replication on the switch.

disable ipmc_vlan_replication

Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable static IP multicast VLAN replication:

```
DGS-3450:admin# disable ipmc_vlan_replication
Command: disable ipmc_vlan_replication

Success.

DGS-3450:admin#
```

config ipmc_vlan_replication

Purpose	Used to configure IP multicast VLAN replication global setting.
Syntax	config ipmc_vlan_replication { ttl [decrease no_decrease] src_mac [replace no_replace]}(1)
Description	Generally, when a multicast packet is forwarded across VLANs, the TTL will be decreased by one. If no_decrease is specified, the TTL will not be decreased. Similarly, it can be specified to replace a source MAC address for a packet to be forwarded across VLANs.
Parameters	<i>ttl</i> - Species whether to decrease the time to live of packet. By default, the TTL will be decreased. <i>src_mac</i> - Specifies whether to replace a source MAC address of a packet. By default, the source MAC address will be replaced.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure an IP multicast VLAN replication's TTL:

```
DGS-3450:admin# config ipmc_vlan_replication ttl no_decrease
Command: config ipmc_vlan_replication ttl no_decrease

Success.

DGS-3450:admin#
```

create ipmc_vlan_replication_entry

Purpose	Used to create an IP multicast VLAN replication entry.
Syntax	create ipmc_vlan_replication_entry <name 16>
Description	This command creates an IPMC VLAN replication entry. The entry will be identified by name. An IP multicast VLAN replication entry defines what traffic will be replicated and how the packet will be replicated.
Parameters	<i>name</i> - The name of the IP multicast VLAN replication entry.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

Create an IP multicast VLAN replication entry named mr1:

```
DGS-3450:admin# create ipmc_vlan_replication_entry mr1
Command: create ipmc_vlan_replication_entry mr1

Success.

DGS-3450:admin#
```

config ipmc_vlan_replication_entry source

Purpose	Used to configure source traffic of an IP multicast VLAN replication entry.
Syntax	config ipmc_vlan_replication_entry source <name 16> [[vlan <vlan_name 32> vlanid <vlanid 1-4094>] group [add delete] [mcast_ip <mcast_address_list> mcast_ipv6 <mcastv6_address_list>] [{source_ip <ipaddr> source_ipv6 <ip6addr>}]]
Description	<p>This command is used to configure the traffic to be replicated by the IP multicast VLAN replication entry. The traffic is described as a source VLAN, a list of multicast group address and an optional source IP address associated with the multicast group. Each (V, G, S) will consume one resource entry. The number of supported resource entries is project dependent. Therefore, the resource entry consumed by a replication entry is not constant and it will be determined by the number of (V, G, S) pair defined by the entry.</p> <p>If the entry (V, G, S) exists in two replication entries, both will take effect. The traffic will be replicated to the destination defined by both entries.</p> <p>If the entries (V, G, S) and (V, G, *) both exist in the table, the entries (V,G, S) will not take effect.</p>
Parameters	<p><i>name</i> - The name of the IP multicast VLAN replication entry to be configured.</p> <p><i>vlan</i> - The source VLAN name.</p> <p><i>vlanid</i> - The source VLAN ID.</p> <p><i>group</i> - Specifies the multicast IP address list.</p> <p><i>mcast_ip</i> - The multicast IP address list.</p> <p><i>source_ip</i> - The source IP address.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To set the source VLAN of an IP multicast VLAN replication entry to VLAN v2:

```
DGS-3450:admin# config ipmc_vlan_replication_entry source mr1 vlan v2
Command: config ipmc_vlan_replication_entry source mr1 vlan v2
Success.

DGS-3450:admin#
```

config ipmc_vlan_replication_entry destination

Purpose	Used to configure the destination of an IP multicast VLAN replication entry.
Syntax	config ipmc_vlan_replication_destination_entry <name 16> [add delete] [vlan <vlan_name 32> vlanid <vidlist>] ports <portlist>
Description	For the traffic that matches an IPMC VLAN replication entry, it will be replicated based on the destination setting. Multiple destination entries can be defined for an IPMC VLAN replication entry. Each destination entry specifies the VLAN and the outgoing port on which the traffic will be replicated. The outgoing port must be a member port of the VLAN. Whether a packet egress to a port is tagged or untagged will be determined by the VLAN setting.
Parameters	<i>name</i> - The name of the IP multicast VLAN replication entry to be configured.

config ipmc_vlan_replication_entry destination

vlan - The outgoing VLAN name.
vlanid - The outgoing VLAN ID.
ports - The outgoing port list.

Restrictions Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the destination of an IP multicast VLAN replication entry named mr1:

```
DGS-3450:admin# config ipmc_vlan_replication_entry mr1 add vlanid 5 port 10-17
Command: config ipmc_vlan_replication_entry mr1 add vlanid 5 port 10-17
```

Success.

```
DGS-3450:admin#
```

delete ipmc_vlan_replication_entry destination

Purpose	Used to delete an IP multicast VLAN replication entry.
Syntax	delete ipmc_vlan_replication_entry <name 16>
Description	This command deletes an IP multicast VLAN replication entry.
Parameters	<i>name</i> - The name of the IP multicast VLAN replication entry to be deleted.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete an IP multicast VLAN replication entry named mr1:

```
DGS-3450:admin# delete ipmc_vlan_replication_entry mr1
Command: delete ipmc_vlan_replication_entry mr1
```

Success.

```
DGS-3450:admin#
```

show ipmc_vlan_replication

Purpose	Used to display the IP multicast VLAN replication global setting.
Syntax	show ipmc_vlan_replication
Description	This command is used to display the IP multicast VLAN replication global setting.
Parameters	None.
Restrictions	None.

Example usage:

This example displays the IP multicast VLAN replication global setting:

```
DGS-3450:admin# show ipmc_vlan_replication
Command: show ipmc_vlan_replication

IP Multicast VLAN Replication State : Enabled
TTL                                  : No Decrease
Source MAC Address                   : No Replace

DGS-3450:admin#
```

show ipmc_vlan_replication_entry

Purpose	Used to display the IP multicast VLAN replication entries.
Syntax	show ipmc_vlan_replication_entry {<name 16> hardware}
Description	This command is used to display the IP multicast VLAN replication entry. The "active/inactive" status indicates whether the entry is inserted into chip successfully.
Parameters	<i>name</i> - The name of the IP multicast VLAN replication entry to be deleted. <i>hardware</i> - Show the (S,G) groups which are in the chipset.
Restrictions	None.

Example usage:

This example displays the IP multicast VLAN replication entry named mr1:

```
DGS-3450:admin# show ipmc_vlan_replication_entry mr1
Command: show ipmc_vlan_replication_entry mr1
IP Multicast VLAN Replication Name   : mr1
-----
Source
VLAN ID/Name : 1/default
Multicast Group Address List (G/S)
      225.1.1.1-225.1.1.10 / *
      225.1.1.1-225.1.1.10 / 10.0.0.1

Destination
VLAN ID/Name : 2/ VLAN2
Portlist     : 1:1-1:11,1:13

DGS-3450:admin#
```

This example displays the IP multicast VLAN replication groups' in the hardware:

```
DGS-3450:admin# show ipmc_vlan_replication_entry hardware
```

```
Command: show ipmc_vlan_replication_entry hardware
```

```
Name      : ipmc_vlan_replication_entry name
```

```
Src-v     : The source VLAN
```

```
Dest-v    : The destination VLAN
```

Name	Src-V	Group	SIP	Dest-V	Portlist
mr1	1	255.1.1.1	*	2	1:1-1:11, 1:13
mr1	1	255.1.1.1	*	3	1:12, 1:15
mr1	1	255.1.1.1	10.0.0.1	2	1:1-1:11, 1:13
mr1	1	255.1.1.1	10.0.0.1	3	1:12, 1:15
mr2	3	255.1.1.2	*	2	1:5-1:6
mr2	3	255.1.1.2	10.0.0.1	2	1:5-1:6

```
DGS-3450:admin#
```

IPv6 Neighbor Discover Commands

The IPv6 Neighbor Discover commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameters
create ipv6 neighbor_cache ipif	<ipif_name 12> <ipv6addr> <macaddr>
delete ipv6 neighbor_cache ipif	[<ipif_name 12> all] [<ipv6addr> static dynamic all]
show ipv6 neighbor_cache ipif	[<ipif_name 12> all] [ipv6address <ipv6addr> static dynamic all]
config ipv6 nd ns ipif	<ipif_name 12> retrans_time <millisecond 0-4294967295>
config ipv6 nd ra ipif	<ipif_name 12> {state [enable disable] life_time <sec 0-9000> reachable_time < millisecond 0-3400000> retrans_time <millisecond 0-4294967295> hop_limit <value 0-255> managed_flag [enable disable] other_config_flag [enable disable] min_rtr_adv_interval <sec 3-1350> max_rtr_adv_interval <sec 4-1800>} (1)
config ipv6 nd ra prefix_option ipif	<ipif_name 12> <ipv6networkaddr> {preferred_life_time <sec 0-4294967295> valid_life_time <sec 0-4294967295> on_link_flag [enable disable] autonomous_flag [enable disable]} (1)
show ipv6 nd	{ipif <ipif_name 12>}

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

create ipv6 neighbor_cache

Purpose	Adds a static neighbor on an IPv6 interface.
Syntax	create ipv6 neighbor_cache ipif <ipif_name 12> <ipv6addr> <macaddr>
Description	Adds a static neighbor on an IPv6 interface.
Parameters	<i>ipif_name</i> - Interface's name. <i>ipv6addr</i> - The address of the neighbor. <i>macaddr</i> - The MAC address of the neighbor.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create a static neighbor cache entry on the interface System, with an IPv6 address of 3ffc::1 and a MAC address of 00:01:02L03:04:05:

```
DGS-3450:admin# create ipv6 neighbor_cache ipif System 3ffc::1 00:01:02:03:04:05
Command: create ipv6 neighbor System _cache ipif 3FFC::1 00:01:02:03:04:05

Success.

DGS-3450:admin#
```

delete ipv6 neighbor_cache

Purpose	Deletes an IPv6 neighbor from the interface neighbor address cache.
Syntax	delete ipv6 neighbor_cache ipif [<ipif_name 12> all] [<ipv6addr> static dynamic

delete ipv6 neighbor_cache

	all]
Description	Deletes a neighbor cache entry or static neighbor cache entries from the address cache or all address cache entries on this IP interface. Both static and dynamic entries can be deleted.
Parameters	<i>ipif_name</i> - The IPv6 interface name <i>ipv6addr</i> - The neighbor's address. <i>all</i> - All entries including static and dynamic entries will be deleted. <i>dynamic</i> - Delete matching dynamic entries. <i>static</i> - Delete matching static entries.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete the neighbor cache entry for IPv6 address 3ffc::1 on the IP interface "System":

```
DGS-3450:admin# delete ipv6 neighbor_cache ipif System 3ffc::1
```

```
Command: delete ipv6 neighbor_cache ipif System 3FFC::1
```

Success.

```
DGS-3450:admin#
```

show ipv6 neighbor_cache

Purpose	Shows the IPv6 neighbor cache.
Syntax	show ipv6 neighbor_cache ipif [<ipif_name 12> all] [ipv6address <ipv6addr> static dynamic all]
Description	Displays the neighbor cache entry for the specified interface. You can display a specific entry, all static entries, all dynamic entries, or all entries.
Parameters	<i>ipif_name</i> - The IPv6 interface name <i>ipv6addr</i> - The neighbor's address. <i>all</i> - Displays all interfaces. <i>dynamic</i> - Display all dynamic entries. <i>static</i> - Display all static neighbor cache entries. <i>all</i> - Displays all entries including static and dynamic entries.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To show all neighbor cache entries for the IP interface "System":

```
DGS-3450:admin# show ipv6 neighbor_cache ipif System all
Command: show ipv6 neighbor_cache ipif System all

IPv6 Address: 2000::221:91FF:FE8D:4D9F          State: Reachable
MAC Address  : 00-21-91-8D-4D-9F    Port  : 1:31
Interface   : ipif1                  VID   : 4094

IPv6 Address: 3000::100                      State: Reachable
MAC Address  : 00-21-91-8D-4D-9F    Port  : 1:31
Interface   : ipif1                  VID   : 4094

IPv6 Address: FE80::221:91FF:FE8D:4D9F       State: Reachable
MAC Address  : 00-21-91-8D-4D-9F    Port  : 1:31
Interface   : ipif1                  VID   : 4094

Total Entries: 3

DGS-3450:admin#
```

config ipv6 nd ns retrans_time

Purpose	Configures the IPv6 ND neighbor solicitation retransmit time · which is the time between the retransmission of neighbor solicitation messages to a neighbor, when resolving the address or when probing the reachability of a neighbor.
Syntax	config ipv6 nd ns ipif <ipif_name 12> retrans_time <millisecond 0-4294967295>
Description	Configures the retransmit time of IPv6 ND neighbor solicitation.
Parameters	<p><i>ipif_name</i> - The IPv6 interface name.</p> <p><i>retrans_time</i> - Neighbor solicitation's retransmit timer in milliseconds. It has the same value as the RA retrans_time in the config IPv6 ND RA command. If the retrans_time parameter is configured in one of the commands, the retrans_time value in the other command will also change so that the values in both commands are the same.</p> <p>If the value user configured is less than 1000ms, Neighbor solicitation's retransmit timer of the device will use 1000ms instead of that value.</p> <p>If the value user configured is large than 1000ms, Neighbor solicitation's retransmit timer of the device will use that value.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the retrans_time of IPv6 ND neighbor solicitation to be 1000000 milliseconds:

```
DGS-3450:admin# config ipv6 nd ns ipif Zira retrans_time 1000000
Command: config ipv6 nd ns ipif Zira retrans_time 1000000

Success.

DGS-3450:admin#
```

config ipv6 nd ra

Purpose	Configures router advertisement related arguments.
Syntax	config ipv6 nd ra ipif <ipif_name 12> {state [enable disable] life_time <sec 0-9000> reachable_time < millisecond 0-3400000> retrans_time <millisecond 0-4294967295> hop_limit <value 0-255> managed_flag [enable disable] other_config_flag [enable

config ipv6 nd ra

	disable] min_rtr_adv_interval <sec 3-1350> max_rtr_adv_interval <sec 4-1800>} (1)
Description	Configures the router advertisement related parameters.
Parameters	<p><i>ipif_name</i> - The name of the interface.</p> <p><i>state</i> - Router advertisement state.</p> <p><i>life_time</i> - Indicates the lifetime of the router as the default router in seconds.</p> <p><i>reachable_time</i> - Indicates the amount of time that a node can consider a neighboring node reachable after receiving a reachability confirmation in milliseconds.</p> <p><i>retrans_time</i> - Indicates the amount of time between retransmissions of router advertisement messages in milliseconds, where the router advertisement packet will be taken to it's host. If the value user configured is less than 1000ms, the device will send RA with that value, but the device's(which received RA) retransmission time of NS messages will use 1000ms instead of it.</p> <p>If the value user configured is large than 1000ms, the device will send RA with that value, and the device's(which received RA) retransmission time of NS messages will also use that value.</p> <p><i>hop_limit</i> - Indicates the default value of the hop limit field in the IPv6 header for packets sent by hosts that receive this RA message.</p> <p><i>managed_flag</i> - When set to enable, it indicates that hosts receiving this RA must use a stateful address configuration protocol to obtain an address, in addition to the addresses derived from the stateless address configuration.</p> <p><i>other_config_flag</i> - When set to enable, it indicates that hosts receiving this RA must use a stateful address configuration protocol to obtain on-address configuration information,.</p> <p><i>min_rtr_adv_interval</i> - The minimum time allowed between sending unsolicited multicast Router Advertisements from the interface, in seconds. MUST be no less than 3 seconds and no greater than $.75 * \text{MaxRtrAdvInterval}$. Default: $0.33 * \text{MaxRtrAdvInterval}$.</p> <p><i>max_rtr_adv_interval</i> - The maximum time allowed between sending unsolicited multicast Router Advertisements from the interface, in seconds. MUST be no less than 4 seconds and no greater than 1800 seconds. Default: 600 seconds.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the RA state as enabled and the life_time of the "triton" interface to be 1000 seconds:

```
DGS-3450:admin#config ipv6 nd ra ipif triton state enable life_time 1000
Command: config ipv6 nd ra ipif triton state enable life_time 1000
```

Success.

```
DGS-3450:admin#
```

config ipv6 nd ra prefix_option

Purpose	Configures the prefix option for the router advertisement function.
Syntax	config ipv6 nd ra prefix_option ipif <ipif_name 12> <ipv6networkaddr> {preferred_life_time <sec 0-4294967295> valid_life_time <sec 0-4294967295> on_link_flag [enable disable] autonomous_flag [enable disable]} (1)
Description	Configures the prefix option for the router advertisement function.
Parameters	<p><i>ipif_name</i> - The name of the interface.</p> <p><i>preferred_life_time</i> - Indicates the number of seconds that an address, based on the specified prefix using the stateless address configuration, remains in preferred state. For an infinite valid lifetime the value can be set to 0xffffffff.</p>

config ipv6 nd ra prefix_option

valid_life_time - Indicates the number of seconds that an address, based on the specified prefix, using the stateless address configuration, remains valid. For an infinite valid lifetime the value can be set to 0xffffffff.

on_link_flag - When set to 1 the addresses implied by the specified prefix are available on the link where the RA message is received.

autonomous_flag - When set to 1 the specified prefix will be used to create an autonomous address configuration.

Restrictions Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the value of the preferred_life_time of prefix option to be 1000 seconds for the prefix 3ffe:501:ffff:100::/64, which is the prefix of the ip1 interface :

```
DGS-3450:admin# config ipv6 nd ra prefix_option ipif ip1 3ffe:501:ffff:100::/64
preferred_life_time 1000
```

```
Command: config ipv6 nd ra prefix_option ipif ip1 3ffe:501:ffff:100::/64
preferred_life_time 1000
```

Success.

```
DGS-3450:admin#
```

show ipv6 nd

Purpose Used to display information regarding neighbor detection on the switch.

Syntax **show ipv6 nd {ipif <ipif_name 12>}**

Description To show IPv6 ND related configuration.

Parameters *ipif_name* - The name of the interface.

If no IP interface is specified, it will show the IPv6 ND related configuration of all interfaces.

Restrictions Only Administrator and Operator-level users can issue this command.

Example usage:

To show IPv6 ND related configuration:

```
DGS-3450:admin# show ipv6 nd ipif System
```

```
Command: show ipv6 nd ipif System
```

```
Interface Name           : System
Hop Limit                : 64
NS Retransmit Time       : 0 (ms)
Router Advertisement     : Disabled
RA Max Router AdvInterval : 600 (s)
RA Min Router AdvInterval : 198 (s)
RA Router Life Time      : 1800 (s)
RA Reachable Time        : 1200000 (ms)
RA Retransmit Time       : 0 (ms)
RA Managed Flag          : Disabled
RA Other Config Flag     : Disabled
```

Prefix	Preferred	Valid	OnLink	Autonomous
2000::/64	604800	2592000	Enabled	Enabled
2002::/64	604800	2592000	Enabled	Enabled

IPv6 ROUTE COMMANDS

The IPv6 Route commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameters
create ipv6route	[default <ipv6networkaddr>] [[<ipif_name 12> <ipv6addr> <ipv6addr>] {<metric 1-65535>} {[primary backup]} ip_tunnel <tunnel_name 12>]
delete ipv6route	[[default <ipv6networkaddr>] [<ipif_name 12> <ipv6addr> <ipv6addr> ip_tunnel <tunnel_name 12>] all]
show ipv6route	{<ipv6networkaddr>} {[static ripng]}

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

create ipv6route

Purpose	Used to create static IPv6 route entry to Switch's IPv6 routing table.
Syntax	create ipv6route [default <ipv6networkaddr>] [[<ipif_name 12> <ipv6addr> <ipv6addr>] {<metric 1-65535>} {[primary backup]} ip_tunnel <tunnel_name 12>]
Description	<p>Create a static IPv6 route entry. If the next hop is a global address, it is not needed to indicate the interface name of the next hop. If the next hop is a link local address, then the interface name of the next hop must be specified. And the unspecified address, loop back address or multicast address can't be configured as the next hop.</p> <p>Note: If an IPv6 global address is added on interface, this local route will be wrote into IPv6 routing table automatically.</p> <p>If both the destination network address and next hop of the new route entry are the same with existed entry, the created command for the new entry will return failure. If only the destination network address is the same with the existed entry and both primary and backup route entries are already existed, the created command for the new entry will return failure. The IP tunnel route doesn't support to create the backup route.</p>
Parameters	<p><i>default</i> - Specify that this route is created as a default route.</p> <p><i>ipv6networkaddr</i> - The destination network of the route.</p> <p><i>ipif_name</i> - The interface name of the next hop, with the maximum of 12 characters.</p> <p><i>ipv6addr</i> - The next hop address of this route.</p> <p><i>metric</i> - The metric for this route, the default value is 1.</p> <p><i>primary</i> - Specify the route as the primary route to the destination.</p> <p><i>backup</i> - Specify the route as the backup route to the destination. If the route is not specified as the primary route or the backup route, then it will be auto-assigned by the system. The first created is the primary, the second created is the backup.</p> <p><i>tunnel_name</i> - The IP tunnel interface name of the next hop. When this option is specified, it is indicated that this new created route is an IP tunnel route.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To add a single static IPv6 route entry in IPv6 format:

```
DGS-3450:admin# create ipv6route 3004::/64 Intface_1 3000::4
Command: create ipv6route 3004::/64 Intface_1 3000::4

Success.

DGS-3450:admin#
```

To add an IP tunnel route entry:

```
DGS-3450:admin# create ipv6route default ip_tunnel ip6_tn
Command: create ipv6route default ip_tunnel ip6_tn

Success.

DGS-3450:admin#
```

delete ipv6route

Purpose	Delete static IPv6 route entries or specified static route entry from Switch's IPv6 routing table
Syntax	delete ipv6route [[default <ipv6networkaddr>] [<ipif_name 12> <ipv6addr> <ipv6addr> ip_tunnel <tunnel_name 12>] all]
Description	Delete a static IPv6 route. If the next hop is a global address, it is not needed to specify the interface name of the next hop. If the next hop is a link local address, then the interface name of the next hop must be specified.
Parameters	<p><i>default</i> - Specify that the route to be deleted is a default route.</p> <p><i>ipv6networkaddr</i> - The destination network of the route.</p> <p><i>ipif_name</i> - The interface name of the next hop, with the maximum of 12 characters.</p> <p><i>ipv6addr</i> - The next hop address of the default route.</p> <p><i>tunnel_name</i> - The tunnel name of the next hop. When this option is specified, it is indicated that this route to be deleted is an IP tunnel route.</p> <p><i>all</i> - All static IPv6 routes will be deleted.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

Delete a static IPv6 route specified by network address:

```
DGS-3450:admin# delete ipv6route 3004::/64 Intface_1 3000::4
Command: delete ipv6route 3004::/64 Intface_1 3000::4
Success.

DGS-3450:admin#
```

show ipv6route

Purpose	Display the Switch's current IPv6 routing table or specified route entries.
Syntax	show ipv6route [{<ipv6networkaddr>}] [{ static ripng }]
Description	Display IPv6 routes in the switch. If this command is not specified by address or route protocol, it will display all the route entries in the routing table. And if this command specified by address or route protocol, it will display the specified IPv6 route entries.
Parameters	<p><i>ipv6networkaddr</i> - The destination network of the route.</p> <p><i>static</i> - Display the static route entries.</p>

show ipv6route*ripng* - Display the RIPng route entries.

Restrictions

Only Administrator and Operator-level users can issue this command.

Example usage:

Show the IPv6 route entries without specified address or route protocol:

```

DGS-3450:admin# show ipv6route
Command: show ipv6route

IPv6 Prefix: ::/0                Protocol: Static   Metric: 1
Next Hop   : 3000::2            IPIF    : Intface_1

IPv6 Prefix: 3000::/64          Protocol: Local    Metric: 1
Next Hop   : ::                 IPIF    : Intface_1

IPv6 Prefix: 3004::/64          Protocol: Static   Metric: 1
Next Hop   : 3000::4            IPIF    : Intface_1

IPv6 Prefix: 3005::/64          Protocol: RIPng    Metric: 1
Next Hop   : 3000::5            IPIF    : Intface_1

IPv6 Prefix: 4000::/64          Protocol: Local    Metric: 1
Next Hop   : ::                 IPIF    : Intface_2

IPv6 Prefix: 4005::/64          Protocol: RIPng    Metric: 1
Next Hop   : 4000::5            IPIF    : Intface_2

Total Entries: 6

DGS-3450:admin#

```

IPv6 TUNNEL COMMANDS

Industry is in the early stages of large scale IPv6 production deployment, and first-generation products need to make tradeoffs between available IPv6 services. Although the success of IPv6 will ultimately depend on the new applications that run over IPv6, there might be organizations or hosts within organizations that will continue to use IPv4 indefinitely.

A key part of the IPv6 design is its ability to integrate into and coexist with existing IPv4 networks. It is expected that IPv4 and IPv6 hosts will need to coexist for a substantial time during the steady migration from IPv4 to IPv6, and the development of transition strategies, tools, and mechanisms has been part of the basic IPv6 design from the start.

The IPv6 tunneling mechanism is one of the strategies for solving the transition from IPv4 to IPv6. This document describes three types of IPv6 tunnels: IPv6 Manually Configured tunnels, Automatic 6to4 Tunnels and ISATAP Tunnels.

The IPv6 Tunnel commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameters
create ip_tunnel	<tunnel_name 12>
delete ip_tunnel	<tunnel_name 12>
config ip_tunnel manual	<tunnel_name 12> {ipv6address <ipv6networkaddr> source <ipaddr> destination <ipaddr>}(1)
config ip_tunnel 6to4	<tunnel_name 12> {ipv6address <ipv6networkaddr> source <ipaddr >}(1)
config ip_tunnel isatap	<tunnel_name 12> {ipv6address <ipv6networkaddr> source <ipaddr>}(1)
show ip_tunnel	{<tunnel_name 12>}
enable ip_tunnel	{<tunnel_name 12>}
disable ip_tunnel	{<tunnel_name 12>}

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

create ip_tunnel

Purpose	Used to create an IPv6 tunnel interface.
Syntax	create ip_tunnel < tunnel_name 12>
Description	The create ip_tunnel command is used to create an IPv6 tunnel interface on the Switch.
Parameters	<tunnel_name 12> - IPv6 Tunnel interface name, maximum of 12 characters.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create an IPv6 tunnel interface (Tunnel name is "tn2").:

```
DGS-3450:admin# create ip_tunnel tn2
Command: create ip_tunnel tn2

Success.

DGS-3450:admin#
```

delete ip_tunnel

Purpose	Used to delete an IPv6 tunnel interface.
Syntax	delete ip_tunnel < tunnel_name 12>
Description	The delete ip_tunnel command is used to delete a specific IPv6 tunnel on the switch.
Parameters	<tunnel_name 12> - IPv6 Tunnel interface name, maximum of 12 characters.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete an IPv6 tunnel interface (Tunnel name is "tn2"):

```
DGS-3450:admin# delete ip_tunnel tn2
```

```
Command: delete ipif tunnel tn2
```

```
Success.
```

```
DGS-3450:admin#
```

config ip_tunnel manual

Purpose	This command is used to configure an IPv6 manual tunnel.
Syntax	config ip_tunnel manual <tunnel_name 12> {ipv6address <ipv6networkaddr> source <ipaddr> destination <ipaddr>}(1)
Description	<p>The config ip_tunnel manual command is used to configure an existing IPv6 tunnel as an IPv6 manual tunnel on the switch. If this tunnel has previously been configured in another mode, the tunnel's information will still exist in the database. However, whether the tunnel's former information is invalid or not, will depend on the current mode.</p> <p>IPv6 Manual tunnels are simple point-to-point tunnels that can be used within a site or between sites.</p>
Parameters	<p>< tunnel_name 12> - IPv6 Tunnel interface name, maximum of 12 characters.</p> <p><i>ipv6address <ipv6networkaddr></i> - The IPv6 address assigned to this IPv6 tunnel interface. IPv6 processing would be enabled on this IPv6 tunnel interface when an IPv6 address is configured. This IPv6 address is not connected with tunnel source or destination IPv4 address.</p> <p><i>source <ipaddr></i> - The source IPv4 address of this IPv6 tunnel interface. It is used as the source address for packets in this IPv6 tunnel.</p> <p><i>destination <ipaddr></i> - The destination IPv4 address of this IPv6 tunnel interface. It is used as the destination address for packets in this IPv6 tunnel. It is not required for 6to4 and ISATAP tunnels.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure an IPv6 manual tunnel (Tunnel name is "tn2", Tunnel source IPv4 address is 1.0.0.1, Tunnel destination IPv4 address is 1.0.0.2, Tunnel IPv6 address is 2001::1/64):

```
DGS-3450:admin# config ip_tunnel manual tn2 source 1.0.0.1 destination 1.0.0.2
Command: config ip_tunnel manual tn2 source 1.0.0.1 destination 1.0.0.2

Success.

DGS-3450:admin# config ip_tunnel manual tn2 ipv6address 2001::1/64
Command: config ip_tunnel manual tn2 ipv6address 2001::1/64

Success.

DGS-3450:admin#
```

config ip_tunnel 6to4

Purpose	Used to configure an IPv6 6to4 tunnel.
Syntax	config ip_tunnel 6to4 <tunnel_name 12> {ipv6address <ipv6networkaddr> source <ipaddr >}(1)
Description	<p>The config ip_tunnel 6to4 command is used to configure an existing IPv6 tunnel as an IPv6 6to4 tunnel on the switch. If this tunnel has previously been configured in another mode, the tunnel's information will still exist in the database. However, whether the tunnel's former information is invalid or not will depend on the current mode. A maximum of one IPv6 6to4 tunnel can exist on the system.</p> <p>IPv6 6to4 tunnels are point-to-multipoint tunnels that can be used to connect isolated IPv6 sites. Each IPv6 site has at least one connection to a shared IPv4 network and this IPv4 network could be the global Internet or a corporate backbone. The key requirement is that each site has a globally unique IPv4 address, which is used to construct a 48-bit globally unique 6to4 IPv6 prefix (It starts with the prefix 2002::/16).</p>
Parameters	<p><i><tunnel_name 12></i> - IPv6 Tunnel interface name, maximum of 12 characters.</p> <p><i>ipv6address <ipv6networkaddr></i> - The IPv6 address assigned to this IPv6 tunnel interface. IPv6 processing would be enabled on this IPv6 tunnel interface when an IPv6 address is configured. The 32 bits following the initial 2002::/16 prefix correspond to an IPv4 address assigned to the tunnel source.</p> <p><i>source <ipaddr></i> - The source IPv4 address of this IPv6 tunnel interface. It is used as the source address for packets in this IPv6 tunnel. The tunnel destination IPv4 address is extracted from the remote tunnel endpoint's IPv6 6to4 address that starts with the prefix 2002::/16.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure an IPv6 6to4 tunnel (Tunnel name is "tn2", Tunnel source IPv4 address is 10.0.0.1, Tunnel IPv6 address is 2002:a00:1::1/64):

```
DGS-3450:admin# config ip_tunnel 6to4 tn2 source 10.0.0.1
Command: config ip_tunnel 6to4 tn2 source 10.0.0.1

Success.

DGS-3450:admin# config ip_tunnel 6to4 tn2 ipv6address 2002:a00:1::1/64
Command: config ip_tunnel 6to4 tn2 ipv6address 2002:a00:1::1/64

Success.

DGS-3450:admin#
```


config ip_tunnel isatap

Purpose	Used to configure an IPv6 ISATAP tunnel.
Syntax	config ip_tunnel isatap <tunnel_name 12> {ipv6address <ipv6networkaddr> source <ipaddr>}(1)
Description	The config ip_tunnel isatap command is used to configure an existing IPv6 tunnel as an IPv6 ISATAP tunnel on the switch. If this tunnel has previously been configured in another mode, the tunnel's information will still exist in the database. However, whether the tunnel's former information is invalid or not will depend on the current mode. IPv6 ISATAP tunnels are point-to-multipoint tunnels that can be used to connect systems within a site. An IPv6 ISATAP address is a well-defined unicast address that includes a 64-bit unicast IPv6 prefix (it can be link local or global prefixes), a 32-bit value 0000:5EFE and a 32-bit tunnel source IPv4 address.
Parameters	<p><i><tunnel_name 12></i> - IPv6 Tunnel interface name, maximum of 12 characters.</p> <p><i>ipv6address <ipv6networkaddr></i> - The IPv6 address assigned to this IPv6 tunnel interface. IPv6 processing would be enabled on this IPv6 tunnel interface when an IPv6 address is configured. The last 32 bits of the IPv6 ISATAP address correspond to an IPv4 address assigned to the tunnel source.</p> <p><i>source <ipaddr></i> - The source IPv4 address of this IPv6 tunnel interface. It is used as the source address for packets in this IPv6 tunnel. The tunnel destination IPv4 address is extracted from the last 32 bits of the remote tunnel endpoint's IPv6 ISATAP address.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure an IPv6 ISATAP tunnel (Tunnel name is "tn2", Tunnel source IPv4 address is 10.0.0.1, Tunnel IPv6 address is 2001::5efe:a00:1/64):

```
DGS-3450:admin# config ip_tunnel isatap tn2 source 10.0.0.1
Command: config ip_tunnel isatap tn2 source 10.0.0.1

Success.

DGS-3450:admin# config ip_tunnel isatap tn2 ipv6address 2001::5efe:a00:1/64
Command: config ip_tunnel isatap tn2 ipv6address 2001::5efe:a00:1/64

Success.

DGS-3450:admin#
```

show ip_tunnel

Purpose	Used to show one or all IPv6 tunnel interfaces' information.
Syntax	show ip_tunnel {<tunnel_name 12>}
Description	The show ip_tunnel command is used to show one or all IPv6 tunnel interfaces' information.
Parameters	<p><i><tunnel_name 12></i> - IPv6 Tunnel interface name, maximum of 12 characters.</p> <p>If no tunnel is specified, all tunnels on the Switch will be displayed.</p>
Restrictions	None.

Example usage:

To show an IPv6 tunnel interface's information (Tunnel name is "tn2"):

```
DGS-3450:admin# show ip_tunnel tn2
Command: show ip_tunnel tn2

Tunnel Interface      : tn2
Interface Admin State : Enabled
Tunnel Mode           : Manual
IPv6 Address          : 2000::1/64
Tunnel Source         : 1.0.0.1
Tunnel Destination    : 1.0.0.2

Success.

DGS-3450:admin#
```

enable ip_tunnel

Purpose	Used to enable an IPv6 tunnel interface or all IPv6 tunnel interfaces.
Syntax	enable ip_tunnel {<tunnel_name 12>}
Description	The enable ip_tunnel command is used to enable an IPv6 tunnel or all IPv6 tunnels on the switch.
Parameters	<tunnel_name 12> - IPv6 Tunnel interface name, maximum of 12 characters. If no tunnel is specified, all tunnels on the Switch will be enabled.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable an IPv6 tunnel interface (Tunnel name is "tn2").:

```
DGS-3450:admin# enable ipif tunnel tn2
Command: enable ipif tunnel tn2

Success.

DGS-3450:admin#
```

disable ip_tunnel

Purpose	Used to disable an IPv6 tunnel interface or all tunnel interfaces.
Syntax	disable ip_tunnel {<tunnel_name 12>}
Description	The disable ip_tunnel command is used to disable an IPv6 tunnel or all IPv6 tunnels on the switch.
Parameters	<tunnel_name 12> - IPv6 Tunnel interface name, maximum of 12 characters. If no tunnel is specified, all tunnels on the Switch will be disabled.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable an IPv6 tunnel interface (Tunnel name is "tn2").:

```
DGS-3450:admin# disable ip_tunnel tn2
```

```
Command: disable ip_tunnel tn2
```

```
Success.
```

```
DGS-3450:admin#
```

JAPANESE WEB-BASED ACCESS CONTROL (JWAC) COMMANDS

The Japanese Web-based Access Control (JWAC) commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameters
enable jwac	
disable jwac	
enable jwac redirect	
disable jwac redirect	
enable jwac forcible_logout	
disable jwac forcible_logout	
enable jwac udp_filtering	
disable jwac udp_filtering	
enable jwac quarantine_server_monitor	
disable jwac quarantine_server_monitor	
config jwac quarantine_server_error_timeout	<sec 5-300>
config jwac redirect	{destination [quarantine_server jwac_login_page] delay_time <sec 0-10>} (1)
config jwac virtual_ip	<ipaddr> {url [<string 128> clear]}
config jwac quarantine_server_url	<string 128>
config jwac clear_quarantine_server_url	
config jwac update_server	[add delete] ipaddress <network_address> {[tcp_port < port_number 1-65535> udp_port < port_number 1-65535>]}
config jwac switch_http_port	<tcp_port_number 1-65535> {[http https]}
config jwac ports	[<portlist> all] {state [enable disable] max_authenticating_host <value 0-50> aging_time [infinite <min 1-1440>] idle_time [infinite <min 1-1440>] block_time [<sec 0-300>] auth_mode [host_based port_based]} (1)
config jwac radius_protocol	[local pap chap ms_chap ms_chapv2 eap_md5]
create jwac user	<username 15> {vlan <vlanid 1-4094>}
config jwac user	<username 15> {vlan <vlanid 1-4094>}
delete jwac	[user <username 15> all_users]
show jwac user	
clear jwac auth_state	[ports [all <portlist>] { authenticated authenticating blocked } mac_addr <macaddr>]
config jwac authorization attributes	{radius [enable disable] local [enable disable]} (1)
show jwac	
show jwac update_server	
show jwac auth_state ports	{<portlist>}
show jwac ports	{<portlist>}
config jwac authentication_page element	[japanese english] [default page_title <desc 128> login_window_title < desc 32> user_name_title < desc 16> password_title < desc 16> logout_window_title < desc 32> notification_line <value 1-5> <desc 128>]
show jwac authenticate_page	

Command	Parameters
config jwac authenticate_page	[japanese english]

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

enable jwac

Purpose	Used to enable JWAC function.
Syntax	enable jwac
Description	<p>The enable jwac command enables JWAC function.</p> <p>JWAC and WAC are mutual exclusive function. That is, they can not be enabled at the same time.</p> <p>Using the JWAC function, PC users need to pass two stages of authentication.</p> <p>The first stage is to do the authentication with the quarantine server and the second stage is the authentication with the switch. For the second stage, the authentication is similar to WAC, except that there is no port VLAN membership change by JWAC after a host passes authentication. The RADIUS server will share the server configuration defined by 802.1X command set.</p>
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable JWAC function:

<pre>DGS-3450:admin# enable jwac Command: enable jwac Success. DGS-3450:admin#</pre>
--

disable jwac

Purpose	Used to disable JWAC function.
Syntax	disable jwac
Description	The disable jwac command disables JWAC function; all authentication entries related to JWAC will be deleted.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable JWAC function:

<pre>DGS-3450:admin# disable jwac Command: disable jwac Success. DGS-3450:admin#</pre>
--

enable jwac redirect

Purpose	Used to enable JWAC redirect function.
Syntax	enable jwac redirect
Description	<p>When redirecting quarantine server is specified, the unauthenticated host will be redirected to quarantine server when it tries to access a random URL. When redirecting JWAC login page is specified, the unauthenticated host will be redirected to JWAC login page in the Switch to finish authentication.</p> <p>When redirect is enabled, all the web accesses are redirect to quarantine server or JWAC login page.</p> <p>When redirecting to quarantine server is specified, a quarantine server must be configured first before enabling JWAC globally.</p>
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable JWAC redirect function:

```
DGS-3450:admin# enable jwac redirect
Command: enable jwac redirect

Success.

DGS-3450:admin#
```

disable jwac redirect

Purpose	Used to disable JWAC redirect function.
Syntax	disable jwac redirect
Description	When redirect is disabled, all web accesses are denied except for accesses to quarantine server or JWAC login page.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable JWAC redirect function:

```
DGS-3450:admin# disable jwac redirect
Command: disable jwac redirect

Success.

DGS-3450:admin#
```

enable jwac forcible_logout

Purpose	Used to enable JWAC forcibly logout function.
Syntax	enable jwac forcible_logout
Description	When forcibly logout feature is enabled, a PING packet from an authenticated host to the JWAC Switch with TTL=1 will be regarded as a logout request, and the host will be moved

enable jwac forcible_logout

	back to unauthenticated state.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable JWAC forcibly logout function:

```
DGS-3450:admin# enable jwac forcible_logout
Command: enable jwac forcible_logout

Success.

DGS-3450:admin#
```

disable jwac forcible_logout

Purpose	Used to disable JWAC forcibly logout function.
Syntax	disable jwac forcible_logout
Description	When forcibly logout feature is disabled, even a PING packet from an authenticated host to the JWAC Switch with TTL=1 will be ignored, and the host is still in an authenticated state.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable JWAC forcibly logout function:

```
DGS-3450:admin# disable jwac forcible_logout
Command: disable jwac forcible_logout

Success.

DGS-3450:admin#
```

enable jwac udp_filtering

Purpose	Used to enable or disable JWAC UDP filtering function.
Syntax	enable jwac udp_filtering
Description	When UDP filtering feature is enabled, all UDP and ICMP packets except for DHCP and DNS packets from unauthenticated hosts will be dropped.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable JWAC UDP filtering function:


```
DGS-3450:admin# enable jwac udp_filtering
Command: enable jwac udp_filtering

Success.

DGS-3450:admin#
```

disable jwac udp_filtering

Purpose	Used to disable JWAC UDP filtering function.
Syntax	disable jwac udp_filtering
Description	When UDP filtering feature is disabled, all UDP and ICMP packets are permitted.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable JWAC UDP filtering function:

```
DGS-3450:admin# disable jwac udp_filtering
Command: disable jwac udp_filtering

Success.

DGS-3450:admin#
```

enable jwac quarantine_server_monitor

Purpose	Used to enable JWAC Quarantien Server monitor function.
Syntax	enable jwac quarantine_server_monitor
Description	When JWAC Quarantine Server monitor feature is enabled, the JWAC Switch will monitor the Quarantine Server to ensure the server is OK. If the Switch detects no Quarantine Server, it will redirect all unauthenticated HTTP accesses to JWAC Login Page forcibly if the redirect is enabled and the redirect destination is configured to be Quarantine Server.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable JWAC Quarantine Server monitor function:

```
DGS-3450:admin# enable jwac quarantine_server_monitor
Command: enable jwac quarantine_server_monitor

Success.

DGS-3450:admin#
```

disable jwac quarantine_server_monitor

Purpose	Used to disable JWAC Quarantien Server monitor function.
---------	--

disable jwac quarantine_server_monitor

Syntax	disable jwac quarantine_server_monitor
Description	Disable JWAC Quarantine Server function enabled previously.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable Quarantine Server monitor function:

```
DGS-3450:admin# disable jwac quarantine_server_monitor
Command: disable jwac quarantine_server_monitor

Success.

DGS-3450:admin#
```

config jwac quarantine_server_error_timeout

Purpose	Used to set Quarantine Server error timeout.
Syntax	config jwac quarantine_server_error_timeout <sec 5-300>
Description	When Quarantine Server monitor is enabled, the JWAC Switch will periodically check if the Quarantine works OK. If the Switch does not receive any response from Quarantine Server during the configured error timeout, the Switch then regards it as working improperly.
Parameters	<sec 5-300> - To specify the error timeout interval.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To set Quarantine Server error timeout:

```
DGS-3450:admin# config jwac quarantine_server_error_timeout 60
Command: config jwac quarantine_server_error_timeout 60

Success.

DGS-3450:admin#
```

config jwac redirect

Purpose	Used to configure redirect destination and delay time before an unauthenticated host is redirect to Quarantine Server or JWAC login web page.
Syntax	config jwac redirect {destination [quarantine_server jwac_login_page] delay_time <sec 0-10>} (1)
Description	This command allows you to configure redirect destination and delay time before an unauthenticated host is redirected to Quarantine Server or the JWAC login web page. 0 means no delaying the redirect.
Parameters	<i>destination</i> - To specify the destination which the unauthenticated host will be redirected to. <i>delay_time</i> - To specify the time period after which the unauthenticated host will be redirected. Unit of this timer is second.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the redirect destination and delay time:

```
DGS-3450:admin# config jwac redirect destination jwac_login_page delay_time 5
Command: config jwac redirect_ destination jwac_login_page delay_time 5

Success.

DGS-3450:admin#
```

config jwac virtual_ip

Purpose	Used to configure JWAC virtual ipaddress to accept authentication requests from un-authenticated hosts.
Syntax	config jwac virtual_ip <ipaddr> {url [<string 128> clear]}
Description	The virtual IP of JWAC is used to accept authentication request from unauthenticated host. Only requests sent to this IP will get response correctly. This IP does not respond to ARP request or ICMP packet!
Parameters	<i><ipaddr></i> - To specify the IP address of the virtual IP. <i>url</i> - This parameter is used to set the URL of virtual IP.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure virtual IP address to accept authentication request from host:

```
DGS-3450:admin# config jwac virtual_ip 1.1.1.1 url www.kyoto.ac.jp
Command: config jwac virtual_ip 1.1.1.1 url www.kyoto.ac.jp

Success.

DGS-3450:admin#
```

config jwac quarantine_server_url

Purpose	Used to configure JWAC Quarantine Server URL.
Syntax	config jwac quarantine_server_url <string 128>
Description	This command allows you to configure URL of Quarantine Server. If the redirection is enabled and the redirection destination is Quarantine Server, when a HTTP request from unauthenticated host which is not headed to Quarantine Server reaches the Switch, the Switch will handle this HTTP packet and send back a message to the host to make it access Quarantine Server with the configured URL When the PC connected to the specified URL, the quarantine server will request the PC user to input the user name and password to authenticate. NOTE: If the quarantine server is linked to the JWAC enabled port on the switch, it must be added to the static FDB correctly before it can work properly.
Parameters	<i><string 128></i> - To specify the entire URL of authentication page on Quarantine Server
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure Quarantine Server URL:

```
DGS-3450:admin# config jwac quarantine_server_url http://10.90.90.88/authpage.html
Command: config jwac quarantine_server_url http://10.90.90.88/authpage.html

Success.

DGS-3450:admin#
```

config jwac clear_quarantine_server_url

Purpose	Used to clear Quarantine Server configuration.
Syntax	config jwac clear_quarantine_server_url
Description	This command will clear Quarantine Server configuration.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To clear Quarantine Server configuration:

```
DGS-3450:admin# config jwac clear_quarantine_server_url
Command: config jwac clear_quarantine_server_url

Success.

DGS-3450:admin#
```

config jwac update_server

Purpose	Used to configure the update server network that PC need to access in order to complete the JWAC authentication.
Syntax	config jwac update_server [add delete] ipaddress <network_address> {[tcp_port < port_number 1-65535> udp_port < port_number 1-65535>]}
Description	<p>The config jwac update server command allows you to add or delete server network address to which the traffic from unauthenticated client host will not be blocked by the JWAC Switch.</p> <p>Any servers (update.microsoft.com or some sites of the Anti-Virus software companies, which the ActiveX needs to access to accomplish the authentication before the client passes the authentication) should be added with its IP address or with the network address it resident. By adding the network address, an entry can serve multiple update servers on the same network.</p> <p>NOTE: If the update server is linked to the JWAC enabled port on the switch, it must be added to the static FDB before it can work properly.</p>
Parameters	<p><i>add</i> - To add an update server network. The total number of Update Servers is depending on project.</p> <p><i>delete</i> - To delete a update server network.</p> <p><i>ipaddress</i> - To specify the network address for the update server network. To set a specific IP address, please use the format x.x.x.x/32</p> <p>If TCP port or UDP port number is not specified, all TCP/UDP ports are accessible.</p> <p><i>tcp_port</i> - The accessible TCP port for the specified update server network.</p> <p><i>udp_port</i> - The accessible UDP port for the specified update server network.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the update server which the un-authenticated host need to access:

```
DGS-3450:admin# config jwac update_server add ipaddress 10.90.90.109/24
Command: config jwac update_server add ipaddress 10.90.90.109/24
Update Server 10.90.90.0/24 is added.

Success.

DGS-3450:admin#
```

config jwac switch_http_port

Purpose	Used to configure the HTTP port which the JWAC Switch listens to.
Syntax	config jwac switch_http_port < tcp_port_number 1-65535> {[http https]}
Description	<p>The config jwac switch_http_port command allows you to configure the TCP port number which the JWAC Switch listens to. This port number is used in the second stage of the authentication. PC user will connect the page on the switch to input the user name and password.</p> <p>If not specified, the default port number is 80.</p> <p>If no protocol specified, the protocol is HTTP.</p> <p>The HTTP cannot run at TCP port 443, and the HTTPS cannot run at TCP port 80.</p>
Parameters	<p><i><tcp_port_number 1-65535></i> - A TCP port which the JWAC Switch listens to and uses to finish the authenticating process.</p> <p><i>http</i> - To specify the JWAC runs HTTP protocol on this TCP port</p> <p><i>https</i> - To specify the JWAC runs HTTPS protocol on this TCP port</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the HTTP port which the Switch listens to:

```
DGS-3450:admin# config jwac switch_http_port 8888 http
Command: config jwac switch_http_port 8888 http

Success.

DGS-3450:admin#
```

config jwac ports

Purpose	Used to configure port's state of JWAC.
Syntax	config jwac ports [<portlist> all] {state [enable disable] max_authenticating_host <value 0-n> aging_time [infinite <min 1-1440>] idle_time [infinite <min 1-1440>] block_time [<sec 0-300>] auth_mode [host_based port_based]} (1)
Description	<p>The config jwac ports command allows you to configure port state of JWAC.</p> <p>The default value of max_authenticating_host is n (The max allowed value, 'n' is project dependent).</p> <p>The default value of aging_time is 1440 minutes.</p> <p>The default value of idle_time is infinite.</p> <p>The default value of block_time is 60 seconds.</p>

config jwac ports

Parameters	<p><i><portlist></i> - A port range to set their JWAC state.</p> <p><i>all</i> - All the Switch ports' JWAC state is to be configured.</p> <p><i>state</i> - To specify the port state of JWAC</p> <p><i>max_authenticating_host</i> - Max number of host process authentication on each port at the same time</p> <p><i>aging_time</i> - A time period during which an authenticated host will keep in authenticated state. "infinite" indicates never to age out the authenticated host on the port</p> <p><i>idle_time</i> - If there is no traffic during <i>idle_time</i>, the host will be moved back to unauthenticated state "infinite" indicates never to check the idle state of the authenticated host on the port.</p> <p><i>block_time</i> - If a host fails to pass the authentication, it will be blocked for a period specified by <i>block_time</i>.</p> <p><i>auth_mode</i> - The port authentication mode can be either host based or port based.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure state and other parameters of the ports:

```
DGS-3450:admin# config jwac ports 1-9 state enable
Command: config jwac ports 1-9 state enable
```

Success.

```
DGS-3450:admin#
```

config jwac radius_protocol

Purpose	Used to configure RADIUS protocol used by JWAC.
Syntax	config jwac radius_protocol [local pap chap ms_chap ms_chapv2 eap_md5]
Description	<p>The config jwac radius_protocol command allows you to specify the RADIUS protocol used by JWAC to complete RADIUS authentication.</p> <p>JWAC shares other RADIUS configuration with 802.1x, when using this command to set the RADIUS protocol, you must make sure the RADIUS server added by "config radius ..." command supports the protocol.</p>
Parameters	<p><i>local</i> - JWAC Switch uses local user DB to complete the authentication</p> <p><i>pap</i> - JWAC Switch uses PAP to communicate with RADIUS Server</p> <p><i>chap</i> - JWAC Switch uses CHAP to communicate with RADIUS Server</p> <p><i>ms_chap</i> - JWAC Switch uses MS-CHAP to communicate with RADIUS Server</p> <p><i>ms_chapv2</i> - JWAC Switch uses MS-CHAPv2 to communicate with RADIUS Server</p> <p><i>eap_md5</i> - JWAC Switch uses EAP MD5 to communicate with RADIUS Server</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure authentication protocol:

```
DGS-3450:admin# config jwac radius_protocol ms_chapv2
Command: config jwac radius_protocol ms_chapv2

Success.

DGS-3450:admin#
```

create jwac user

Purpose	Used to create JWAC user into local DB.
Syntax	create jwac user <username 15> {vlan <vlanid 1-4094>}
Description	The create jwac user command creates JWAC users into the local DB. And when “local” is chosen when configuring JWAC RADIUS protocol, the local DB will be used.
Parameters	<username 15> - The user name to be created <vlanid 1-4094> - Target VLAN ID for authenticated host which uses this user account to pass authentication
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create a local user:

```
DGS-3450:admin# create jwac user 112233
Command: create jwac user 112233

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

DGS-3450:admin#
```

config jwac user

Purpose	Used to update local user DB.
Syntax	config jwac user <username 15> {vlan <vlanid 1-4094>}
Description	The config jwac user command updates the local user DB. Only created user can be configured.
Parameters	<username 15> - The user name to be configured <vlanid 1-4094> - Target VLAN ID for authenticated host which uses this user account to pass authentication
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure a local user:

```
DGS-3450:admin# create jwac user juser_tom vlan 3
Command: create jwac user juser_tom vlan 3

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

DGS-3450:admin#
```

delete jwac user

Purpose	Used to delete JWAC user into local DB.
Syntax	delete jwac [user <username 15> all_users]
Description	The delete jwac user command deletes JWAC users from the local DB.
Parameters	<i>user</i> - To specify the user name to be deleted <i>all_user</i> - All user accounts in local DB will be deleted.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete a local user.

```
DGS-3450:admin# delete jwac user juser_tom
Command: delete jwac user juser_tom

Success.

DGS-3450:admin#
```

show jwac user

Purpose	Used to show JWAC user into local DB.
Syntax	show jwac user
Description	The show jwac user command displays JWAC users in the local DB.
Parameters	None.
Restrictions	None.

Example usage:

This example displays the JWAC users in the local database:

```
DGS-3450:admin# show jwac user
Command: show jwac user

Username      Password      VID
-----
juser_tom    1             3

Total Entries : 1

DGS-3450:admin#
```


clear jwac auth_state

Purpose	Used to clear the JWAC authentication entry.
Syntax	clear jwac auth_state [ports [all <portlist>] { authenticated authenticating blocked } mac_addr <macaddr>]
Description	The user can use this command to clear the authentication entry.
Parameters	<p><i>ports</i> - To specify the port range to delete host on them.</p> <p><i>authenticated</i> - To specify the state of host to delete.</p> <p><i>authenticating</i> - To specify the state of host to delete.</p> <p><i>blocked</i> - To specify the state of host to delete.</p> <p><i><macaddr></i> - To delete a specified host with this MAC.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete authentication entry:

```
DGS-3450:admin# clear jwac auth_state ports all blocked
Command: clear jwac auth_state ports all blocked

Success.

DGS-3450:admin#
```

config jwac authorization attributes

Purpose	The enable authorization command will enable acceptance of authorized configuration.
Syntax	config jwac authorization attributes {radius [enable disable] local [enable disable]} (1)
Description	<p>Used to enable or disable acceptance of authorized configuration.</p> <p>When the authorization is enabled for JWAC's RADIUS, the authorized data assigned by the RADIUS server will be accepted if the global authorization network is enabled.</p> <p>When the authorization is enabled for JWAC's local, the authorized data assigned by the local database will be accepted.</p>
Parameters	<p><i>radius</i> - If specified to enable, the authorized data assigned by the RADIUS server will be accepted if the global authorization network is enabled. The default state is enabled.</p> <p><i>local</i> - If specified to enable, the authorized data assigned by the local database will be accepted if the global authorization network is enabled. The default state is enabled.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

The following example will disable the configuration authorized from the local database:

```
DGS-3450:admin# config jwac authorization attributes local disable
Command: config jwac authorization attributes local disable

Success.

DGS-3450:admin#
```

show jwac

Purpose	Used to display the configuration of JWAC.
Syntax	show jwac
Description	The show jwac command allows you to show all the configuration of JWAC.
Parameters	None.
Restrictions	None.

Example usage:

To display global configuration of JWAC:

```
DGS-3450:admin# show jwac
Command: show jwac

State                : Enabled
Enabled Ports       : 1:1,1:11,1:23,1:25,1:35
Virtual IP/URL      : 1.1.1.1/www.kyoto.ac.jp
Switch HTTP Port    : 21212 (HTTP)
UDP Filtering       : Enabled
Forcible Logout     : Enabled
Redirect State      : Enabled
Redirect Delay Time : 3 Seconds
Redirect Destination: Quarantine Server
Quarantine Server   : http://172.18.212.147/pcinventory
Q-Server Monitor    : Enabled (Running)
Q-Server Error Timeout : 5 Seconds
RADIUS Auth-Protocol : PAP
RADIUS Authorization : Enabled
Local Authorization : Enabled

DGS-3450:admin#
```

show jwac update_server

Purpose	Used to display the configuration of JWAC update server.
Syntax	show jwac update_server
Description	This command displays the configured update server's network and their accessible ports. The function will use system's common resource, thus some entries may not active if the resource is not sufficient when JWAC is enabled.
Parameters	None.
Restrictions	None.

Example usage:

To show update server:

```
DGS-3450:admin# show jwac update_server
```

```
Command: show jwac update_server
```

Index	IP	TCP/UDP	Port	State
1	10.0.0.0/8	-	-	Inactive
2	10.1.1.1/32	UDP	90	Inactive
3	10.3.3.3/32	TCP	80	Inactive
4	10.3.3.4/32	-	-	Inactive
5	10.3.3.5/32	-	-	Inactive
6	10.3.3.6/32	-	-	Inactive
7	10.3.3.7/32	-	-	Inactive
8	10.3.3.9/32	-	-	Inactive
9	10.3.3.10/32	-	-	Inactive
10	100.100.100.100/32	TCP	9080	Inactive

```
DGS-3450:admin#
```

show jwac auth_state

Purpose	Used to display information of JWAC client host.
Syntax	show jwac auth_state ports {<portlist>}
Description	The show jwac auth_state command allows you to show the information of JWAC client host.
Parameters	<i>ports</i> - A port range to show the information of client host. If no port is specified, all ports' JWAC authentication state will be displayed.
Restrictions	None.

Example usage:

Supposed that port 1 is in host-based mode:

- MAC 00-00-00-00-00-01 is authenticated without VLAN assigned (may be the specified target VLAN does not exist or target VLAN has not been specified at all), the ID of RX VLAN will be displayed (RX VLAN ID is 4004 in this example).
- MAC 00-00-00-00-00-02 is authenticated with target VLAN assigned, the ID of target VLAN will be displayed (target VLAN ID is 1234 in this example)
- MAC 00-00-00-00-00-03 failed to pass authentication, the VID field will be shown as "-" indicating that packets with SA 00-00-00-00-00-03 will be dropped no matter which VLAN these packets are from.
- MAC 00-00-00-00-00-04 attempts to start authentication, the VID field will be shown as "-" until authentication completed.

Supposed that port 2 is in port-based mode:

- MAC 00-00-00-00-00-10 is the MAC which made port 2 pass authentication, MAC address is followed by "(P)" indicating that this authentication is from a port in port-based mode.

Supposed that port 3 is in port-based mode:

- MAC 00-00-00-00-00-20 attempts to start authentication, MAC address is followed by "(P)" to indicate the port-based mode authentication.
- MAC 00-00-00-00-00-21 failed to pass authentication, MAC address is followed by "(P)" to indicate the port-based mode authentication.

NOTE: In port-based mode, the VLAN ID field is displayed in the same way as host-based mode.

```
DGS-3450:admin# show jwac auth_state ports 1-2
```

```
Command: show jwac auth_state ports 1-2
```

```
Pri - Priority. State - A:Authenticated, B:Blocked, -:Authenticating
```

```
Time - Aging Time/Idle Time for authenticated entries.
```

Port	MAC Address	State	VID	Pri	Time	IP	User Name
1	00-00-00-00-00-01	A	4004	3	-/40	192.168.101.239	juser_tom
1	00-00-00-00-00-02	A	1234	-	-/50	172.18.61.242	name_of_15chars
1	00-00-00-00-00-03	B	-	-	60	172.18.61.242	Jack
1	00-00-00-00-00-04	-	-	-	10	-	-
2	00-00-00-00-00-10(P)	A	1234	2	1440/20	10.10.10.90	Logan
3	00-00-00-00-00-20(P)	-	-	-	20	10.10.10.131	-
3	00-00-00-00-00-21(P)	B	-	-	200	-	Victor
Total Authenticating Hosts				: 2			
Total Authenticated Hosts				: 3			
Total Blocked Hosts				: 2			

DGS-3450:admin#

show jwac ports

Purpose	Used to display port configuration of JWAC.
Syntax	show jwac ports {<portlist>}
Description	The show jwac port command allows you to display port configuration of JWAC.
Parameters	<i>all</i> - To show all ports' configuration of JWAC <portlist> - To specify a port range to show the configuration of JWAC If no port is specified, the configuration for all ports will be displayed.
Restrictions	None.

Example usage:

To display port configuration:

```
DGS-3450:admin# show jwac ports 1-4
```

```
Command: show jwac ports 1-4
```

Port	State	Aging Time (min)	Idle Time (min)	Block Time (sec)	Auth Mode	Max Hosts
1	Enabled	Infinite	20	10	Port-based	10
2	Disabled	60	10	2	Port-based	10
3	Enabled	1440	Infinite	2	Host-based	50
4	Enabled	600	30	5	Host-based	50

```
DGS-3450:admin#
```

config jwac authentication_page element

Purpose	Used to customize the authenticate page.
Syntax	config jwac authentication_page element [japanese english] [default page_title <desc 128> login_window_title < desc 32> user_name_title < desc 16> password_title < desc 16> logout_window_title < desc 32> notification_line <value 1-5> <desc 128>]
Description	This command let administrator customize the JWAC authenticate page.

config jwac authentication_page element

Parameters	<p><i>japanese</i> - Change to Japanese page.</p> <p><i>english</i> - Change to English page.</p> <p><i>default</i> - Reset the page element to default.</p> <p><i>page_title</i> - The title of the authenticate page.</p> <p><i>login_window_title</i> - The login window title of the authenticate page</p> <p><i>user_name_title</i> - The user name title of the authenticate page</p> <p><i>password_title</i> - The password title of the authenticate page</p> <p><i>logout_window_title</i> - The logout window title mapping of the authenticate page</p> <p><i>notification_line</i> - This parameter is used to set the notification information by line in authentication web pages.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To customize the authenticate page:

```
DGS-3450:admin# config jwac page_element japanese page_title "ディーリンクジャパン株式会社"
"
Command: config jwac page_element japanese page_title "ディーリンクジャパン株式会社"

Success.

DGS-3450:admin#
```

show jwac authenticate_page

Purpose	Used to show the element mapping of the customized authenticate page.
Syntax	show jwac authenticate_page
Description	Used to show the element mapping of the customized authenticate page.
Parameters	None.
Restrictions	None.

Example usage:

The following example displays the default authentication page:

```
DGS-3450:admin# show jwac authenticate_page
```

```
Command: show jwac authenticate_page
```

```
Current Page :English Version
```

English Page Element

```
-----
Page Title           : Alpha Networks Inc.
Login Window Title   : Authentication Login
User Name Title      : User Name
Password Title       : Password
Logout Window Title  : Logout
Notification         :
Copyright @ 2010 D-Link All Rights Reserved
Site: http://support.dlink.com
```

Japanese Page Element

```
-----
Page Title           :
Login Window Title   : 社内 LAN 認証ログイン
User Name Title      : ユーザ ID
Password Title       : パスワード
Logout Window Title  : 社内 LAN 認証ログアウト
Notification         :
Copyright @ 2010 ディーリンクジャパン株式会社
    サイト (http://www.dlink-jp.com)
```

```
DGS-3450:admin#
```

config jwac authenticate_page

Purpose	Used to choose authenticate page language.
Syntax	config jwac authenticate_page [japanese english]
Description	This let administrator decide which authenticated page need to be used.
Parameters	<i>japanese</i> - Choose the Japanese page <i>english</i> - Choose the English page. This is the default page.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To choose authenticate page language:

```
DGS-3450:admin# config jwac authenticate_page japanese
```

```
Command: config jwac authenticate_page japanese
```

```
Success.
```

```
DGS-3450:admin#
```

JUMBO FRAME COMMANDS

Certain switches can support jumbo frames (frames larger than the Ethernet frame size of 1536 bytes). To transmit frames of up to 9K (and 9216 bytes tagged), the user can increase the maximum transmission unit (MTU) size from the default of 1536 by enabling the Jumbo Frame command.

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

Command	Parameters
enable jumbo_frame	
disable jumbo_frame	
show jumbo_frame	

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

enable jumbo_frame

Purpose	Used to enable the jumbo frame function on the Switch.
Syntax	enable jumbo_frame
Description	This command will allow ethernet frames larger than 1536 bytes to be processed by the Switch. The maximum size of the jumbo frame may not exceed 9216 bytes tagged.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable the jumbo frame function on the Switch:

```
DGS-3450:admin# enable jumbo_frame
Command: enable jumbo_frame

Success.

DGS-3450:admin#
```

disable jumbo_frame

Purpose	Used to disable the jumbo frame function on the Switch.
Syntax	disable jumbo_frame
Description	This command will disable the jumbo frame function on the Switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable the jumbo frame function on the Switch:

```
DGS-3450:admin# disable jumbo_frame
Command: disable jumbo_frame

Success.

DGS-3450:admin#
```

show jumbo_frame

Purpose	Used to show the status of the jumbo frame function on the Switch.
Syntax	show jumbo_frame
Description	This command will show the status of the jumbo frame function on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To show the jumbo frame status currently configured on the Switch:

```
DGS-3450:admin# show jumbo_frame
Command: show jumbo_frame

Jumbo frame state: disabled
Maximum frame size: 1536 bytes

DGS-3450:admin#
```


LIMITED IP MULTICAST ADDRESS

The Limited IP Multicast command allows the administrator to permit or deny access to a port or range of ports by specifying a range of multicast addresses. The Limited IP Multicast Commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameters
config limited multicast address	<portlist> {from <multicast_ipaddr> to <multicast_ipaddr> access [permit deny] state [enable disable]}
delete limited multicast address	[all <portlist>]
show limited multicast address	{<portlist>}

Each command is listed in detail in the following sections.

config limited multicast address

Purpose	Used to configure limited IP multicast address range.
Syntax	config limited multicast address <portlist> {from <multicast_ipaddr> to <multicast_ipaddr> access [permit deny] state [enable disable]}
Description	The config limited multicast address command allows the user to configure the multicast address range, access level, and state.
Parameters	<p><i><portlist></i> – A port or range of ports to config the limited multicast address. The beginning and end of the port list range are separated by a dash. Non-contiguous portlist entries are separated by a comma. (ex:1-3, 7-9)</p> <p><i>from</i> – Enter the lowest multicast IP address of the range.</p> <p><i>to</i> – Enter the highest multicast IP address of the range.</p> <p><i>access</i> – Use the access field to either <i>permit</i> or <i>deny</i> to limit or grant access to a specified range of Multicast addresses on a particular port or range of ports.</p> <p><i>state</i> – This parameter allows the user to <i>enable</i> or <i>disable</i> the limited multicast address range on a specific port or range of ports.</p>
Restrictions	Only Administrator and Operator-level users can issue this command. This command is used as a backwards compatible command for legacy devices and firmware.

Example usage:

To configure the limited multicast address on ports 1 to 3:

```
DGS-3450:admin# config limited multicast address 1-3 from 224.1.1.1 to 224.1.1.2 access permit state enable
Command: config limited multicast address 1-3 from 224.1.1.1 to 224.1.1.2 access permit state enable

Success.

DGS-3450:admin#
```

delete limited multicast address

Purpose	Used to delete Limited IP multicast address range.
Syntax	delete limited multicast address [all <portlist>]
Description	The delete limited multicast address command allows the user to delete all multicast address ranges or a selected range based on what port or ports the range has been assigned to.
Parameters	<i>all</i> – Allows the user to delete all limited multicast addresses that have been configured on the Switch. <i><portlist></i> – Allows the user to delete only those multicast address ranges that have been assigned to a particular port or range of ports. The beginning and end of the port list range are separated by a dash. Non-contiguous portlist entries are separated by a comma. (ex: 1-3,7-9)
Restrictions	Only Administrator and Operator-level users can issue this command. This command is used as a backwards compatible command for legacy devices.

Example usage:

To delete the limited multicast address on ports 1 to 3:

```
DGS-3450:admin# delete limited multicast address 1-3
Command: delete limited multicast address 1-3

Success.

DGS-3450:admin#
```

show limited multicast address

Purpose	Used to show per-port limited IP multicast address range.
Syntax	show limited multicast address {<portlist>}
Description	The show limited multicast address command allows users to show multicast address range by ports.
Parameters	<i><portlist></i> – A port or range of ports on which the limited multicast address range to be shown has been assigned. The beginning and end of the port list range are separated by a dash. Non-contiguous portlist entries are separated by a comma. (ex: 1-3,7-9)
Restrictions	None. This command is used as a backwards compatible command for legacy devices.

Example usage:

To show the limited multicast address on ports 1 to 2:

```
DGS-3450:admin# show limited multicast address 1-2
```

```
Command: show limited multicast address 1-2
```

Port	From	To	Access	Status
1:1	0.0.0.0	0.0.0.0		disable
1:2	0.0.0.0	0.0.0.0		disable

```
DGS-3450:admin#
```

LINK AGGREGATION COMMANDS

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

Link aggregation, also known as trunking, is a method of grouping physical link segments of the same media type and speed, and treating them as if they were part of a single, logical link segment. In general, link aggregation provides two important benefits: increased performance and increased resiliency.

Command	Parameters
create link_aggregation group_id	<value 1-32> {type [lacp static]}
delete link_aggregation group_id	<value 1-32>
config link_aggregation group_id	<value 1-32> {master_port <port> ports <portlist> state [enable disable]}
config link_aggregation algorithm	[mac_source mac_destination mac_source_dest ip_source ip_destination ip_source_dest]
show link_aggregation	{group_id <value 1-32> algorithm}
config lacp_port	<portlist> mode [active passive]
show lacp_port	{<portlist>}

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

create link_aggregation

Purpose	Used to create a link aggregation group on the Switch.
Syntax	create link_aggregation group_id <value 1-32> {type [lacp static]}
Description	This command will create a link aggregation group with a unique identifier.
Parameters	<p><value> – Specifies the group ID. The Switch allows up to 32 link aggregation groups to be configured. The group number identifies each of the groups.</p> <p><i>type</i> – Specify the type of link aggregation used for the group. If the type is not specified the default type is <i>static</i>.</p> <ul style="list-style-type: none"> • <i>lacp</i> – 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. • <i>static</i> – 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.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create a link aggregation group:

```
DGS-3450:admin# create link_aggregation group_id 1
Command: create link_aggregation group_id 1

Success.

DGS-3450:admin#
```

delete link_aggregation group_id

Purpose	Used to delete a previously created link aggregation group.
Syntax	delete link_aggregation group_id <value 1-32>
Description	This command is used to delete a previously configured link aggregation group.
Parameters	<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.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete link aggregation group:

```
DGS-3450:admin# delete link_aggregation group_id 6
Command: delete link_aggregation group_id 6

Success.

DGS-3450:admin#
```

config link_aggregation

Purpose	Used to configure a previously created link aggregation group.
Syntax	config link_aggregation group_id <value 1-32> {master_port <port> ports <portlist> state [enable disable]}
Description	This command allows users to configure a link aggregation group that was created with the create link_aggregation command above.
Parameters	<p><i>group_id <value 32></i> – Specifies the group ID. The Switch allows up to 32 link aggregation groups to be configured. The group number identifies each of the groups.</p> <p><i>master_port <port></i> – Master port ID. Specifies which port (by port number) of the link aggregation group will be the master port. All of the ports in a link aggregation group will share the port configuration with the master port.</p> <p><i>ports <portlist></i> – Specifies a port or range of ports that will belong to the link aggregation group including the master port. The beginning and end of the port list range are separated by a dash. Non-contiguous portlist entries are separated by a comma. (ex: 1-3,7-9)</p> <p><i>state [enable disable]</i> – Allows users to enable or disable the specified link aggregation group.</p>
Restrictions	Only Administrator and Operator-level users can issue this command. Link aggregation groups may not overlap.

Example usage:

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

```
DGS-3450:admin# config link_aggregation group_id 1 master_port 1:5 ports 1:5-1:7,9
Command: config link_aggregation group_id 1 master_port 1:5 ports 1:5-1:7,1:9
Success.

DGS-3450:admin#
```

config link_aggregation algorithm

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

Example usage:

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

```
DGS-3450:admin# config link_aggregation algorithm mac_source_dest
Command: config link_aggregation algorithm mac_source_dest

Success.

DGS-3450:admin#
```

show link_aggregation

Purpose	Used to display the current link aggregation configuration on the Switch.
Syntax	show link_aggregation {group_id <value 1-32> algorithm}
Description	This command will display the current link aggregation configuration of the Switch.
Parameters	<p><i><value 1-32></i> – Specifies the group ID. The Switch allows up to 32 link aggregation groups to be configured. The group number identifies each of the groups.</p> <p><i>algorithm</i> – Allows you to specify the display of link aggregation by the algorithm in use by that group.</p>
Restrictions	None.

Example usage:

To display Link Aggregation configuration:

```
DGS-3450:admin# show link_aggregation
Command: show link_aggregation

Link Aggregation Algorithm = IP-source
Group ID      : 1
Type         : TRUNK
Master Port  : 1:5
Member Port  : 1:5-1:7,1:9
Active Port  :
Status      : Disabled
Flooding Port:

Total Entries : 1
DGS-3450:admin#
```

config lacp_ports

Purpose	Used to configure settings for LACP compliant ports.
Syntax	config lacp_ports <portlist> mode [active passive]
Description	This command is used to configure ports that have been previously designated as LACP ports (see create link_aggregation).
Parameters	<p><i><portlist></i> – Specifies a port or range of ports to be configured. The beginning and end of the port list range are separated by a dash. Non-contiguous portlist entries are separated by a comma. (ex: 1-3,7-9)</p> <p><i>mode</i> – Select the mode to determine if LACP ports will process LACP control frames.</p> <ul style="list-style-type: none"> <i>active</i> – Active LACP ports are capable of processing and sending LACP control frames. This allows LACP compliant devices to negotiate the aggregated link so the group may be changed dynamically as needs require. In order to utilize the ability to change an aggregated port group, that is, to add or subtract ports from the group, at least one of the participating devices must designate LACP ports as active. Both devices must support LACP. <i>passive</i> – LACP ports that are designated as passive cannot process LACP control frames. In order to allow the linked port group to negotiate adjustments and make changes dynamically, at one end of the connection must have “active” LACP ports (see above).
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure LACP port mode settings:

```
DGS-3450:admin# config lacp_port 1:1-1:12 mode active
Command: config lacp_port 1:1-1:12 mode active

Success.

DGS-3450:admin#
```

show lacp_port

Purpose	Used to display current LACP port mode settings.
---------	--

show lacp_port

Syntax	show lacp_port {<portlist>}
Description	This command will display the LACP mode settings as they are currently configured.
Parameters	<i><portlist></i> – Specifies a port or range of ports to be configured. The beginning and end of the port list range are separated by a dash. Non-contiguous portlist entries are separated by a comma. (ex: 1-3,7-9) If no parameter is specified, the system will display the current LACP status for all ports.
Restrictions	None.

Example usage:

To display LACP port mode settings:

```
DGS-3450:admin# show lacp_port 1-10
Command: show lacp_port 1-10
```

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

```
DGS-3450:admin#
```


LINK LAYER DISCOVERY PROTOCOL (LLDP) COMMANDS

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

The Link Layer Discovery Protocol (LLDP) specified in this standard allows stations attached to an 802 LAN to advertise to other stations attached to the same 802 LAN the connectivity and management information necessary to identify to those management entities the station's point of attachment to the 802 LAN. The information distributed via this protocol is stored by its recipients in a standard management information base (MIB), making it possible for the information to be accessed by a network management system (NMS) using a management protocol such as the Simple Network Management Protocol (SNMP)

Command	Parameters
enable lldp	
disable lldp	
config lldp	message_tx_interval <sec 5-32768>
config lldp	message_tx_hold_multiplier <int 2-10>
config lldp	tx_delay <sec 1-8192>
config lldp	reinit_delay <sec 1-10>
config lldp	notification_interval <sec 5-3400>
config lldp ports	[<portlist> all] notification [enable disable]
config lldp ports	[<portlist> all] admin_status [tx_only rx_only tx_and_rx disable]
config lldp ports	[<portlist> all] mgt_addr [ipv4 <ipaddr> ipv6 <ipv6addr>] [enable disable]
config lldp ports	[<portlist> all] basic_tlvs [all {port_description system_name system_description system_capabilities}] [enable disable]
config lldp ports	[<portlist> all] dot1_tlv_pvid [enable disable]
config lldp ports	[<portlist> all] dot1_tlv_protocol_vid [vlan [all <vlan_name 32>] vlanid <vidlist>] [enable disable]
config lldp ports	[<portlist> all] dot1_tlv_vlan_name [vlan [all <vlan_name 32>] vlanid <vidlist>] [enable disable]
config lldp ports	[<portlist> all] dot1_tlv_protocol_identity[all { eapol lacp gvrp stp}] [enable disable]
config lldp ports	[<portlist> all] dot3_tlvs [all {mac_phy_configuration_status link_aggregation maximum_frame_size}] [enable disable]
config lldp	forward_message [enable disable]
show lldp	
show lldp mgt_addr	{[ipv4 <ipaddr> ipv6 <ipv6addr>]}
show lldp ports	{<portlist>}
show lldp local_ports	{<portlist>} {mode [brief normal detailed]}
show lldp remote_ports	{<portlist>} {mode [brief normal detailed]}
show lldp statistics	
show lldp statistics ports	{<portlist>}

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

enable lldp

Purpose	Used to enable LLDP operation on the Switch.
Syntax	enable lldp
Description	This is a global control for the LLDP function. When this function is enabled, the switch can start to transmit LLDP packets and receive and process the LLDP packets. The specific function of each port will depend on the per port LLDP setting. For the advertisement of LLDP packets, the switch announces the information to its neighbor through ports. For the receiving of LLDP packets, the switch will learn the information from the LLDP packets advertised from the neighbor in the Neighbor's table. The default state for LLDP is disabled.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable LLDP:

```
DGS-3450:admin# enable lldp
Command: enable lldp

Success.

DGS-3450:admin#
```

disable lldp

Purpose	Used to disable LLDP operation on the Switch.
Syntax	disable lldp
Description	This command will stop the sending and receiving of LLDP advertisement packets on the Switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable LLDP:

```
DGS-3450:admin# disable lldp
Command: disable lldp

Success.

DGS-3450:admin#
```

config lldp message_tx_interval

Purpose	Used to change the packet transmission interval.
Syntax	config lldp message_tx_interval <sec 5 – 32768>
Description	This interval controls how often active ports retransmit advertisements to their neighbors.
Parameters	<i>message_tx_interval</i> – Changes the interval between consecutive transmissions of LLDP advertisements on any given port. The range is from 5 seconds to 32768 seconds. The default setting is 30 seconds.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To show the packet transmission interval:

```
DGS-3450:admin# config lldp message_tx_interval 30
Command: config lldp message_tx_interval 30

Success.

DGS-3450:admin#
```

config lldp message_tx_hold_multiplier

Purpose	Used to configure the message hold multiplier.
Syntax	config lldp message_tx_hold_multiplier <int 2-10 >
Description	This parameter is a multiplier on the msgTxInterval that is used to compute the TTL value of txTTL in an LLDPDU. TheTTL will be carried in the LLDPDU packet. The lifetime will be the minimum of 65535 and (message_tx_interval * message_tx_hold_multiplier). At the partner switch, when the time-to-live for a given advertisement expires, the advertised data is deleted from the neighbor switch's MIB
Parameters	<i>message_hold_multiplier</i> – The range is from 2 to 10. The default setting is 4.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To change the multiplier value:

```
DGS-3450:admin# config lldp message_tx_hold_multiplier 3
Command: config lldp message_tx_hold_multiplier 3

Success.

DGS-3450:admin#
```

config lldp tx_delay

Purpose	Used to change the minimum time (delay-interval) LLDP ports will delay in advertising successive LLDP advertisements due to a change in LLDP MIB content. The tx_delay defines the minimum interval between sending of LLDP messages due to constantly change of MIB content.
Syntax	config lldp tx_delay < sec 1–8192 >
Description	The LLDP message_tx_interval (transmit interval) must be greater than or equal to (4 x tx_delay interval).
Parameters	<i>tx_delay</i> – The range is from 1 second to 8192 seconds. The default setting is 2 seconds. NOTE: txDelay should be less than or equal to 0.25 * msgTxInterval
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the delay interval:

```
DGS-3450:admin# config lldp tx_delay 8
Command: config lldp tx_delay 8

Success.

DGS-3450:admin#
```

config lldp reinit_delay

Purpose	Change the minimum time of the reinitialization delay interval.
Syntax	config lldp reinit_delay <sec 1 - 10>
Description	A re-enabled LLDP port will wait for reinit_delay after last disable command before reinitializing.
Parameters	<i>reinit_delay</i> – The range is from 1 second to 10 seconds. The default setting is 2 seconds.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To changes the re-initialization delay interval to five seconds:

```
DGS-3450:admin# config lldp reinit_delay 5
Command: config lldp reinit_delay 5

Success.

DGS-3450:admin#
```

config lldp notification _interval

Purpose	Used to configure the timer of the notification interval for sending notification to configured SNMP trap receiver(s).
Syntax	config lldp notification _interval <sec 5 – 3400 >
Description	Globally change the interval between successive LLDP change notifications generated by the switch.
Parameters	<i>notification_interval</i> – The range is from 5 seconds to 3400 seconds. The default setting is 5 seconds.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To change the notification interval to 10 seconds:

```
DGS-3450:admin# config lldp notification_interval 10
Command: config lldp notification_interval 10

Success.

DGS-3450:admin#
```

config lldp ports notification

Purpose	Used to configure each port for sending notification to configured SNMP trap receiver(s).
Syntax	config lldp ports [<portlist> all] notification [enable disable]
Description	Enable or disable each port for sending changes notification to configured SNMP trap receiver(s) if an LLDP data change is detected in an advertisement received on the port from an LLDP neighbor. The definition of change includes new available information, information timeout, information update. And the changed type includes any data update /insert/remove.
Parameters	<i><portlist></i> – Use this parameter to define ports to be configured. <i>all</i> – Use this parameter to set all ports in the system. <i>notification</i> – Enables or disables the SNMP trap notification of LLDP data changes detected on advertisements received from neighbor devices. The default notification state is disabled.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To change the SNMP notification state of ports 1 to 5 to enable:

```
DGS-3450:admin# config lldp ports 1:1-1:5 notification enable
Command: config lldp ports 1:1-1:5 notification enable

Success.

DGS-3450:admin#
```

config lldp ports admin_status

Purpose	Used to configure per-port transmit and receive modes.
Syntax	config lldp ports [<portlist> all] admin_status [tx_only rx_only tx_and_rx disable]
Description	These options enable the user to control which ports participate in LLDP traffic and whether the participating ports allow LLDP traffic in only one direction or in both directions.
Parameters	<p><portlist> – Use this parameter to define ports to be configured.</p> <p>all – Use this parameter to set all ports in the system.</p> <p>admin_status – tx_only: Configure the specified port(s) to transmit LLDP packets, but block inbound LLDP packets from neighbor devices; rx_only: Configure the specified port(s) to receive LLDP packets from neighbors, but block outbound packets to neighbors; tx_and_rx: Configure the specified port(s) to both transmit and receive LLDP packets; disable: Disable LLDP packet transmit and receive on the specified port(s). The default per port state is tx_and_rx.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure ports 1 to 5 to transmit and receive:

```
DGS-3450:admin# config lldp ports 1:1-1:5 admin_status tx_and_rx
Command: config lldp ports 1:1-1:5 admin_status tx_and_rx

Success.

DGS-3450:admin#
```

config lldp ports mgt_addr

Purpose	Used to enable or disable port(s) specified for advertising indicated management address instance.
Syntax	config lldp ports [<portlist> all] mgt_addr [ipv4 <ipaddr> ipv6 <ipv6addr>] [enable disable]
Description	This command specifies whether the system's IP address needs to be advertised from the specified port. For layer 3 devices, each managed address can be individually specified. The management addresses that are added in the list will be advertised in the LLDP from the specified interface associated with each management address. The interface for that management address will be also advertised in the if-index form
Parameters	<p><portlist> – Use this parameter to define ports to be configured.</p> <p>all – Use this parameter to set all ports in the system.</p> <p>ipv4 – The IP address of IPv4.</p> <p>ipv6 – The IP address of IPv6.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable ports 1 to 2 to manage address entry:

```
DGS-3450:admin# config lldp ports 1:1-1:2 mgt_addr ipv4 192.168.254.10 enable
Command: config lldp ports 1:1-1:2 mgt_addr ipv4 192.168.254.10 enable

Success.

DGS-3450:admin#
```

config lldp ports basic_tlvs

Purpose	Used to configure an individual port or group of ports to exclude one or more optional TLV data types from outbound LLDP advertisements.
Syntax	config lldp ports [<portlist> all] basic_tlvs [all {port_description system_name system_description system_capabilities}] [enable disable]
Description	An active LLDP port on the switch always includes the mandatory data in its outbound advertisements. And there are four optional data that can be configured for an individual port or group of ports to exclude one or more of these data types from outbound LLDP advertisements. The mandatory data type include four basic types of information (end f LLDPDU TLV, chassis ID TLV, port ID TLV, and Time to Live TLV). The mandatory type can not be disabled. There are also four data types which can be optionally selected. They are <i>port_description</i> , <i>system_name</i> , <i>system_description</i> , and <i>system_capability</i> .
Parameters	<p><i><portlist></i> – Use this parameter to define ports to be configured.</p> <p><i>all</i> – Use this parameter to set all ports in the system.</p> <p><i>port_description</i> – This TLV optional data type indicates that LLDP agent should transmit 'Port Description TLV' on the port. The default state is disabled.</p> <p><i>system_name</i> – This TLV optional data type includes indicates that LLDP agent should transmit 'System Name TLV'. The default state is disabled.</p> <p><i>system_description</i> – This TLV optional data type includes indicates that LLDP agent should transmit 'System Description TLV'. The default state is disabled.</p> <p><i>system_capabilities</i> – This TLV optional data type includes indicates that LLDP agent should transmit 'System Capabilities TLV'. The system capability will indicate whether the device provides repeater, bridge, or router function, and whether the provided functions are currently enabled. The default state is disabled.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure exclude the system name TLV from the outbound LLDP advertisements for all ports:

```
DGS-3450:admin# config lldp ports all basic_tlvs system_name enable
Command: config lldp ports all basic_tlvs system_name enable

Success.

DGS-3450:admin#
```

config lldp dot1_tlv_pvid

Purpose	Used to configure an individual port or group of ports to exclude one or more of IEEE 802.1 organization port VLAN ID TLV data types from outbound LLDP advertisements.
Syntax	config lldp ports [<portlist> all] dot1_tlv_pvid [enable disable]
Description	This TLV optional data type determines whether the IEEE 802.1 organization defined port VLAN TLV transmission is allowed on a given LLDP transmission capable port.
Parameters	<p><portlist> – Use this parameter to define ports to be configured.</p> <p>all – Use this parameter to set all ports in the system.</p> <p>dot1_tlv_pvid – This TLV optional data type determines whether the IEEE 802.1 organization defined port VLAN ID TLV transmission is allowed on a given LLDP transmission capable port. The default state is disabled.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure exclude the VLAN nameTLV from the outbound LLDP advertisements for all ports:

```
DGS-3450:admin# config lldp ports all dot1_tlv_pvid enable
Command: config lldp ports all dot1_tlv_pvid enable

Success.

DGS-3450:admin#
```

config lldp dot1_tlv_protocol_vid

Purpose	Used to configure an individual port or group of ports to exclude one or more of IEEE 802.1 organization port and protocol VLAN ID TLV data types from outbound LLDP advertisements.
Syntax	config lldp ports [<portlist> all] dot1_tlv_protocol_vid [vlan [all <vlan_name 32>] vlanid <vidlist>] [enable disable]
Description	This TLV optional data type indicates whether the corresponding Local System's port and protocol VLAN ID instance will be transmitted on the port. If a port is associated with multiple protocol VLANs, those enabled port and protocol VLAN IDs will be advertised.
Parameters	<p><portlist> – Use this parameter to define ports to be configured.</p> <p>all – Use this parameter to set all ports in the system.</p> <p>dot1_tlv_protocol_vid – This TLV optional data type determines whether the IEEE 802.1 organization defined port and protocol VLAN ID TLV transmission is allowed on a given LLDP transmission capable port. The default state is disabled.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure exclude the port and protocol VLAN ID TLV from the outbound LLDP advertisements for all ports:

```
DGS-3450:admin# config lldp ports all dot1_tlv_protocol_vid vlnaid 1-3 enable
Command: config lldp ports all dot1_tlv_protocol_vid vlnaid 1-3 enable

Success.

DGS-3450:admin#
```


config lldp dot1_tlv_vlan_name

Purpose	Used to configure an individual port or group of ports to exclude one or more of IEEE 802.1 organization VLAN name TLV data types from outbound LLDP advertisements.
Syntax	config lldp ports [<portlist> all] dot1_tlv_vlan_name [vlan [all <vlan_name 32>] vlanid <vidlist>] [enable disable]
Description	This TLV optional data type indicates whether the corresponding Local System's VLAN name instance will be transmitted on the port. If a port is associated with multiple VLANs, those enabled VLAN IDs will be advertised.
Parameters	<p><portlist> – Use this parameter to define ports to be configured.</p> <p>all – Use this parameter to set all ports in the system.</p> <p>dot1_tlv_vlan_name – This TLV optional data type indicates whether the corresponding Local System's VLAN name instance will be transmitted on the port. If a port is associated with multiple VLANs, those enabled VLAN IDs will be advertised. The default state is disabled.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure exclude the VLAN name TLV from the outbound LLDP advertisements for all ports:

```
DGS-3450:admin# config lldp ports all dot1_tlv_vlan_name vlanid 1-3 enable
Command: config lldp ports all dot1_tlv_vlan_name vlanid 1-3 enable

Success.

DGS-3450:admin#
```

config lldp dot1_tlv_protocol_identity

Purpose	Used to configure an individual port or group of ports to exclude one or more of IEEE 802.1 organization protocol identity TLV data types from outbound LLDP advertisements.
Syntax	config lldp ports [<portlist> all] dot1_tlv_protocol_identity [all {eapol lacp gvrp stp }] [enable disable]
Description	This TLV optional data type indicates whether the corresponding Local System's Protocol Identity instance will be transmitted on the port. The Protocol Identity TLV provides a way for stations to advertise protocols that are important to the operation of the network. Such as Spanning Tree Protocol, the Link Aggregation Control Protocol, and numerous vendor proprietary variations are responsible for maintaining the topology and connectivity of the network. If EAPOL, GVRP, STP (including MSTP), and LACP protocol identity is enabled on this port and it is enabled to be advertised, then this protocol identity will be advertised.
Parameters	<p><portlist> – Use this parameter to define ports to be configured.</p> <p>all – Use this parameter to set all ports in the system.</p> <p>dot1_tlv_protocol_identity – This TLV optional data type indicates whether the corresponding Local System's Protocol Identity instance will be transmitted on the port. The Protocol Identity TLV provides a way for stations to advertise protocols that are important to the operation of the network, such as Spanning Tree Protocol, the Link Aggregation Control Protocol, and numerous vendor proprietary variations which are responsible for maintaining the topology and connectivity of the network. If EAPOL, GVRP, STP (including MSTP), and LACP protocol identity is enabled on this port and it is enabled to be advertised, then this protocol identity will be advertised. The default state is disabled.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure exclude the protocol identity TLV from the outbound LLDP advertisements for all ports:

```
DGS-3450:admin# config lldp ports all dot1_tlv_protocol_identity all enable
Command: config lldp ports all dot1_tlv_protocol_identity all enable

Success.

DGS-3450:admin#
```

config lldp dot3_tlvs

Purpose	Used to configure an individual port or group of ports to exclude one or more of IEEE 802.3 organization specific TLV data types from outbound LLDP advertisements.
Syntax	config lldp ports [<portlist> all] dot3_tlvs [all {mac_phy_configuration_status link_aggregation maximum_frame_size}] [enable disable]
Description	Each Specific TLV in this extension can be enabled individually.
Parameters	<p><portlist> – Use this parameter to define ports to be configured.</p> <p>all – Use this parameter to set all ports in the system.</p> <p>mac_phy_configuration_status – This TLV optional data type indicates that LLDP agent should transmit 'MAC/PHY configuration/status TLV'. This type indicates it is possible for two ends of an IEEE 802.3 link to be configured with different and/or speed settings and still establish some limited network connectivity. More precisely, the information includes whether the port support the auto-negotiation function, whether the function is enabled, the auto-negotiated advertised capability, and the operational MAU type. The default state is disabled.</p> <p>link_aggregation – This TLV optional data type indicates that LLDP agent should transmit 'Link Aggregation TLV'. This type indicates the current link aggregation status of IEEE 802.3 MACs. More precisely, the information should include whether the port is capable of doing link aggregation, whether the port is aggregated in a aggregated link, and the aggregated port ID. The default state is disabled.</p> <p>power_via_mdi – This TLV optional data type indicates that the LLDP agent should transmit 'Power via MDI TLV'. Three IEEE 802.3 PMD implementations (10BASE-T, 100BASE-TX, and 1000BASE-T) allow power to be supplied over the link for connected non-powered systems. The Power Via MDI TLV allows network management to advertise and discover the MDI power support capabilities of the sending IEEE 802.3 LAN station. The default state is disabled.</p> <p>NOTE: Not supported in the current release.</p> <p>maximum_frame_size – This TLV optional data type indicates that LLDP agent should transmit 'Maximum-frame-size TLV'. The default state is disabled.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure exclude the MAC/PHY configuration/status TLV from the outbound LLDP advertisements for all ports:

```
DGS-3450:admin# config lldp ports all dot3_tlvs mac_phy_configuration_status enable
Command: config lldp ports all dot3_tlvs mac_phy_configuration_status enable

Success.

DGS-3450:admin#
```

config lldp forward_message

Purpose	Used to configure the forwarding of LLDPDU packets when LLDP is disabled.
Syntax	config lldp forward_message [enable disable]
Description	When LLDP is disabled and LLDP forward_message is enabled, the received LLDPDU packets will be forwarded. The default state is disabled.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure LLDP forward_message:

```
DGS-3450:admin# config lldp forward_message enable
Command: config lldp forward_message enable

Success.

DGS-3450:admin#
```

show lldp

Purpose	This command displays the switch's general LLDP configuration status.
Syntax	show lldp
Description	This command displays the switch's general LLDP configuration status.
Parameters	None.
Restrictions	None.

Example usage:

To display the LLDP system level configuration status:

```
DGS-3450:admin# show lldp
Command: show lldp

LLDP System Information
  Chassis ID Subtype      : MAC Address
  Chassis ID              : 00-19-5B-F5-26-C0
  System Name             :
  System Description      : Gigabit Ethernet Switch
  System Capabilities     : Repeater, Bridge

LLDP Configurations
  LLDP Status             : Disabled
  LLDP Forward Status     : Disabled
  Message Tx Interval     : 30
  Message Tx Hold Multiplier: 4
  ReInit Delay            : 2
  Tx Delay                : 2
  Notification Interval   : 5

DGS-3450:admin#
```

show lldp mgt_addr

Purpose	Used to display the LLDP management address information.
Syntax	show lldp mgt_addr {[ipv4 <ipaddr> ipv6 <ipv6addr>]}
Description	Displays the LLDP management address information.
Parameters	<i>ipv4</i> – The IP address of IPv4. <i>ipv6</i> – The IP address of IPv6.
Restrictions	None.

Example usage:

To display management address information for port 1:

```
DGS-3450:admin# show lldp mgt_addr ipv4 192.168.254.10
Command: show lldp mgt_addr ipv4 192.168.254.10
```

Address 1

```
-----
Subtype           : IPv4
Address           : 192.168.254.10
IF type          : Unknown
OID              : 1.3.6.1.4.1.171.10.36.1.11
Advertising Ports : 1:1-1:5, 1:7, 2:10-2:20
```

```
DGS-3450:admin#
```

show lldp ports

Purpose	Display the LLDP per port configuration for advertisement options.
Syntax	show lldp ports {<portlist>}
Description	This command displays the LLDP per port configuration for advertisement options.
Parameters	<portlist> – Use this parameter to define ports to be configured.
Restrictions	None.

Example usage:

To display the LLDP per port TLV option configuration:

```
DGS-3450:admin# show lldp ports 1
```

```
Command: show lldp ports 1
```

```
Port ID : 1:1
```

```
-----
```

```
Admin Status : TX_and_RX
```

```
Notification Status : Disabled
```

```
Advertised TLVs Option :
```

```
Port Description Disabled
```

```
System Name Disabled
```

```
System Description Disabled
```

```
System Capabilities Disabled
```

```
Enabled Management Address
```

```
(None)
```

```
Port VLAN ID Disabled
```

```
Enabled Port_and_Protocol_VLAN_ID
```

```
(None)
```

```
Enabled VLAN Name
```

```
(None)
```

```
Enabled Protocol_Identity
```

```
(None)
```

```
MAC/PHY Configuration/Status Disabled
```

```
Link Aggregation Disabled
```

```
Maximum Frame Size Disabled
```

```
DGS-3450:admin#
```

show lldp local_ports

Purpose	Used to display the per-port information currently available for populating outbound LLDP advertisements.
Syntax	show lldp local_ports {<portlist>} {mode [brief normal detailed]}
Description	This command displays the per-port information currently available for populating outbound LLDP advertisements.
Parameters	<p><i><portlist></i> – Use this parameter to define ports to be configured.</p> <p><i>brief</i> – Display the information in brief mode.</p> <p><i>normal</i> – Display the information in normal mode. This is the default display mode.</p> <p><i>detailed</i> – Display the information in detailed mode.</p>
Restrictions	None.

Example usage:

To display outbound LLDP advertisements for port 1:

```
DGS-3450:admin# show lldp local_ports 1
Command: show lldp local_ports 1

Port ID : 1:1
-----
Port ID Subtype           : Local
Port ID                   : 1/1
Port Description          :
Port PVID                 : 1
Management Address Count : 1
PPVID Entries Count      : 0
VLAN Name Entries Count  : 1
Protocol Identity Entries Count : 0
MAC/PHY Configuration/Status : (See Detail)
Link Aggregation         : (See Detail)
Maximum Frame Size       : 1536

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

show lldp remote_ports

Purpose	Used to display the information learned from the neighbor.
Syntax	show lldp remote_ports {<portlist>} {mode [brief normal detailed]}
Description	This command display the information learned from the neighbor parameters. Due to a memory limitation, only 32 VLAN Name entries and 10 Management Address entries can be received.
Parameters	<p><portlist> – Use this parameter to define ports to be configured.</p> <p>mode – Choose from three options:</p> <p>brief – Display the information in brief mode.</p> <p>normal – Display the information in normal mode. This is the default display mode.</p> <p>detailed – Display the information in detailed mode.</p>
Restrictions	None.

Example usage:

To display remote table in brief mode:

```
DGS-3450:admin# show lldp remote_ports 1-2 mode brief
Command: show lldp remote_ports 1-2 mode brief

Port ID: 1:1
-----
Remote Entities Count   : 1
Entity 1
  Chassis ID Subtype    : MAC Address
  Chassis ID            : 00-01-0-2-03-04-01
  Port ID Subtype      : Local
  Port ID               : 1/3
  Port Description      : RMON Port 1 on Unit 3

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

show lldp statistics

Purpose	Used to display the system LLDP statistics information.
Syntax	show lldp statistics
Description	The global LLDP statistics displays an overview of neighbor detection activity on the switch.
Parameters	None.
Restrictions	None.

Example usage:

To display global statistics information:

```
DGS-3450:admin# show lldp statistics
```

```
Command: show lldp statistics
```

```
Last Change Time      : 4875
Number of Table Insert : 0
Number of Table Delete : 0
Number of Table Drop   : 0
Number of Table Ageout : 0
```

```
DGS-3450:admin#
```

show lldp statistics ports

Purpose	Used to display the ports LLDP statistics information.
Syntax	show lldp statistics ports{<portlist>}
Description	The per-port LLDP statistics command displays per-port LLDP statistics.
Parameters	<i><portlist></i> – Use this parameter to define ports to be configured. When portlist is not specified, information for all ports will be displayed.
Restrictions	None.

Example usage:

To display statistics information of port 1:

```
DGS-3450:admin# show lldp statistics ports 1
```

```
Command: show lldp statistics ports 1
```

```
Port ID : 1:1
```

```
-----
LLDPStatsTxPortFramesTotal      : 0
LLDPStatsRxPortFramesDiscardedTotal : 0
LLDPStatsRxPortFramesErrors     : 0
LLDPStatsRxPortFramesTotal      : 0
LLDPStatsRxPortTLVsDiscardedTotal : 0
LLDPStatsRxPortTLVsUnrecognizedTotal : 0
LLDPStatsRxPortAgeoutsTotal     : 0
```

```
DGS-3450:admin#
```

MAC NOTIFICATION COMMANDS

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

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

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

enable mac_notification

Purpose	Used to enable global MAC address table notification on the Switch.
Syntax	enable mac_notification
Description	This command is used to enable MAC address notification without changing configuration.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable MAC notification without changing basic configuration:

```
DGS-3450:admin# enable mac_notification
Command: enable mac_notification
```

Success.

```
DGS-3450:admin#
```

disable mac_notification

Purpose	Used to disable global MAC address table notification on the Switch.
Syntax	disable mac_notification
Description	This command is used to disable MAC address notification without changing configuration.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable MAC notification without changing basic configuration:


```
DGS-3450:admin# disable mac_notification
Command: disable mac_notification

Success.

DGS-3450:admin#
```

config mac_notification

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

Example usage:

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

```
DGS-3450:admin# config mac_notification interval 1 historysize 500
Command: config mac_notification interval 1 historysize 500

Success.

DGS-3450:admin#
```

config mac_notification ports

Purpose	Used to configure MAC address notification status settings.
Syntax	config mac_notification ports [<portlist> all] [enable disable]
Description	MAC address notification is used to monitor MAC addresses learned and entered into the FDB.
Parameters	<i><portlist></i> – Specify a port or range of ports to be configured. The beginning and end of the port list range are separated by a dash. Non-contiguous portlist entries are separated by a comma. (ex: 1-3,7-9) <i>all</i> – Entering this command will set all ports on the system. <i>[enable disable]</i> – These commands will enable or disable MAC address table notification on the Switch.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable port 7 for MAC address table notification:

```
DGS-3450:admin# config mac_notification ports 7 enable
Command: config mac_notification ports 7 enable

Success.

DGS-3450:admin#
```

show mac_notification

Purpose	Used to display the Switch's MAC address table notification global settings
Syntax	show mac_notification
Description	This command is used to display the Switch's MAC address table notification global settings.
Parameters	None.
Restrictions	None.

Example usage:

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

```
DGS-3450:admin# show mac_notification
Command: show mac_notification

Global Mac Notification Settings

State      : Enabled
Interval   : 1
History Size : 1

DGS-3450:admin#
```

show mac_notification ports

Purpose	Used to display the Switch's MAC address table notification status settings
Syntax	show mac_notification ports {<portlist>}
Description	This command is used to display the Switch's MAC address table notification status settings.
Parameters	<portlist> – Specify a port or group of ports to be viewed. The beginning and end of the port list range are separated by a dash. Non-contiguous portlist entries are separated by a comma. (ex: 1-3,7-9) Entering this command without the parameter will display the MAC notification table for all ports.
Restrictions	None.

Example usage:

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

```
DGS-3450:admin# show mac_notification ports
```

```
Command: show mac_notification ports
```

```
Port #   MAC Address Table Notification State
```

```
-----
```

1	Disabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled
8	Disabled
9	Disabled
10	Disabled
11	Disabled
12	Disabled
13	Disabled
14	Disabled
15	Disabled
16	Disabled
17	Disabled
18	Disabled
19	Disabled
20	Disabled

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

MAC-BASED ACCESS CONTROL COMMANDS

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

Command	Parameters
enable mac_based_access_control	
disable mac_based_access_control	
config mac_based_access_control password	<passwd 16>
config mac_based_access_control method	[local radius]
config mac_based_access_control guest_vlan ports	<portlist>
config mac_based_access_control ports	[<portlist> all] {state [enable disable] mode [port_based host_based] aging_time [infinite <min 1-1440>] [block_time hold_time] [infinite <sec 1-300>] max_users [<value 1-4000> no_limit]}(1)
create mac_based_access_control	[guest_vlan <vlan_name 32> guest_vlanid <vlanid 1-4094>]
delete mac_based_access_control	[guest_vlan <vlan_name 32> guest_vlanid <vlanid 1-4094>]
clear mac_based_access_control auth_state	[ports [all <portlist>] mac_addr <macaddr>]
create mac_based_access_control_local mac	<macaddr> {[vlan <vlan_name 32> vlanid <vlanid 1-4094>]}
config mac_based_access_control_local mac	<macaddr> [vlan <vlan_name 32> vlanid <vlanid 1-4094> clear_vlan]
delete mac_based_access_control_local	[mac <macaddr> vlan <vlan_name 32> vlanid <vlanid 1-4094>]
config mac_based_access_control authorization network	{radius [enable disable] local [enable disable]} (1)
show mac_based_access_control	{ports {<portlist>}}
show mac_based_access_control_local	{[mac <macaddr> vlan <vlan_name 32> vlanid <1-4094>]}
show mac_based_access_control auth_state ports	<portlist>
config mac_based_access_control max_users	[<value 1-4000> no_limit]

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

enable mac_based_access_control

Purpose	Used to enable MAC-based Access Control.
Syntax	enable mac_based_access_control
Description	This command enables the MAC-based Access Control function.

enable mac_based_access_control

Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable the MAC-based Access Control global state:

```
DGS-3450:admin# enable mac_based_access_control
Command: enable mac_based_access_control
```

Success.

```
DGS-3450:admin#
```

disable mac_based_access_control

Purpose	Used to disable MAC-based Access Control.
Syntax	disable mac_based_access_control
Description	This command disables the MAC-based Access Control function.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable the MAC-based Access Control global state:

```
DGS-3450:admin# disable mac_based_access_control
Command: disable mac_based_access_control
```

Success.

```
DGS-3450:admin#
```

config mac_based_access_control password

Purpose	Used to configure the RADIUS authentication password for MAC-based Access Control.
Syntax	config mac_based_access_control password <passwd 16>
Description	This command will set the password that will be used for authentication via the RADIUS server.
Parameters	<passwd 16> - In RADIUS mode, the switch will communicate with the RADIUS server using this password. The maximum length of the key is 16.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To set the MAC-based Access Control password:

```
DGS-3450:admin# config mac_based_access_control password switch
Command: config mac_based_access_control password switch

Success.

DGS-3450:admin#
```

config mac_based_access_control method

Purpose	Used to configure the MAC-based Access Control authentication method.
Syntax	config mac_based_access_control method [local radius]
Description	Specify the authentication method used via the local database or via the RADIUS server.
Parameters	<i>local</i> - Specify to authenticate via the local database. <i>radius</i> - Specify to authenticate via a RADIUS server.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To set the MAC-based Access Control authentication method as local:

```
DGS-3450:admin# config mac_based_access_control method local
Command: config mac_based_access_control method local

Success.

DGS-3450:admin#
```

config mac_based_access_control guest_vlan

Purpose	Used to configure the MAC-based Access Control guest VLAN membership.
Syntax	config mac_based_access_control guest_vlan ports <portlist>
Description	This command will assign a specified port list to the MAC-based Access Control guest VLAN. Ports that are not contained in port list will be removed from the MAC-based Access Control guest VLAN.
Parameters	<portlist> - Specify MAC-based Access Control guest VLAN membership.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To set the MAC-based Access Control guest VLAN membership:

```
DGS-3450:admin# config mac_based_access_control guest_vlan ports 1-8
Command: config mac_based_access_control guest_vlan ports 1-8

Success.

DGS-3450:admin#
```

config mac_based_access_control ports

Purpose	Used to configure the port parameters for MAC-based Access Control.
---------	---

config mac_based_access_control ports

Syntax	config mac_based_access_control ports [<portlist> all] {state [enable disable] mode [port_based host_based] aging_time [infinite <min 1-1440>] [block_time hold_time] [infinite <sec 1-300>] max_users [<value 1-4000> no_limit]}(1)
Description	<p>This command allows configures MAC-based Access Control port's setting.</p> <p>When the MAC-based Access Control function is enabled for a port and the port is not a MAC-based Access Control guest VLAN member, the user who is attached to this port will not be forwarded unless the user passes the authentication. A user that does not pass the authentication will not be serviced by the switch. If the user passes the authentication, the user will be able to forward traffic operated under the assigned VLAN.</p> <p>When the MAC-based Access Control function is enabled for a port, and the port is a MAC-based Access Control guest VLAN member, the port(s) will be removed from the original VLAN(s) member ports, and added to MAC-based Access Control guest VLAN member ports. Before the authentication process starts, the user is able to forward traffic under the guest VLAN. After the authentication process, the user will be able to access the assigned VLAN.</p> <p>If the port authorize mode is port based mode, when the port has been moved to the authorized VLAN, the subsequent users will not be authenticated again. They will operate in the current authorized VLAN. If the port authorize mode is host based mode, then each user will be authorized individually and be capable of getting its own assigned VLAN.</p>
Parameters	<p><i>ports</i> - Specifies a range of ports for configuring the MAC-based Access Control function parameters.</p> <p><i>state</i> - Specifies whether the port's MAC-based Access Control function is enabled or disabled.</p> <p><i>mode</i> - See below:</p> <p style="padding-left: 2em;"><i>port_based</i> - Port based means that all users connected to a port share the first authentication result.</p> <p style="padding-left: 2em;"><i>host_based</i> - Host based means that each user has its own authentication result. If the Switch does not support MAC-based VLANs, the switch will not allow the host based option for ports that are in guest VLAN mode.</p> <p><i>aging_time</i> - A time period during which an authenticated host will be kept in an authenticated state. When the aging time has timed-out, the host will be moved back to unauthenticated state. If the aging time is set to infinite, it means that authorized clients will not be aged out automatically.</p> <p><i>block_time</i> - If a host fails to pass the authentication, the next authentication will not start within the block time unless the user clears the entry state manually. If the block time is set to 0, it means do not block the client that failed authentication.</p> <p><i>block_time</i> – Specify the block time here.</p> <p><i>infinite</i> – Specify to set the time to infinite.</p> <p><i>max_users</i> - Specify maximum number of users per port. The range is 1 to 4000. The default value is 128.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the MAC-based Access Control state for ports 1 to 8:

```
DGS-3450:admin# config mac_based_access_control ports 1-8 state enable
Command: config mac_based_access_control ports 1-8 state enable
```

Success.

```
DGS-3450:admin#
```

To configure the MAC-based Access Control authorization mode for ports 1 to 8:

```
DGS-3450:admin# config mac_based_access_control ports 1-8 mode host_based
Command: config mac_based_access_control ports 1-8 mode host_based

Success.

DGS-3450:admin#
```

To configure an unlimited number of maximum users for MAC-based Access Control on ports 1 to 8:

```
DGS-3450:admin# config mac_based_access_control ports 1-8 max_users no_limit
Command: config mac_based_access_control ports 1-8 max_users no_limit

Success.

DGS-3450:admin#
```

To configure the MAC-based Access Control timer parameters to have an infinite aging time and a block time of 120 seconds on ports 1 to 8:

```
DGS-3450:admin# config mac_based_access_control ports 1-8 aging_time infinite block_time
120
Command: config mac_based_access_control ports 1-8 aging_time infinite block_time 120

Success.

DGS-3450:admin#
```

create mac_based_access_control guest_vlan

Purpose	Used to assign a static 802.1Q VLAN as a MAC-based Access Control guest VLAN.
Syntax	create mac_based_access_control [guest_vlan <vlan_name 32> guest_vlanid <vlanid 1-4094>]
Description	Used to assign a static 802.1Q VLAN as a MAC-based Access Control guest VLAN. This command can be used to manage unauthenticated hosts in this guest VLAN, that is, the unauthenticated host will stay in this guest VLAN until a successful authentication attempt.
Parameters	<i>guest_vlan</i> - Specify MAC-based Access Control guest VLAN by name, it must be a static 1Q VLAN. <i>guest_vlanid</i> - Specify MAC-based Access Control guest VLAN by VID, it must be a static 1Q VLAN.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create a MAC-based Access Control guest VLAN:

```
DGS-3450:admin# create mac_based_access_control guest_vlan VLAN8
Command: create mac_based_access_control guest_vlan VLAN8

Success.

DGS-3450:admin#
```


delete mac_based_access_control guest_vlan

Purpose	Used to remove a MAC-based Access Control guest VLAN.
Syntax	delete mac_based_access_control [guest_vlan <vlan_name 32> guest_vlanid <vlanid 1-4094>]
Description	Use this command to remove a MAC-based Access Control guest VLAN. When the guest VLAN is removed, the guest VLAN function will be disabled.
Parameters	<i>guest_vlan</i> - Specifies the name of the MAC-based Access Control's guest VLAN <i>guest_vlanid</i> - Specifies the VID of the MAC-based Access Control's guest VLAN
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete the MAC-based Access Control guest VLAN called default:

```
DGS-3450:admin# delete mac_based_access_control guest_vlan default
Command: delete mac_based_access_control guest_vlan default

Success.

DGS-3450:admin#
```

clear mac_based_access_control auth_state

Purpose	Used to clear the clients' authentication information by specific port(s) or MAC address.
Syntax	clear mac_based_access_control auth_state [ports [all <portlist>] mac_addr <macaddr>]
Description	This command is used to clear the authentication state of a user (or port). The port (or the user) will return to an un-authenticated state. All the timers associated with the port (or the user) will be reset.
Parameters	<i>ports</i> - To specify the port range to delete MAC addresses on them. <i><macaddr></i> - To delete a specified host with this MAC address.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To clear MAC-based Access Control clients' authentication information for all ports:

```
DGS-3450:admin# clear mac_based_access_control auth_state ports all
Command: clear mac_based_access_control auth_state ports all

Success.

DGS-3450:admin#
```

To delete the MAC-based Access Control authentication information for the host that has a MAC address of 00-00-00-47-04-65:

```
DGS-3450:admin# clear mac_based_access_control auth_state mac_addr 00-00-00-47-04-65
Command: clear mac_based_access_control auth_state mac_addr 00-00-00-47-04-65

Success.

DGS-3450:admin#
```

create mac_based_access_control_local

Purpose	Used to create a MAC-based Access Control local database entry that will be used for authentication. This command can also specify the VLAN that an authorized host will be assigned to.
Syntax	create mac_based_access_control_local mac <macaddr> {[vlan <vlan_name 32> vlanid <vlanid 1-4094>]}
Description	This command is used to create a database entry. The user also has the option of specifying a target VLAN for this entry.
Parameters	<p><i>mac</i> - Specify the MAC address that can pass local authentication.</p> <p><i>vlan</i> - Specify the target VLAN by using the VLAN name. When this host is authorized, it will be assigned to this VLAN.</p> <p><i>vlanid</i> - Specify the target VLAN by using the VID. When this host is authorized, it will be assigned to this VLAN if the target VLAN exists.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create one MAC-based Access Control local database entry for MAC address 00-00-00-00-00-01 and specify that the host will be assigned to the “default” VLAN after the host has been authorized:

```
DGS-3450:admin# create mac_based_access_control_local mac 00-00-00-00-00-01 vlan default
Command: create mac_based_access_control_local mac 00-00-00-00-00-01 vlan default

Success.

DGS-3450:admin#
```

config mac_based_access_control_local

Purpose	Used to configure a MAC-based Access Control local database entry.
Syntax	config mac_based_access_control_local mac <macaddr> [vlan <vlan_name 32> vlanid <vlanid 1-4094> clear_vlan]
Description	This command is used to configure a MAC-based Access Control local database entry.
Parameters	<p><i>mac</i> - Specify the authenticated host's MAC address.</p> <p><i>vlan</i> - Specify the target VLAN by VLAN name. When this host is authorized, the host will be assigned to this VLAN.</p> <p><i>vlanid</i> - Specify the target VLAN by VID. When this host is authorized, the host will be assigned to this VLAN if the target VLAN exists.</p> <p><i>clear_vlan</i> - Clear target VLAN information for specific hosts from the local database.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the target VLAN “default” for the MAC-based Access Control local database entry 00-00-00-00-00-01:

```
DGS-3450:admin# config mac_based_access_control_local mac 00-00-00-00-00-01 vlan default
Command: config mac_based_access_control_local mac 00-00-00-00-00-01 vlan default

Success.

DGS-3450:admin#
```

delete mac_based_access_control_local

Purpose	Used to delete a MAC-based Access Control local database entry.
Syntax	delete mac_based_access_control_local [mac <macaddr> vlan <vlan_name 32> vlanid <vlanid 1-4094>]
Description	This command is used to delete a MAC-based Access Control local database entry.
Parameters	<i>mac</i> - Delete local database entry by specific MAC address. <i>vlan</i> - Delete local database entries by specific target VLAN name. <i>vlanid</i> - Delete local database entries by specific target VLAN ID.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete the MAC-based Access Control local database entry for MAC address 00-00-00-00-00-01:

```
DGS-3450:admin# delete mac_based_access_control_local mac 00-00-00-00-00-01
Command: delete mac_based_access_control_local mac 00-00-00-00-00-01

Success.

DGS-3450:admin#
```

To delete the MAC-based Access Control local database entry for the VLAN name VLAN3:

```
DGS-3450:admin# delete mac_based_access_control_local vlan VLAN3
Command: delete mac_based_access_control_local vlan VLAN3

Success.

DGS-3450:admin#
```

config mac_based_access_control authorization network

Purpose	Used to enable or disable the acceptance of an authorized configuration.
Syntax	config mac_based_access_control authorization network {radius [enable disable] local [enable disable]} (1)
Description	Used to enable or disable the acceptance of an authorized configuration. When authorization is enabled for MAC-based Access Controls with RADIUS authentication, the authorized attributes (for example VLAN, 802.1p default priority, and ACL) assigned by the RADIUS server will be accepted if the global authorization status is enabled. When authorization is enabled for MAC-based Access Controls with local authentication, the authorized attributes assigned by the local database will be accepted.
Parameters	<i>radius</i> - If specified to enable, the authorized attributes (for example VLAN, 802.1p default priority, and ACL) assigned by the RADIUS server will be accepted if the global authorization status is enabled. The default state is enabled. <i>local</i> - If specified to enable, the authorized attributes assigned by the local database will be

config mac_based_access_control authorization network

	accepted if the global authorization status is enabled. The default state is enabled.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

The following example will disable the configuration authorized from the local database:

```
DGS-3450:admin# config mac_based_access_control authorization attributes local disable
Command: config mac_based_access_control authorization attributes local disable

Success.

DGS-3450:admin#
```

show mac_based_access_control

Purpose	Used to display the MAC-based Access Control setting.
Syntax	show mac_based_access_control {ports {<portlist>}}
Description	This command is used to display the MAC-based Access Control settings.
Parameters	If the ports parameter is not specified, the global MAC-based Access Control settings will be displayed. <portlist> - Displays the MAC-based Access Control settings for a specific port or range of ports. If no port list is specified, the settings will be displayed for ports which have MAC-based Access Control enabled.
Restrictions	None.

Example usage:

To show the MAC-based Access Control port configuration for ports 1 to 4:

```
DGS-3450:admin# show mac_based_access_control ports 1-4
Command: show mac_based_access_control ports 1-4
```

Port	State	Aging Time	Block Time (min)	Auth Mode (sec)	Max Users
1	Disabled	100	100	Port-based	128
2	Disabled	100	200	Host-based	128
3	Disabled	50	0	Port-based	2000
4	Disabled	Infinite	100	Host-based	No Limit

```
DGS-3450:admin#
```

show mac_based_access_control_local

Purpose	Used to display the MAC-based Access Control local database entry(s).
Syntax	show mac_based_access_control_local {[mac <macaddr> vlan <vlan_name 32> vlanid <1-4094>]}
Description	This command is used to display the MAC-based Access Control local database entries.
Parameters	Displays all MAC-based Access Control local database entries.

show mac_based_access_control_local

mac - Displays MAC-based Access Control local database entries for a specific MAC address.
vlan - Displays MAC-based Access Control local database entries for a specific target VLAN name.
vlanid - Displays MAC-based Access Control local database entries for a specific target VLAN ID.

Restrictions None.

Example usage:

To show the MAC-based Access Control local database:

```
DGS-3450:admin# show mac_based_access_control_local
Command: show mac_based_access_control_local
```

MAC Address	VID
00-00-00-00-00-01	1
00-00-00-00-00-02	123
00-00-00-00-00-03	123
00-00-00-00-00-04	1

Total Entries:4

DGS-3450:admin#

To show the MAC-based Access Control local database for the MAC address 00-00-00-00-00-01:

```
DGS-3450:admin# show mac_based_access_control_local mac 00-00-00-00-00-01
Command: show mac_based_access_control_local mac 00-00-00-00-00-01
```

MAC Address	VID
00-00-00-00-00-01	1

Total Entries:1

DGS-3450:admin#

To show MAC-based Access Control local database for the VLAN called 'default':

```
DGS-3450:admin# show mac_based_access_control_local vlan default
Command: show mac_based_access_control_local vlan default
```

MAC Address	VID
00-00-00-00-00-01	1
00-00-00-00-00-04	1

Total Entries:2

DGS-3450:admin#

show mac_based_access_control_auth_state

Purpose	Used to display the MAC-based Access Control authentication status.
Syntax	show mac_based_access_control_auth_state ports <portlist>
Description	This command is used to display the MAC-based Access Control authentication status.
Parameters	<portlist> - Display authentication status by specific port. If not specified port(s), it will display all of MAC-based Access Control ports authentication status.
Restrictions	None.

Example usage:

Suppose that port 1 is in host based mode:

- MAC 00-00-00-00-00-01 is authenticated without a VLAN assigned (may be the specified target VLAN does not exist or the target VLAN has not been specified at all), the ID of the RX VLAN will be displayed (RX VLAN ID is 4004 in this example).
- MAC 00-00-00-00-00-02 is authenticated with a target VLAN assigned, the ID of the target VLAN will be displayed (target VLAN ID is 1234 in this example).
- MAC 00-00-00-00-00-03 fails to pass authentication, the VID field will be shown as "-", indicating that packets with SA 00-00-00-00-00-03 will be dropped no matter which VLAN these packets are from.
- MAC 00-00-00-00-00-04 attempts to start authentication, the VID field will be shown as "--" until authentication completes.

Suppose that port 2 is in port based mode:

- MAC 00-00-00-00-00-10 is the host which causes port 2 to pass authentication; the MAC address is followed by "(P)" to indicate port based mode authentication.

Suppose that port 3 is in port based mode:

- MAC 00-00-00-00-00-20 attempts to start authentication, the MAC address is followed by "(P)" to indicate port based mode authentication.
- MAC 00-00-00-00-00-21 fails to pass authentication, the MAC address is followed by "(P)" to indicate port based mode authentication.

NOTE: In port-based mode, the VLAN ID field is displayed in the same way as host based mode.

To display the MAC-based Access Control authentication status on port 1, 2, 3.

```
DGS-3450:admin# show mac_based_access_control auth_state ports 1-3
```

```
Command: show mac_based_access_control auth_state ports 1-3
```

```
(P):Port based
```

Port	MAC Address	State	VID	Priority	Aging Time/ Block Time
1	00-00-00-00-00-01	Authenticated	4004	3	Infinite
1	00-00-00-00-00-02	Authenticated	1234	-	Infinite
1	00-00-00-00-00-03	Blocked	-	-	60
1	00-00-00-00-00-04	Authenticating	-	-	5
2	00-00-00-00-00-10(P)	Authenticated	1234	4	1440
3	00-00-00-00-00-20(P)	Authenticating	-	-	20
3	00-00-00-00-00-21(P)	Blocked	-	-	120

```
Total Authenticating Hosts :2
```

```
Total Authenticated Hosts :3
```

```
Total Blocked Hosts :2
```

```
DGS-3450:admin#
```

config mac_based_access_control max_users

Purpose	Used to configure the maximum number of authorized clients.
Syntax	config mac_based_access_control max_users [<value 1-4000> no_limit]
Description	This setting is a global limitation on the maximum number of users that can be learned via MAC-based Access Control. In addition, to the global limitation, the maximum number of users per port is also limited. This is specified by the config config mac_based_access_control ports max_users command.
Parameters	<i><value 1-4000></i> - Specify to set the maximum number of authorized clients on the whole device. <i>no_limit</i> - Specify to not limit the maximum number of users on the system. By default, there is no limit on the number of users.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the maximum number of users the MAC-based Access Control system supports:

```
DGS-3450:admin# config mac_based_access_control max_users 128
```

```
Command: config mac_based_access_control max_users 128
```

```
Success.
```

```
DGS-3450:admin#
```

MIRROR COMMANDS

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

Command	Parameters
config mirror port	<port> {[add delete] source ports <portlist> [rx tx both]}
enable mirror	
disable mirror	
show mirror	{group_id <value 1-4>}
create mirror group_id	<value 1-4>
delete mirror group_id	<value 1-4>
config mirror group_id	<value 1-4> {target_port <port> [add delete] source ports <portlist> [rx tx both] state [enable disable]}(1)

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

config mirror port

Purpose	Used to configure a mirror port – source port pair on the switch. Traffic from any source port to a target port can be mirrored for real-time analysis. A logic analyzer or an RMON probe then can be attached to study the traffic crossing the source port in a completely unobtrusive manner. When mirroring port traffic, please note that the target port must be configured in the same VLAN and operates at the same speed as the source port. If the target port is operating at a lower speed, the source port will be forced to drop its operating speed to match that of the target port.
Syntax	config mirror port <port> {[add delete] source ports <portlist> [rx tx both]}
Description	<p>The config mirror command allows a range of ports to have all of their traffic also sent to a destination port – where a network sniffer or other device can monitor the network traffic. In addition, you can specify that only traffic received by or sent by or both are mirrored to the target port.</p> <p>This command used for single mirror session configuration primarily. If used for multiple session configurations, it configures the parameters on mirror group 1. If group 1 not exist, create group 1 firstly, and than configure the parameters on group 1.</p>
Parameters	<p><i>port</i> - The port that will receive the packets duplicated at the mirror port.</p> <p><i>add</i> - The mirror entry to be added.</p> <p><i>delete</i> - The mirror entry to be deleted.</p> <p><i>portlist</i> - The port that will be mirrored. All packets entering and leaving the source port can be duplicated in the mirror port.</p> <p><i>rx</i> - Allows the mirroring packets received (flowing into) the port or ports in the port list.</p> <p><i>tx</i> - Allows the mirroring packets sent (flowing out of) the port or ports in the port list.</p> <p><i>both</i> - Mirrors all the packets received or sent by the port or ports in the port list.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To add the mirroring ports:


```
DGS-3450:admin# config mirror port 1:3 add source ports 1:7-1:12 both
Command: config mirror port 1:5 add source ports 1:1-1:5 both

Success.

DGS-3450:admin#
```

enable mirror

Purpose	Used to enable mirror globally.
Syntax	enable mirror
Description	This command, combined with the disable mirror command below, allows you to enable or disable mirror function without having to modify the mirror session configuration.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable mirroring function:

```
DGS-3450:admin# enable mirror
Command: enable mirror

Success.

DGS-3450:admin#
```

disable mirror

Purpose	Used to disable mirror globally.
Syntax	disable mirror
Description	This command, combined with the enable mirror command above, allows you to enable or disable mirror function without having to modify the mirror session configuration.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable mirroring function:

```
DGS-3450:admin# disable mirror
Command: disable mirror

Success.

DGS-3450:admin#
```

show mirror

Purpose	Used to show the current ports mirroring configuration on the switch.
Syntax	show mirror {group_id <value 1-4>}

show mirror

Description	The show mirror command displays the current mirror function state and mirror session configuration on the switch. If don't specify the "group_id" parameter, display the all mirror settings.
Parameters	<i>group_id</i> - The mirror group identify. <i>value</i> - The mirror group identify value.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To display mirroring configuration:

```
DGS-3450:admin# show mirror
```

```
Command: show mirror
```

```
Mirror Global State: Enabled
```

Group	State	Target Port	Source Ports
1	Enabled	2:1	RX: 1:1 TX: 1:1
3	Enabled	3:5	RX: 1:24 TX: 1:24

```
DGS-3450:admin#
```

create mirror group_id

Purpose	Used to create a mirror group on the switch.
Syntax	create mirror group_id <value 1-4>
Description	This command used to create a mirror group. If the mirror group has existed, do nothing and return success.
Parameters	<i>group_id</i> - The mirror groups identify. <i>value</i> - The mirror groups identify value.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

Create mirror group 3:

```
DGS-3450:admin# create mirror group_id 3
```

```
Command: create mirror group_id 3
```

```
Success.
```

```
DGS-3450:admin#
```

delete mirror group_id

Purpose	Used to delete a mirror group on the switch.
Syntax	delete mirror group_id <value 1-4>
Description	This command used to delete a mirror group.

delete mirror group_id

Parameters	<i>group_id</i> - The mirror groups identify. <i>value</i> - The mirror groups identify value.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

Create mirror group 2:

```
DGS-3450:admin# delete mirror group_id 3
Command: delete mirror group_id 3
```

Success.

```
DGS-3450:admin#
```

config mirror group_id

Purpose	Used to configure mirror group on the switch.
Syntax	config mirror group_id <value 1-4> {target_port <port> [add delete] source ports <portlist> [rx tx both] state [enable disable]}(1)
Description	This command used to configure mirror group's parameters. It can configure mirror group's target port, state and source ports. The mirror group target port can't be a member of all mirror groups' source ports. Each mirror group's target port can be the same port. But each mirror group's source ports can't overlap.
Parameters	<i>group_id</i> - The mirror groups identify. <i>value</i> - The mirror groups identify value. <i>target_port</i> - The port that will receive the packets duplicated at the mirror port. <i>state</i> - The mirror group state to enable or disable the mirror group function <i>add</i> - The mirror source ports to be add. <i>delete</i> - The mirror source ports to be delete <i>portlist</i> - The port list of mirror group source ports <i>rx</i> - Only the received packets on the mirror group source ports will be mirrored to the mirror group target port. <i>tx</i> - Only the sent packets on the mirror group source ports will be mirrored to the mirror group target port. <i>both</i> - Both the received and sent packets on the mirror group source ports will be mirrored to the mirror group target port.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

Configure mirror group 2 with state enable and add source ports 1:4-1:9:

```
DGS-3450:admin# config mirror group_id 2 state enable add source ports 1:4-1:9 both
Command: config mirror group_id 2 state enable add source ports 1:4-1:9 both
```

Success.

```
DGS-3450:admin#
```

MSTP DEBUG ENHANCEMENT COMMANDS

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

Command	Parameters
debug buffer	[utilization dump clear upload_toTFTP <ipaddr> <path_filename 64>]
debug output	module mstp [buffer console]
debug stp config ports	[< portlist > all] [event bpdu state_machine all] state [disable brief detail]
debug stp show information	
debug stp show flag	{ports <portlist>}
debug stp show counter	{ports [<portlist> all]}
debug stp clear counter	[ports < portlist > all]
debug stp state	[enable disable]

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

debug buffer

Purpose	Use the debug buffer command to dump, clear, or upload the debug buffer to the TFTP server.
Syntax	debug buffer [utilization dump clear upload_toTFTP <ipaddr> <path_filename 64>]
Description	Dump, clear or upload the debug buffer to a TFTP server.
Parameters	<p><i>dump</i> - Displays the debug message in the debug message buffer.</p> <p><i>clear</i> - Clears the debug message buffer.</p> <p><i>upload_toTFTP <ipaddr></i> - Uploads the debug message buffer to a TFTP server with a specified IP address</p> <p><i><path_filename 64></i> - Upload the debug message buffer to a TFTP server and name the uploaded file using the string identified in the <path_filename 64> option.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To clear the debug information in the buffer:

```
DGS-3450:admin# debug buffer clear
Command: debug buffer clear
```

Success.

```
DGS-3450:admin#
```

debug output

Purpose	Use the debug output command to specify if the MSTP debug message output should be to the buffer or console.
---------	--

debug output

Syntax	debug output module mstp [buffer console]
Description	Sets if the MSTP debug message output should be set to the buffer or console.
Parameters	<i>buffer</i> - Specifies the debug messages of MSTP will output to the buffer. <i>console</i> - Specifies the debug messages of MSTP will output to the console.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To set the MSTP debug information to output to the console:

```
DGS-3450:admin# debug output module mstp console
Command: debug output module mstp console
```

Success.

```
DGS-3450:admin#
```

debug stp config ports

Purpose	Used to configure per-port STP debug level.
Syntax	debug stp config ports [< portlist > all] [event bpdu state_machine all] state [disable brief detail]
Description	This command used to configure per-port STP debug level on the specified ports.
Parameters	<i>debug flags</i> - See below: <i>event</i> - Debug the external operation and event processing. <i>bpdu</i> - Debug the BPDU's that have been received and transmitted. <i>state_machine</i> - Debug the state change of the STP state machine. <i>all</i> - Debug all of the above. <i>ports</i> - See below: <i>portlist</i> - Specifies the STP port range to debug. <i>all</i> - Specifies to debug all ports on the switch. <i>state</i> - See below: <i>disable</i> - Disables the debug mechanism. <i>brief</i> - Sets the debug level to brief. <i>detail</i> - Sets the debug level to detail.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure all STP debug flags to brief level on all ports:

```
DGS-3450:admin# debug stp config ports all all state brief
Command: debug stp config ports all all state brief
```

Success.

```
DGS-3450:admin#
```

debug stp show information

Purpose	Used to show the STP debug information.
Syntax	debug stp show information
Description	This command used to display STP detailed information, such as the hardware tables, the STP state machine, etc.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To show STP debug information:

DGS-3450:admin# debug stp show information

Command: debug stp show information

Spanning Tree debug information:

 Port status in hardware table:

Instance 0:

Port 1 :BLK Port 2 :BLK Port 3 :BLK Port 4 :BLK Port 5 :BLK Port 6 :BLK

Port 7 :FOR Port 8 :BLK Port 9 :BLK Port 10:BLK Port 11:BLK Port 12:BLK

Instance 1:

Port 1 :BLK Port 2 :BLK Port 3 :BLK Port 4 :BLK Port 5 :BLK Port 6 :BLK

Port 7 :FOR Port 8 :BLK Port 9 :BLK Port 10:BLK Port 11:BLK Port 12:BLK

Root Priority and Times :

Instance 0:

Designated Root Bridge : 32768/00-01-02-03-04-00

External Root Cost : 0

Regional Root Bridge : 32768/00-01-02-03-04-00

Internal Root Cost : 0

Designated Bridge : 32768/00-01-02-03-04-00

Designated Port : 0

Message Age : 0

Max Age : 20

Forward Delay : 15

Hello Time : 2

Instance 1:

Regional Root Bridge : 32769/00-01-02-03-04-00

Internal Root Cost : 0

Designated Bridge : 32769/00-01-02-03-04-00

Designated Port : 0

Remaining Hops : 20

Designated Prioirty and Times

Instance 0:

Port 1 :

Designated Root Bridge : 0 /00-00-00-00-00-00

External Root Cost : 0

Regional Root Bridge : 0 /00-00-00-00-00-00

Internal Root Cost : 0

Designated Bridge : 0 /00-00-00-00-00-00

Designated Port : 0

Message Age : 0

Max Age : 20

Forward Delay : 15

Hello Time : 2

Instance 1:

Port 1 :

Regional Root Bridge : 0 /00-00-00-00-00-00

Internal Root Cost : 0

Designated Bridge : 0 /00-00-00-00-00-00

Designated Port : 0

Remaining Hops : 20

Success.

DGS-3450:admin#

debug stp show flag

Purpose	Used to show the per-port STP debug level.
Syntax	debug stp show flag {ports <portlist>}
Description	This command used to display the STP debug level on specified ports.
Parameters	<i>ports <portlist></i> - Specifies the STP ports to display If no parameter is specified, all ports on the switch will be displayed.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To display the debug STP levels on all ports:

```
DGS-3450:admin# debug stp show flag
Command: debug stp show flag
```

Global State: Enabled

Port Index	Event flag	BPDU Flag	State Machine Flag
1	Detail	Brief	Disable
2	Detail	Brief	Disable
3	Detail	Brief	Disable
4	Detail	Brief	Disable
5	Detail	Brief	Disable
6	Detail	Brief	Disable
7	Detail	Brief	Disable
8	Detail	Brief	Disable
9	Detail	Brief	Disable
10	Detail	Brief	Disable
11	Detail	Brief	Disable
12	Detail	Brief	Disable

Success.

```
DGS-3450:admin#
```

debug stp show counter

Purpose	Used to show the STP counters.
Syntax	debug stp show counter { ports [< portlist > all] }
Description	This command used to display the STP counters.
Parameters	<i>ports <portlist></i> - Specifies the STP ports for display.. <i>all</i> - Display all port's counters If no parameter is specified, display the global counters.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To show the STP counters for port 9:


```
DGS-3450:admin#debug stp show counter ports 9
```

```
Command: debug stp show counter ports 9
```

STP Counters

```
-----
Port 9 :
Receive:
Total STP Packets      :32
Configuration BPDU    :0
TCN BPDU              :0
RSTP TC-Flag          :15
RST BPDU              :32

Transmit:
Total STP Packets      :32
Configuration BPDU    :0
TCN BPDU              :0
RSTP TC-Flag          :7
RST BPDU              :32

Discarded:
Total Discard BPDU    :0
Global STP Disable    :0
Port STP Disabled     :0
Invalid Packet Format  :0
Invalid Protocol      :0
Config BPDU Length    :0
TCN BPDU Length       :0
RST BPDU Length       :0
Invalid Type          :0
Invalid Timers        :0
Success.
```

```
DGS-3450:admin#
```

debug stp clear counter

Purpose	Used to clear STP counters.
Syntax	debug stp clear counter [ports < portlist > all]
Description	This command used to clear the STP counters.
Parameters	<i>ports <portlist></i> - Specifies the port range. <i>all</i> - Clears all port counters.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To clear all STP counters on the switch:

```
DGS-3450:admin#debug stp clear counter all
```

```
Command : debug stp clear counter all
```

```
Success.
```

```
DGS-3450:admin#
```

debug stp state

Purpose	Used to configure the STP debug state.
Syntax	debug stp state [enable disable]
Description	This command is used to enable or disable the STP debug state.

debug stp state

Parameters	<i>state</i> - See below: <i>enable</i> - Enable the STP debug state. <i>disable</i> - Disable the STP debug state.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the STP debug state to enable, and then disable the STP debug state:

```
DGS-3450:admin#debug stp state enable
Command: debug stp state enable

Success.

DGS-3450:admin# debug stp state disable
Command: debug stp state disable

Success.

DGS-3450:admin#
```

IGMP SNOOPING MULTICAST (ISM) VLAN COMMANDS

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

Command	Parameters
create igmp_snooping multicast_vlan	<vlan_name 32> <vlanid 2-4094> { remap_priority [<value 0-7> none] { replace_priority } }
config igmp_snooping multicast_vlan	<vlan_name 32> { member_port <portlist> [source_port <portlist> untag_source_port <portlist>] tag_member_port <portlist> state [enable disable] replace_source_ip <ipaddr> remap_priority[<value 0-7> none] {replace_priority}}
config igmp_snooping multicast_vlan_group	<vlan_name 32> [add <mcast_address_list> delete <mcast_address_list> delete_all]
show igmp_snooping multicast_vlan_group	{< vlan_name 32> }
delete igmp_snooping multicast_vlan	<vlan_name 32>
show igmp_snooping multicast_vlan	{<vlan_name 32>}

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

create igmp_snooping multicast_vlan

Purpose	Used to create a multicast VLAN.
Syntax	create igmp_snooping multicast_vlan <vlan_name 32> <vlanid 2-4094> { remap_priority [<value 0-7> none] { replace_priority } }
Description	<p>The create igmp_snooping command creates a multicast VLAN and implements relevant parameters as specified. More than one multicast VLANs can be configured. The maximum number of configurable VLANs is project dependent.</p> <p>Newly created IGMP snooping must use a unique VLAN ID and name, i.e. they cannot use the VLAN ID or name of any existing 802.1q VLAN.</p> <p>Also keep in mind the following conditions:</p> <ul style="list-style-type: none"> • Multicast VLANs cannot be configured or displayed using 802.1Q VLAN commands. • An IP interface cannot be bound to a multicast VLAN. • The multicast VLAN snooping function co-exists with the 802.1q VLAN snooping function.
Parameters	<p><i>vlan_name</i> - The name of the multicast VLAN to be created. Each multicast VLAN is given a name that can be up to 32 characters.</p> <p><i>vlanid</i> - The VLAN ID of the multicast VLAN to be created. The range is 2 - 4094.</p> <p><i>remap_priority</i> - The remap priority (0 to 7) to be associated with the data traffic to be forwarded on the multicast VLAN. If none is specified, the packet's original priority will be used. The default setting is none.</p> <p><i>replace_priority</i> - Specify that packet's priority will be changed by the switch, based on the remap priority. This flag will only take effect when the remap priority is set.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create an IGMP snooping multicast VLAN with the VLAN name mv1 and the VID 2:

```
DGS-3450:admin# create igmp_snoop multicast_vlan mv1 2
Command: create igmp_snooping multicast_vlan mv1 2

Success.

DGS-3450:admin#
```

config igmp_snooping multicast_vlan

Purpose	Used to configure the parameters of a specific IGMP snooping multicast VLAN.
Syntax	config igmp_snooping multicast_vlan <vlan_name 32> {member_port <portlist> [source_port <portlist> untag_source_port <portlist>] tag_member_port <portlist> state [enable disable] replace_source_ip <ipaddr> remap_priority [<value 0-7> none] {replace_priority}}
Description	<p>The config igmp_snooping multicast_vlan command allows you to add member ports and source ports to a list of multicast VLAN member ports. Member ports automatically become untagged members of the multicast VLAN and source ports automatically become tagged members of the multicast VLAN. If the port list of an existing multicast VLAN is changed without specifying add or delete, the newly added port list replaces the existing port list. A member port list cannot overlap with a source port list of the same multicast VLAN. However, member ports of one multicast VLAN are allowed to overlap with member ports on a different multicast VLAN.</p> <p>A multicast VLAN must first be created using the create igmp_snooping multicast_vlan command before the multicast VLAN can be configured.</p>
Parameters	<p><i>vlan_name</i> - The name of the multicast VLAN to be configured. Can be up to 32 characters.</p> <p><i>member_port</i> - A member port or range of member ports to be added to the multicast VLAN. The specified range of ports will become untagged members of the multicast VLAN.</p> <p><i>source_port</i> - A port or range of ports to be added to the multicast VLAN.</p> <p><i>untag_source_port</i> - Specify the source port or range of source ports as untagged members of the multicast VLAN. The PVID of the untagged source port is automatically changed to the multicast VLAN. Source ports must be either tagged or untagged for any single multicast VLAN, i.e. both types cannot be members of the same multicast VLAN.</p> <p><i>tag_member_port</i> - A member port or range of member ports to be added to the multicast VLAN. The specified range of ports will become tagged members of the multicast VLAN.</p> <p><i>state</i> - Used to specify if the multicast VLAN for a chosen VLAN should be enabled or disabled.</p> <p><i>replace_source_ip</i> - Before forwarding the report packet sent by the host, the source IP address in the join packet must be replaced by this IP address.</p> <p><i>remap_priority</i> - The remap priority value (0 to 7) to be associated with the data traffic to be forwarded on the multicast VLAN. If none is specified, the packet's original priority is used. The default setting is none.</p> <p><i>replace_priority</i> - Specify that the packet priority will be changed to the remap_priority, but only if remap_priority is set.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure an IGMP snooping multicast VLAN with the name "v1", make ports 1 and 3 members of the VLAN, and set the state to enable:

```
DGS-3450:admin# config igmp_snooping multicast_vlan v1 member_port 1:1,1:3 state enable
Command: config igmp_snooping multicast_vlan v1 member_port 1:1,1:3 state enable
Success.
```

```
DGS-3450:admin#
```

config igmp_snooping multicast_vlan_group

Purpose	Used to configure the IGMP multicast groups learned with the specified multicast VLAN.
Syntax	config igmp_snooping multicast_vlan_group <vlan_name 32> [add <mcast_address_list> delete <mcast_address_list> delete_all]
Description	Used to configure the multicast group learned with the specific multicast VLAN. The following two cases can be considered for examples: Case 1- The multicast group is not configured, multicast VLANs do not have any member ports overlapping and the join packet received by the member port is learned on only the multicast VLAN that this port is a member of. Case 2- The join packet is learned with the multicast VLAN that contains the destination multicast group. If the destination multicast group of the join packet cannot be classified into any multicast VLAN to which this port belongs, then the join packet will be learned on the natural VLAN of the packet.
Parameters	<i>vlan_name</i> - The name of the multicast VLAN to be configured. Each multicast VLAN is given a name of up to 32 characters. <i>add</i> - Used to associate a profile to a multicast VLAN. <i>delete</i> - Used to de-associate a profile from a multicast VLAN.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To add an IGMP snooping multicast vlan group to a multicast VLAN group with the name "v1":

```
DGS-3450:admin# config igmp_snooping multicast_vlan_group v1 add 239.1.1.1
Command: config igmp_snooping multicast_vlan_group v1 add 239.1.1.1
```

```
Success.
```

```
DGS-3450:admin#
```

show igmp_snooping multicast_vlan_group

Purpose	Used to show an IGMP snooping multicast VLAN group.
Syntax	show igmp_snooping multicast_vlan_group {< vlan_name 32> }
Description	The show igmp_snooping multicast_vlan_group command allows you to show the multicast VLAN groups.
Parameters	<vlan_name 32> - Specify the name of the multicast VLAN to be displayed.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To show all IGMP snooping multicast VLAN groups setup on the switch:

```
should be " DGS-3450:admin# show igmp_snooping multicast_vlan_group
Command: show igmp_snooping multicast_vlan_group
```

VLAN Name	VLAN ID	Multicast Group Profiles
-----	-----	-----
mod	8	test

Success.

DGS-3450:admin#

delete igmp_snooping multicast_vlan

Purpose	Used to delete an IGMP snooping multicast VLAN.
Syntax	delete igmp_snooping multicast_vlan <vlan_name 32>
Description	The delete igmp_snooping multicast_vlan command allows you to delete a multicast VLAN.
Parameters	<i>vlan_name</i> - The name of the multicast VLAN to be deleted.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete an IGMP snooping multicast VLAN called "v1":

```
DGS-3450:admin# delete igmp_snooping multicast_vlan v1
Command: delete igmp_snooping multicast_vlan v1
```

Success.

DGS-3450:admin#

show igmp_snooping multicast_vlan

Purpose	Used to display information for a multicast VLAN.
Syntax	show igmp_snooping multicast_vlan {<vlan_name 32>}
Description	The show igmp_snooping multicast_vlan command allows information for a specific multicast VLAN to be displayed.
Parameters	<i>vlan_name</i> - The name of the multicast VLAN to be shown.
Restrictions	None.

Example usage:

To display all IGMP snooping multicast VLANs:

```
DGS-3450:admin# show igmp_snooping multicast_vlan
```

```
Command: show igmp_snooping multicast_vlan
```

```
IGMP Multicast VLAN Global State      : Disabled
```

```
IGMP Multicast VLAN Forward Unmatched: Disabled
```

```
VLAN Name                               :test
```

```
VID                                      :100
```

```
Member(Untagged) Ports                  :1
```

```
Tagged Member Ports                     :
```

```
Source Ports                            :3
```

```
Untagged Source Ports                   :
```

```
Status                                  :Disabled
```

```
Replace Source IP                       : 0.0.0.0
```

```
Remap Priority                           :None
```

```
Total Entries: 1
```

```
DGS-3450:admin#
```

MULTIPLE SPANNING TREE PROTOCOL (MSTP) COMMANDS

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

Command	Parameters
show stp	
show stp instance	<value 0-15>
show stp ports	{<portlist>} {instance_id <0-15>}
show stp mst_config_id	
create stp instance_id	<value 1-15>
delete stp instance_id	<value 1-15>
config stp instance_id	<value 1-15> [add_vlan remove_vlan] <vidlist>
config stp mst_config_id	{name <string> revision_level <int 0-65535>}
enable stp	
disable stp	
config stp version	[mstp rstp stp]
config stp priority	<value 0-61440> instance_id <value 0-15>
config stp	{maxage <value 6-40> maxhops <value 1-40> hellotime <value 1-10> forwarddelay <value 4-30> txholdcount <value 1-10> fbpdu [enable(3) disable(2)] lbd [enable(1) disable(0)] lbd_recover_timer [<value 0> <value 60-1000000>] nni_bpdu_addr [dot1d dot1ad]}(1)
config stp ports	<portlist> {externalCost [auto <value 1-200000000>] hellotime <value 1-10> migrate [yes no] edge [true false auto] p2p [true false auto] state [enable disable] restricted_role [true false] restricted_tcn [true false] lbd [enable disable] fbpdu [enable disable]}(1)
config stp mst_ports	<portlist> instance_id <value 0-15> {internalCost [auto <value 1-200000000>] priority <value 0-240>}

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

show stp

Purpose	Used to show the bridge parameters global settings. (CIST or msti id=0)
Syntax	show stp
Description	The show stp command is used to show the bridge parameters global settings.
Parameters	None.
Restrictions	None.

Example usage:

To show stp:


```

DGS-3450:admin# show stp
Command: show stp

STP Bridge Global Settings
-----
STP Status          : Enabled
STP Version         : MSTP
Max Age             : 20
Forward Delay       : 15
Max Hops            : 20
TX Hold Count       : 3
Forwarding BPDU     : Enabled
LoopBack Detection  : Enabled
NNI BPDU Address    : dot1d

DGS-3450:admin#

```

show stp instance

Purpose	Used to show each instance parameters settings.
Syntax	show stp instance <value 0-15>
Description	This command displays each instance parameters settings. Value means the instance id, if there is no input of this value, all instance will be shown.
Parameters	<i>instance</i> - MSTP instance id . Instance 0 represents for default instance : CIST. The bridge support total 16 Instance (0-15) at most.
Restrictions	None.

Example usage:

To show stp instance:

```

DGS-3450:admin# show stp instance
Command: show stp instance

STP Instance Settings
-----
Instance Type           : CIST
Instance Status        : Enabled
Instance Priority       : 32768(Bridge Priority : 32768, SYS ID Ext : 0 )

STP Instance Operational Status
-----
Designated Root Bridge : 32768/00-22-22-22-22-00
External Root Cost     : 0
Regional Root Bridge   : 32768/00-22-22-22-22-00
Internal Root Cost     : 0
Designated Bridge      : 32768/00-22-22-22-22-00
Root Port              : None
Max Age                : 20
Forward Delay          : 15
Last Topology Change   : 2430
Topology Changes Count : 0

DGS-3450:admin#

```

show stp ports

Purpose	Used to show the port information includes parameters setting and operational value.
Syntax	show stp ports {<portlist>}
Description	This command displays each port's parameters settings. If not input the portlist, all ports will be shown . If there are multi instances on this bridge , the parameters of the port on different instances will be shown.
Parameters	<p><i>ports</i> - To show parameters of the designated port numbers , to be distinguish ed from showing parameters of the bridge.</p> <p><i>portlist</i> - One of CLI Value Type , restrict the input value and format of the ports, refer to section 1-4 Switch Numerical Ranges.</p> <p><i>instance_id</i> - specifies the stp instance id.</p>
Restrictions	None.

Example usage:

To show stp ports:

```
DGS-3450:admin# show stp ports
```

```
Command: show stp ports
```

MSTP Port Information

```
Port Index      : 1 , Hello Time: 2 / 2 , Port STP : Enabled , LBD : No
External PathCost : Auto/20000 , Edge Port : False/No , P2P : Auto /Yes
Port RestrictedRole : False, Port RestrictedTCN : False
```

Msti	Designated Bridge	Internal PathCost	Prio	Status	Role
0	N/A	200000		128 Disabled	Disabled
2	N/A	200000		128 Disabled	Disabled

```
DGS-3450:admin#
```

show stp mst_config_id

Purpose	Used to show the MST Configuration Identification.
Syntax	show stp mst_config_id
Description	Show the 3 elements of the MST configuration Identification, including: Configuration Name, Revision Level, and MST configuration Table. The default Configuration name is the MAC address of the bridge.
Parameters	<i>mst_config_id</i> - If two bridges has the same three elements in mst_config_id, that means they are in the same MST region.
Restrictions	None.

Example usage:

```
show stp mst_config_id:
```

```
DGS-3450:admin# show stp mst_config_id
```

```
Command: show stp mst_config_id
```

Current MST Configuration Identification

```
-----
Configuration Name : 00-22-22-22-22-00                      Revision Level :0
MSTI ID      Vid list
-----
CIST         1-4094
```

```
DGS-3450:admin#
```

create stp instance_id

Purpose	To create an MST Instance without mapping the corresponding VLANs yet.
Syntax	create stp instance_id <value 1-15>
Description	To create a new MST instance independent from the default Instance: CIST (Instance 0). After creating the MST instance, need to do the configuration of VLANs, or this newly created MST instance will still be in disable state.
Parameters	<i>instance_id</i> - MSTP instance id. Instance 0 represents for default instance, CIST. The DUT support 16 Instance (0-15) at most.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create mstp instance:

```
DGS-3450:admin# create stp instance_id 2
Command: create stp instance_id 2

Success.

DGS-3450:admin#
```

delete stp instance_id

Purpose	Used to delete MST Instance.
Syntax	delete stp instance_id <value 1-15>
Description	To delete the specified MST Instance . CIST (Instance 0) can not be deleted and only can delete one instance at a time.
Parameters	<i>instance_id</i> - MSTP instance id. Instance 0 represents for default instance, CIST. The DUT support 16 Instance (0-15) at most.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete mstp instance:

```
DGS-3450:admin# delete stp instance_id 2
Command: delete stp instance_id 2

Success.

DGS-3450:admin#
```

config stp instance_id

Purpose	To map or remove the VLAN range of the specified MST instance for the existed MST Instances.
Syntax	config stp instance_id <value 1-15> [add_vlan remove_vlan] <vidlist>
Description	There are 2 different action type to deal with an MST Instance. They are listed as follows: add_vlan: to map specified VLAN lists to an existed MST Instance . remove_vlan: to delete specified VLAN lists from an existed MST Instance.
Parameters	<i>instance_id</i> - MSTP instance id . Instance 0 represents for default instance, CIST. The DUT support 16 Instance (0-15) at most. <i>add_vlan</i> - Defined action type to configure an MST Instance. <i>remove_vlan</i> - Defined action type to configure an MST Instance. <i>vidlist</i> - Specifies a list of VLANs by VLAN ID.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To map vlan id to mstp instance:

```
DGS-3450:admin# config stp instance_id 2 add_vlan 1 to 3
Command: config stp instance_id 2 add_vlan 1 to 3

Success.

DGS-3450:admin#
```

To remove vlan id from mstp instance:

```
DGS-3450:admin# config stp instance_id 2 remove_vlan 2
Command: config stp instance_id 2 remove_vlan 2

Success.

DGS-3450:admin#
```

config stp mst_config_id

Purpose	Used to change the name or revision level of the MST configuration Identification.
Syntax	config stp mst_config_id {name <string> revision_level <int 0-65535>}
Description	To configure configuration name, revision level in the MST configuration Identification. The default configuration name is the MAC address of the bridge.
Parameters	<i>name</i> - The name given for a specified MST region. <i>revision_level</i> - The same given name with different revision level also represents for different MST region.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To change the name and revision level of the MST configuration Identification:

```
DGS-3450:admin# config stp mst_config_id name R&D_BlockG revision_level 1
Commands: config stp mst_config_id name R&D_BlockG revision_level 1

Success.

DGS-3450:admin#
```

enable stp

Purpose	Used to enable STP globally.
Syntax	enable stp
Description	May be we could modify to allow user enable stp per instance. But CIST should be enabled first before enable other instances. Current design is when user enable the CIST, all MSTIs will be enabled automatically if FORCE_VERSION is set to MSTP(3) and there is at least one vlan mapped to this instance.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable stp:

```
DGS-3450:admin# enable stp
Command: enable stp

Success.

DGS-3450:admin#
```

disable stp

Purpose	Used to disable STP globally.
Syntax	disable stp
Description	To disable STP functionality in every existed instance.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable stp:

```
DGS-3450:admin# disable stp
Command: disable stp

Success.

DGS-3450:admin#
```

config stp version

Purpose	Used to enable STP globally.
Syntax	config stp version [mstp rstp stp]
Description	If version is configured as stp or rstp, all currently running MSTIs should be disabled. For version is configured as mstp, current design is enabled all available MSTIs (assume that CIST is enabled). Further discussion needed to decide whether we let user to enable the MSTIs.
Parameters	<i>version</i> - To decide to run under which version of STP. <i>mstp</i> - Multiple Spanning Tree Protocol. <i>rstp</i> - Rapid Spanning Tree Protocol. <i>stp</i> - Spanning Tree Protocol.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To config stp version:

```
DGS-3450:admin# config stp version mstp
Command: config stp version mstp

Success.

DGS-3450:admin#
```

To config stp version with the same value of old configuration:

```
DGS-3450:admin# config stp version mstp
Command: config stp version mstp

Configure value is the same with current value.
Fail!

DGS-3450:admin#
```

config stp priority

Purpose	Used to configure the instance priority.
Syntax	config stp priority <value 0-61440> instance_id <value 0-15>
Description	One of the parameters used to select the Root Bridge.
Parameters	<i>priority</i> - The bridge priority value must be divisible by 4096. <i>instance_id</i> - Identifier to distinguish different STP instances.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To config stp instance_id:

```
DGS-3450:admin# config stp priority 61440 instance_id 0
Command: config stp priority 61440 instance_id 0

Success.

DGS-3450:admin#
```

config stp

Purpose	Used to configure the bridge management parameters for CIST (instance_id = 0).
Syntax	config stp {maxage <value 6-40> maxhops <value 1-40> hellotime <value 1-10> forwarddelay <value 4-30> txholdcount <value 1-10> fbpdu [enable(3) disable(2)] lbd [enable(1) disable(0)] lbd_recover_timer [<value 0> <value 60-1000000>] nni_bpdu_addr [dot1d dot1ad]}(1)
Description	This command is used to configure the bridge parameters global settings.
Parameters	<i>maxage</i> - Used to determine if a BPDU is valid. The default value is 20. <i>maxhops</i> - Used to restrict the forwarded times of one BPDU. The default value is 20. <i>forwarddelay</i> - The maximum delay time for one BPDU to be transmitted by a bridge and received from another bridge. The default value is 15. <i>txholdcount</i> - Used to restrict the numbers of BPDU transmitted in a time interval (per Hello Time). <i>fbpdu</i> - To decide if the Bridge will flood STP BPDU when STP functionality is disabled. <i>nni_bpdu_addr</i> - Used to determine the BPDU protocol address for STP in service provide site. It can use 802.1d STP address, 802.1ad service provider STP address or an user defined mutilcast address. The range of the user defined address is 0180C2000000 - 0180C2FFFFFF.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To config stp:

```
DGS-3450:admin# config stp maxage 25
Command: config stp maxage 25

Success.

DGS-3450:admin#
```

config stp ports

Purpose	Used to configure the ports management parameters only at CIST level.
Syntax	config stp ports <portlist> {externalCost [auto <value 1-20000000>] hellotime <value 1-10> migrate [yes no] edge [true false auto] p2p [true false auto] state [enable disable] restricted_role [true false] restricted_tcn [true false] lbd [enable disable] fbpdu [enable disable]}(1)
Description	This command can configure all the parameters of ports, except for Internal Path Cost and Port Priority.
Parameters	<p><i>portlist</i> - One of CLI Value Type , restrict the input value and format of the ports, refer to section 1-4 Switch Numerical Ranges.</p> <p><i>external_cost</i> - The path cost between MST regions from the transmitting Bridge to the CIST Root Bridge. It is only used at CIST level.</p> <p><i>hellotime</i> - The default value is 2 . This is a per-Bridge parameter in RSTP, but it becomes a per-Port parameter in MSTP.</p> <p><i>migrate</i> - Operation of management in order to specify the port to send MSTP BPDU for a delay time.</p> <p><i>edge</i> - To decide if this port is connected to a LAN or a Bridged LAN. In auto mode, the bridge will delay for a period to become edge port if no bridge BPUD is received. The default is auto mode.</p> <p><i>p2p</i> - To decide if this port is in Full-Duplex or Half-Duplex mode.</p> <p><i>state</i> - To decide if this port supports the STP functionality.</p> <p><i>restricted_role</i> - To decide if this port not to be selected as Root Port. The default value is false.</p> <p><i>restricted_tcn</i> - To decide if this port not to propagate topology change. The default value is false.</p> <p><i>fbpdu</i> - To decide if this port will flood STP BPDU when STP functionality is disabled. When the state is set to enable, the received BPDU will be forwarded. When the state is set to disable, the received VPDU will be dropped.</p> <p><i>hw_filtering</i> is an option that is only required by some legacy chipset which cannot support per L2 protocol packet control. When the state is set to hw_filtering, if STP BPDU is received by this port, the port will be changed to BPDU hardware filtering mode such that all layer 2 control packets will be dropped by hardware. The default state is disable.</p> <p><i>recover_hw_filtering</i> - When a port is in BPDU hardware filtering mode, it can be recovered by this option.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To config stp ports:

```
DGS-3450:admin# config stp ports 1 external_cost auto
Command: config stp ports 1 external_cost auto

Success.

DGS-3450:admin#
```


config stp mst_ports

Purpose	Used to configure the ports management parameters at CIST (instance_id = 0) or MSTI (instance_id = 1) level.
Syntax	config stp mst_ports <portlist> instance_id <value 0-15> {internalCost [auto <value 1-200000000>] priority <value 0-240>}
Description	Internal Path Cost and Port Priority of a Port in MSTI can be separately configured to different values from the configuration of CIST (instance_id = 0).
Parameters	<p><i>mst_ports</i> - To be distinguished from the parameters of ports only at CIST level.</p> <p><i>portlist</i> - One of CLI Value Type , restrict the input value and format of the ports, refer to section 1-4 Switch Numerical Ranges.</p> <p><i>instance_id</i> - Instance = 0 represents for CIST , Instance from 1 to 15 represents for MSTI 1 - MSTI 15.</p> <p><i>internalCost</i> - Port Path Cost used in MSTP.</p> <p><i>priority</i> - Port Priority.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To config stp mst_ports:

```
DGS-3450:admin# config stp mst_ports 1 instance_id 0 internal_cost auto
Command: config stp mst_ports 1 instance_id 0 internal_cost auto
```

Success.

```
DGS-3450:admin#
```

NETWORK LOAD BALANCING (NLB) COMMANDS

The NLB indicates the Network Load Balancing: it is a MAC forwarding control for supporting Microsoft's Network Load Balancing technique.

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

Command	Parameters
create nlb multicast_fdb	[<vlan_name 32> vlanid <vlanid>] <macaddr>
delete nlb multicast_fdb	[<vlan_name 32> vlanid <vlanid>] <macaddr>
config nlb multicast_fdb	[<vlan_name 32> vlanid <vlanid>] <macaddr> [add delete] <portlist>
show nlb fdb	

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

create nlb multicast_fdb

Purpose	Use to create the switch's NLB multicast FDB entry.
Syntax	create nlb multicast_fdb [<vlan_name 32> vlanid <vlanid>] <macaddr>
Description	<p>The create nlb multicast_fdb command creates a NLB multicast FDB entry. The number of supported entries is project dependent.</p> <p>The network load balancing command set is used to support the Microsoft server load balancing application where multiple servers can share the same IP address and MAC address. The requests from clients will be forwarded to all servers, but will only be processed by one of them. The server can work in multicast mode. In multicast mode, the client use the multicast MAC address as the destination MAC to reach the server. Regarding of the mode, this destination Mac is the named the shared MAC. The server uses its own MAC address (rather than the shared MAC) as the source MAC address of the reply packet.</p> <p>The NLB multicast FDB entry will be mutual exclusive with the L2 multicast entry.</p>
Parameters	<p><i>vlan_name</i> - Specify the VLAN of the NLB multicast FDB entry to be created.</p> <p><i>vlanid <vlanid></i> - Specify the VLAN by the VLAN ID.</p> <p><i><macaddr></i> - Specify the MAC address of the NLB multicast FDB entry to be created.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create a NLB multicast FDB entry:

```
DGS-3450:admin# create nlb multicast_fdb default 03-bf-01-01-01-01
Command: create nlb multicast_fdb default 03-bf-01-01-01-01
Success.
DGS-3450:admin#
```

delete nlb multicast_fdb

Purpose	Use to delete the switch's NLB multicast FDB entry.
Syntax	delete nlb multicast_fdb [<vlan_name 32> vlanid <vlanid>] <macaddr>
Description	The delete nlb multicast_fdb command is used to delete the NLB multicast FDB entry.

delete nlb multicast_fdb

Parameters	<p><i><vlan_name 32></i> - Specify the VLAN of the NLB multicast FDB entry to be deleted.</p> <p><i>vlanid <vlanid></i> - Specify the VLAN by VLAN ID.</p> <p><i><macaddr></i> - Specify the MAC address of the NLB multicast FDB entry to be deleted.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete NLB multicast FDB entry:

```
DGS-3450:admin# delete nlb multicast_fdb default 03-bf-01-01-01-01
Command: delete nlb multicast_fdb default 03-bf-01-01-01-01
Success.
DGS-3450:admin#
```

config nlb multicast_fdb

Purpose	Use to configure the switch's NLB multicast FDB entry.
Syntax	config nlb multicast_fdb [<i><vlan_name 32></i> <i>vlanid <vlanid></i>] <i><macaddr></i> [add delete] <i><portlist></i>
Description	The config nlb multicast_fdb command is used to add or delete the forwarding ports for the specified NLB multicast FDB entry.
Parameters	<p><i>vlan_name</i> - Specify the VLAN of the NLB multicast FDB entry to be configured.</p> <p><i>vlanid <vlanid></i> - Specify the VLAN by the VLAN ID.</p> <p><i><macaddr></i> - Specify the Mac address of the NLB multicast FDB entry to be configured.</p> <p><i>add <portlist></i> - Specify a list of forwarding ports to be added.</p> <p><i>delete <portlist></i> - Specify a list of forwarding ports to be removed.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure NLB multicast MAC forwarding database:

```
DGS-3450:admin# config nlb multicast_fdb default 03-bf-01-01-01-01 add 1:1-1:5
Command: config nlb multicast_fdb default 03-bf-01-01-01-01 add 1:1-1:5
Success.
DGS-3450:admin#
```

show nlb fdb

Purpose	Used to show NLB configured entry.
Syntax	show nlb fdb
Description	The show nlb fdb command is used to show the NLB Configured entry.
Parameters	None.
Restrictions	None.

Example usage:

To display the NLB forwarding table:

```
DGS-3450:admin# show nlb fdb
```

```
Command: show nlb fdb
```

MAC Address	VLAN ID	Egress Ports
03-bf-01-01-01-01	100	1:1-1:5,1:26,2:26
03-bf-01-01-01-01	1	1:1-1:5,1:26,2:26

```
Total Entries : 2
```

```
DGS-3450:admin#
```

PASSWORD ENCRYPTION COMMANDS

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

Command	Parameters
enable password encryption	
disable password encryption	
create account	[admin operator user] <username 15>
config account	<username> {encrypt [plain_text sha_1] <password>}
show account	
delete account	<username>

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

enable password encryption

Purpose	Used to create user accounts.
Syntax	enable password encryption
Description	The user account configuration information will be stored in the configuration file, and can be applied to the system later. If the password encryption is enabled, the password will be in encrypted form.
Parameters	None.
Restrictions	Only Administrator users can issue this command.

Example usage:

To enable the password encryption:

```
DGS-3450:admin# enable password encryption
Command: enable password encryption

Success.

DGS-3450:admin#
```

disable password encryption

Purpose	Used to create user accounts
Syntax	disable password encryption
Description	The user account configuration information will be stored in the configuration file, and can be applied to the system later. When password encryption is disabled, if the user specifies the password in plain text form, the password will be in plan text form. However, if the user specifies the password in encrypted form, or if the password has been converted to encrypted form by the last enable password encryption command, the password will still be in the encrypted form. It can not be reverted to the plaintext.

disable password encryption

Parameters	None.
Restrictions	Only Administrator users can issue this command.

Example usage:

To disable the password encryption:

```
DGS-3450:admin# disable password encryption
Command: disable password encryption

Success.

DGS-3450:admin#
```

create account

Purpose	Used to create user accounts.
Syntax	create account [admin operator] user <username 15>
Description	The create account command creates user accounts. The username is between 1 and 15 characters, the password is between 0 and 15 characters. It is case sensitive. The number of account (include admin and user) is up to 8.
Parameters	<i>admin <username 15></i> - Name of the admin account. <i>user <username 15></i> - Name of the user account. <i>operator <username 15></i> - Name for a operator user account.
Restrictions	Only Administrator users can issue this command.

Example usage:

To create the admin-level user "dlink":

```
DGS-3450:admin# create account admin dlink
Command: create account admin dlink

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

DGS-3450:admin#
```

config account

Purpose	Used to configure user accounts.
Syntax	config account <username> {encrypt [plain_text] sha_1} <password>
Description	When the password information is not specified in the command, the system will prompt the user to input the password interactively. For this case, the user can only input the plain text password. If the password is present in the command, the user can select to input the password in the plain text form or in the encrypted form. The encryption algorithm is based on SHA-1.
Parameters	<i><username></i> - Name of the account. The account must already be defined. <i>plain_text</i> - Select to specify the password in plain text form.

config account

sha_1 - Select to specify the password in the SHA-1 encrypted form.

<password> - The password for the user account. The length for of password in plain-text form and in encrypted form are different. For the plain-text form, passwords must have a minimum of 0 character and can have a maximum of 15 characters. For the encrypted form password, the length is fixed to 35 bytes long. The password is case-sensitive.

Restrictions

Only Administrator users can issue this command.

Example usage:

To configure the user password of “dlink” account:

```
DGS-3450:admin# config account dlink
Command: config account dlink

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

DGS-3450:admin#
```

To configure the user password of “dlink” account:

```
DGS-3450:admin# config account administrator
Command: config account administrator encrypt sha_1 *@&cRDtpNCeBiq15KOQsKVyrA0sAiCIZQwq
Success.

DGS-3450:admin#
```

show account

Purpose	Used to display user accounts.
Syntax	show account
Description	The show account command displays user accounts that have been created.
Parameters	None.
Restrictions	Only Administrator users can issue this command.

Example usage:

To display the accounts that have been created:

```
DGS-3450:admin# show account
```

```
Command: show account
```

```
Current Accounts:
```

```
Username          Access Level
```

```
-----
```

```
System           User
```

```
dlink            Admin
```

```
Total Entries : 2
```

```
DGS-3450:admin#
```

delete account

Purpose	Used to delete an existing account.
Syntax	delete account <username>
Description	The delete account command deletes an existing account.
Parameters	<username> - Name of the user who will be deleted.
Restrictions	Only Administrator users can issue this command.

Example usage:

To delete the user account "System":

```
DGS-3450:admin# delete account System
```

```
Command: delete account System
```

```
Success.
```

```
DGS-3450:admin#
```


PASSWORD RECOVERY COMMANDS

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

Command	Parameters
reset config	{force_agree(1)}
reboot	{force_agree(1)}
reset account	
reset password	{<username>}
show account	

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

reset config

Purpose	Used to reset the configuration.
Syntax	reset config {force_agree(1)}
Description	Used to reset the configuration.
Parameters	<i>force_agree</i> – Specify to forcibly agree with the command.
Restrictions	This command is only available in password recovery mode.

Example usage:

To reset the configuration:

```
DGS-3450:admin# reset config
Command: reset config

Are you sure to proceed with reset config?(y/n) y
Success.
DGS-3450:admin#
```

reboot

Purpose	Used to exit Reset Configuration Mode and restart the switch.
Syntax	reboot {force_agree(1)}
Description	The reboot command exit Reset Configuration Mode and restart the switch. And it pops out a confirmation message to save the current setting.
Parameters	<i>force_agree</i> – Specify to forcibly agree with the command.
Restrictions	This command is only available in password recovery mode.

Example usage:

To exit Reset Configuration Mode and restart the switch:

```
DGS-3450:admin# reboot
Command: reboot

Save current setting before system restart?(y/n)

Please wait, the switch is rebooting...
```

reset account

Purpose	Used to delete the created account.
Syntax	reset account
Description	The reset account command deletes all of the created user accounts.
Parameters	None.
Restrictions	This command is only available in password recovery mode.

Example usage:

To delete the created account:

```
DGS-3450:admin# reset account
Command: reset account

Success
```

reset password

Purpose	Used to reset the password for user account.
Syntax	reset password {<username>}
Description	The reset password command resets the password of the specified user to empty. If username is not specified, password of all users will be reset.
Parameters	<username> - Specify to enter an existing username.
Restrictions	This command is only available in password recovery mode.

Example usage:

To reset the password for user account:

```
DGS-3450:admin# reset password
Command: reset password

Success
DGS-3450:admin#
```

show account

Purpose	Used to show the created account.
Syntax	show account

show account

Description	The show account command display all already created accounts.
Parameters	None.
Restrictions	This command is only available in password recovery mode.

Example usage:

To show the created account:

```
DGS-3450:admin# show account
```

```
Command: show account
```

```
DGS-3450:admin# show account
```

```
Command: show account
```

```
Current Accounts:
```

Username	Access Level	Password
-----	-----	-----
admin1	Admin	
user1	User	*****

```
Total Entries : 2
```

PING COMMANDS

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

Command	Parameters
ping	[<ipaddr> <domain_name 255>] {times <value 1-255> timeout <sec 1-99> source_ip <ipaddr>}
ping6	<ipv6addr> {times <value 1-255> size <value 1-6000> timeout <sec 1-99> source_ip <ipv6addr>}
enable broadcast_ping_reply	
disable broadcast_ping_reply	
show broadcast_ping_reply	

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

ping

Purpose	Used to test the connectivity between network devices.
Syntax	ping [<ipaddr> <domain_name 255>] {times <value 1-255> timeout <sec 1-99> source_ip <ipaddr>}
Description	The ping command sends Internet Control Message Protocol (ICMP) echo messages to a remote IP address. The remote IP address will then “echo” or return the message. This is used to confirm connectivity between the switch and the remote device.
Parameters	<p><i>ipaddr</i> - Specify the IP address of the host.</p> <p><i>domain_name</i> - Specify the domain name of the host.</p> <p><i>times</i> - The number of individual ICMP echo messages to be sent. A value of 0 will send an infinite number of ICMP echo messages. The maximum value is 255. The default is 0, indicating infinity. Press "CTRL+C" to terminate the ping test.</p> <p><i>timeout</i> - Specify 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.</p> <p><i>source_ip</i> - Specify the source IP address of the ping packets. If specified, , this IP address will be used as the packets' source IP address that ping sends to the remote host.</p>
Restrictions	None.

Example usage:

To send ICMP echo message to “10.51.17.1” for 4 times:

```
DGS-3450:admin# ping 10.51.17.1 times 4
Command: ping 10.51.17.1 times 4

Reply from 10.51.17.1, time<10ms
Reply from 10.51.17.1, time<10ms
Reply from 10.51.17.1, time<10ms
Reply from 10.51.17.1, time<10ms

Ping Statistics for 10.51.17.1
Packets: Sent =4, Received =4, Lost =0

DGS-3450:admin#
```

To use the host domain name for the ping command to test the network connectivity. When the 4th response has been received, press “CTRL+C” to terminate the ping:

```
DGS-3450:admin# ping www.dlink.com
Command: ping www.dlink.com

Reply from 207.232.83.10, time<10ms
Reply from 207.232.83.10, time<10ms
Reply from 207.232.83.10, time<10ms
Reply from 207.232.83.10, time<10ms

Ping Statistics for 207.232.83.10
Packets: Sent =4, Received =4, Lost =0

DGS-3450:admin#
```

To send ICMP echo message with source IP address “10.51.17.8” to “10.51.17.2” for 3 times (the Switch’s IP address is 10.51.17.8):

```
DGS-3450:admin# ping 10.51.17.2 times 3 source_ip 10.51.17.8
Command: ping 10.51.17.2 times 3 source_ip 10.51.17.8

Reply from 10.51.17.2, time<10ms
Reply from 10.51.17.2, time<10ms
Reply from 10.51.17.2, time<10ms

Ping Statistics for 10.51.17.2
Packets: Sent =3, Received =3, Lost =0

DGS-3450:admin#
```

ping6

Purpose	Used to test the IPv6 connectivity between network devices.
Syntax	ping6 <ipv6addr> {times <value 1-255> size <value 1-6000> timeout <sec 1-99> source_ip <ipv6addr>}
Description	The ping6 command sends IPv6 Internet Control Message Protocol (ICMP) echo messages to a remote IPv6 address. The remote IPv6 address will then “echo” or return the message. This is used to confirm the IPv6 connectivity between the switch and the remote device.
Parameters	<ipv6addr> - Specify the IPv6 address of the host. times - Specify the number of individual ICMP echo messages to be sent. A value of 0 will send an infinite ICMP echo messages. The maximum value is 255. The default is 0, indicating infinity. Press “CTRL+C” to terminate the ping test.

ping6

size - Specify the size of the test packet.

timeout - Specify the time-out period while waiting for a response from the remote device. A value of 1 to 10 seconds can be specified. The default is 1 second.

source_ip - Specify the source IPv6 address of the ping packets. If specified, , the IPv6 address will be used as the packets' source IPv6 address that ping6 sends to the remote host.

Restrictions

None.

Example usage:

To send ICMP echo message to "3000::1" for 4 times:

```
DGS-3450:admin# ping6 3000::1 times 4
Command: ping6 3000::1 times 4

Reply from 3000::1, bytes=200, time<10ms
Reply from 3000::1, bytes=200, time<10ms
Reply from 3000::1, bytes=200, time<10ms
Reply from 3000::1, bytes=200, time<10ms

Ping Statistics for 3000::1
Packets: Sent =4, Received =4, Lost =0

DGS-3450:admin#
```

To send ICMP echo message with source IPV6 address "3000::11" to "3000::1" for 3 times (the Switch's IP address are 3000::11 and 3000::10):

```
DGS-3450:admin# ping6 3000::1 times 3 source_ip 3000::11
Command: ping6 3000::1 times 3 source_ip 3000::11

Reply from 3000::1, bytes=200, time<10ms
Reply from 3000::1, bytes=200, time<10ms
Reply from 3000::1, bytes=200, time<10ms

Ping Statistics for 3000::1
Packets: Sent =4, Received =4, Lost =0

DGS-3450:admin#
```

enable broadcast_ping_reply

Purpose	Used to enable the broadcast ping reply state.
Syntax	enable broadcast_ping_reply
Description	The device will reply to the broadcast ping request.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable the broadcast ping reply state:

```
DGS-3450:admin# enable broadcast_ping_reply
Command: enable broadcast_ping_reply

Success.

DGS-3450:admin#
```

disable broadcast_ping_reply

Purpose	Used to disable the broadcast ping reply state.
Syntax	disable broadcast_ping_reply
Description	The device won't reply to the broadcast ping request.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable the broadcast ping reply state:

```
DGS-3450:admin# disable broadcast_ping_reply
Command: disable broadcast_ping_reply

Success.

DGS-3450:admin#
```

show broadcast_ping_reply

Purpose	Used to show the broadcast ping reply state.
Syntax	show broadcast_ping_reply
Description	Show the device broadcast ping reply state.
Parameters	None.
Restrictions	None.

Example usage:

To show the broadcast ping reply state:

```
DGS-3450:admin# show broadcast_ping_reply
Command: show broadcast_ping_reply

Broadcast Ping Reply State: Enabled

DGS-3450:admin#
```

PORT SECURITY COMMANDS

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

Command	Parameters
config port_security ports	[<portlist> all] {admin_state [enable disable] max_learning_addr <max_lock_no 0-64> lock_address_mode [permanent delete ontimeout deleteonreset]}(1)
delete port_security_entry vlan_name	<vlan_name 32> port <port> mac_address <macaddr>
clear port_security_entry port	<portlist>
show port_security	{ports <portlist>}

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

config port_security

Purpose	This command is used to set the port level port security setting.
Syntax	config port_security ports [<portlist> all] {admin_state [enable disable] max_learning_addr <max_lock_no 0-64> lock_address_mode [permanent delete ontimeout deleteonreset]}(1)
Description	This command configures admin state, maximum learning address and lock address mode. There are four levels of limitations on the learned entry number, for the entire system, for a port, for a VLAN, and for specific VLAN on a port. If any limitation is exceeded, the new entry will be discarded.
Parameters	<p><i>portlist</i> - Specifies a range of ports to be configured.</p> <p><i>all</i> - Specifies that all ports will be configured.</p> <p><i>admin_state</i> - Specifies to enable/disable the port security function on the port. By default, the setting is disabled.</p> <p><i>max_learning_addr</i> - Specifies the maximum of port security entries that can be learned on this port. If the value is set to 0, it means that no user can get authorized by port security function on this port. If the setting is smaller than the number of current learned entries on the port, the command will be rejected. The default value is 1.</p> <p><i>lock_address_mode</i> - Indicates the mode of locking address. The default mode is deleteonreset.</p> <p><i>permanent</i> - The address will never be deleted unless the user removes it manually or the VLAN of the entry is removed or the port is removed from the VLAN, or port security is disabled on the port where the address resides..</p> <p><i>deleteontimeout</i> - This entry will be removed if it's idle for the ageing time.</p> <p><i>deleteonreset</i> - This address will be removed if the switch is reset or reboots. The cases under which the permanent entries are deleted also apply to the deleteonreset entries,</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To config port security setting:


```
DGS-3450:admin# config port_security ports 1:6 admin_state enable max_learning_addr 10
lock_address_mode Permanent
Command: config port_security ports 1:6 admin_state enable max_learning_addr 10
lock_address_mode Permanent

Success.

DGS-3450:admin#
```

delete port_security_entry vlan_name

Purpose	Used to delete a port security entry.
Syntax	delete port_security_entry vlan_name <vlan_name 32> port <port> mac_address <macaddr>
Description	Used to delete a port security entry.
Parameters	<i><vlan_name></i> - Specifies the VLAN by VLAN name. <i>mac_address</i> - Specifies the MAC address of the entry.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete a port security entry:

```
DGS-3450:admin# delete port_security_entry vlan_name default port 1 mac_address 00-01-30-10-2C-C7
Command: delete port_security_entry vlan_name default port 1 mac_address 00-01-30-10-2C-C7

Success.

DGS-3450:admin#
```

clear port_security_entry port

Purpose	Used to clear the MAC entries learned by the port security function.
Syntax	clear port_security_entry port <portlist>
Description	Used to clear the MAC entries learned by the port security function.
Parameters	<i><portlist></i> - Specifies a range of ports to be configured. The port-security entries learned on the specified port will be cleared.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To clear port security entry by port(s):

```
DGS-3450:admin# clear port_security_entry port 1:6
Command: clear port_security_entry port 1:6

Success.

DGS-3450:admin#
```

show port_security

Purpose	This command is to used to display port security configuration.
Syntax	show port_security {ports <portlist>}
Description	The show port_security command displays the port security related information.
Parameters	<portlist> - Specifies a range of ports to show their configuration.
Restrictions	None.

Example usage:

To display the port security configuration:

```
DGS-3450:admin# show port_security
Command: show port_security

Port      Admin State  Max. Learning Addr.  Lock Address Mode
-----
1:1       Disabled    1                    DeleteOnReset
1:2       Disabled    1                    DeleteOnReset
1:3       Disabled    1                    DeleteOnReset
1:4       Disabled    1                    DeleteOnReset
1:5       Disabled    1                    DeleteOnReset
1:6       Disabled    1                    DeleteOnReset
1:7       Disabled    1                    DeleteOnReset
1:8       Disabled    1                    DeleteOnReset
1:9       Disabled    1                    DeleteOnReset
```

POWER OVER ETHERNET (POE) COMMANDS

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

Command	Parameters
config poe system	{[units <unitlist> all]} {power_limit <value m-n> power_disconnect_method [deny_next_port deny_low_priority_port] legacy_pd [enable disable]}
config poe ports	[all <portlist>] {state [enable disable] [time_range <range_name 32> clear_time_range] priority [critical high low] power_limit [class_0 class_1 class_2 class_3 user_define <value m - n>]}
show poe system	{units <unitlist>}
show poe ports	{<portlist>}

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

config poe system

Purpose	Used to configure the parameters for the POE system-wise function.
Syntax	config poe system {[units <unitlist> all]} {power_limit <value m-n> power_disconnect_method [deny_next_port deny_low_priority_port] legacy_pd [enable disable]}
Description	Configure the parameters for the whole PoE system.
Parameters	<p><i>units</i> - Specified the units that will be configured. If no specified units, all supported PoE units in the system will be configured.</p> <p><i>power_limit</i> - Configure the power budget of PoE system. The range of value which can be specified is determined by the system. Normally, the minimum setting is 37 W and the maximum setting is 370 W. The actual range will depend on power supply capability.</p> <p><i>power_disconnect_method</i> - Configure the disconnection method that will be used when the power budget is running out. When the system attempts to supply power to a new port, if the power budget is insufficient to do this, PoE controller will initiate port disconnection procedure to prevent overloading the power supply. The controller uses one of the following two ways to perform the disconnection procedure.</p> <p><i>deny_next_port</i> - The port with max port number will be denied regardless of its priority. Note: that if the disconnect_method is set to deny_next_port, then the power provision will not utilize the system's maximum power. There is a 19W safe margin. That is, when the system has only 19W remaining, this power cannot be utilized.</p> <p><i>deny_low_priority_port</i> - If there are ports that have been supplied power that have a priority lower than the new port, the port with the lowest priority will be disconnected. This process will stop until enough power is released for the new port. Note: that if the disconnect_method is set to deny_low_priority_port, then the power provision can utilize the system's maximum power.</p> <p><i>legacy_pd</i> - Configure legacy PDs detection status, enable for support, if set to disable, can't detect legacy PDs signal.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To config PoE system-wise was setting:

```
DGS-3450:admin# config poe system power_limit 250 power_disconnect_method
deny_low_priority_port
Command: config poe system power_limit 250 power_disconnect_method deny_low_priority_port

Success.

DGS-3450:admin#
```

config poe ports

Purpose	Used to configure the PoE port settings.
Syntax	config poe ports [all <portlist>] {state [enable disable] [time_range <range_name 32> clear_time_range] priority [critical high low] power_limit [class_0 class_1 class_2 class_3 user_define <value m - n>]}
Description	Configure the PoE port settings.
Parameters	<p><i>portlist</i> - Specified the list of ports whose setting is under configuration.</p> <p><i>all</i> - Specifies that all ports will be used.</p> <p><i>state</i> - When the state is set to disable, power will not be supplied to the powered device connected to this port.</p> <p><i>time_range</i> - Specifies the time range that applies to the port of the POE. If time range is configured, the power can only be supplied during the period specified by time range.</p> <p><i>clear_time_range</i> - Remove the time range.</p> <p><i>priority</i> - Port priority determines the priority the system attempts to supply the power to port. There are three levels of priority that can be selected, critical, high, and low. When multiple ports happen to have the same level of priority, the port ID will be used to determine the priority. The lower port ID has higher priority. The setting of priority will affect the ordering of supplying power. Whether the disconnect_method is set to deny_low_priority_port, priority of port will be used by the system to manage to supply power to ports.</p> <p><i>power_limit</i> - Configure the per-port power limit. If a port exceeds its power limit, it will be shut down.</p> <p>Based on 802.3af, there are 5 kinds of PD classes, class 0, class 1, class 2, and class 3. The power consumption ranges for them are 0.44~12.95W, 0.44~3.84W, 3.84~6.49W, 6.49~12.95W, and 12.95~ 29.5W, respectively.</p> <p>The five pre-defined settings are for users' convenience: The following is the power limit applied to the port for these four classes. For each class, the power limit is a little more than the power consumption range for the class. This takes the factor of the power loss on cable into account. Thus, the following are the typical values defined by the chip vendor.</p> <p>Class_0 : 15400mW class_1 : 4000mW class_2 : 7000mW clase_3 : 15400mW</p> <p>Other than these four pre-defined settings, users can directly specify any value that the chip supported, Normally, the minimum setting is 1000mW, and the maximum setting is 15400mW for 802.3af and >=35000mW for 802.3at.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Note: PD means powered device, for example, Web Cam, IP phone, wireless AP, etc.

PSE means power sourcing equipment, for example, our PoE switch.

Example usage:

To config PoE port:

```
DGS-3450:admin# config poe ports 1-4 state enable priority critical power_limit class_1
Command: config poe ports 1-4 state enable priority critical power_limit class_1

Power limit has been set to 4000mW (Class 1 PD upper power limit 3.84W + power loss on
cable).
Success.

DGS-3450:admin# config poe ports 5 state enable priority critical power_limit user_define
1000
Command: config poe ports 5 state enable priority critical power_limit user_define 1000

Power limit has been set to 1000mW.
Success.

DGS-3450:admin#
```

show poe system

Purpose	Used to display the setting and actual values of the whole PoE system.
Syntax	show poe system {units <unitlist>}
Description	Display the setting and actual values of the whole PoE system.
Parameters	<i>units</i> - Specified units that will be displayed. If no parameter specified, the system will display the status of all supported poe units in the systems.
Restrictions	None.

Example usage:

To display PoE system:

```
DGS-3450:admin# show poe system units 1
Command: show poe system units 1

Unit 1 PoE System Information
-----
Power Limit           : 250(watts)
Power Consumption     : 0(watts)
Power Remained        : 250(watts)
Power Disconnection Method : Deny Low Priority Port
Detection Legacy PD   : Disabled

If Power Disconnection Method is set to deny next port, then the system cannot utilize
its maximum power capacity. The maximum unused watt is 19W.

DGS-3450:admin#
```

show poe ports

Purpose	Used to display the setting and actual values of PoE port.
Syntax	show poe ports {<portlist>}
Description	Display the setting and actual values of PoE port.
Parameters	<i>portlist</i> - Specified a list of ports to be displayed. If no parameter specified, the system will display the status for all ports.

show poe ports

Restrictions None.

Example usage:

To display PoE port:

```
DGS-3450:admin# show poe ports 1-6
Command: show poe ports 1-6

Port  State      Priority  Power Limit(mW)  Time Range
      Class      Power(mW)  Voltage(decivolt)  Current(mA)
      Status
=====
1     Enabled    Critical  15400(Class 0)   Time_range_is_32_bytes____
      0          0          0                 0
      OFF   : Interim state during line detection
2     Enabled    Critical  4000(Class 1)
      0          8200       504               162
      ON    : 802.3af-compliant PD was detected
3     Enabled    Critical  7000(Class 2)
      0          0          0                 0
      OFF   : Interim state during line detection
4     Enabled    Critical  15400(Class 3)
      0          400        504               10
      ON    : 802.3af-compliant PD was detected
5     Enabled    Low       15400(User-defined)
      0          0          0                 0
      OFF   : Interim state during line detection
6     Enabled    Low       10000(User-defined)
      0          0          0                 0
      OFF   : Interim state during line detection

DGS-3450:admin#
```

PROTOCOL VLAN GROUP COMMANDS

For bridges that implement Port-and-Protocol-based VLAN classification, the VID associated with an Untagged or Priority-tagged Frame is determined based on the Port of arrival of the frame into the bridge and on the protocol identifier of the frame. If there is no protocol VLAN configured on the ingress port, all the untagged packets incoming on the port will be classified into PVID VLAN. This classification mechanism requires defining the protocol groups which specified frame type and protocol value to match for. A protocol group can be bound to a port and given a VLAN ID. If the incoming untagged packet matches the protocol group the VLAN ID will be assigned. A port can bind with multiple protocol groups. This allows untagged packets be classified into different VLANs based on packet content. The same protocol group can be assigned to multiple ports with different VLAN ID assigned, i.e. the same protocol can be given different VLAN ID through binding to different ports.

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

Command	Parameter
create dot1v_protocol_group	group_id <id>
config dot1v_protocol_group	group_id <id> [add delete] protocol [ethernet_2 ieee802.3_snap ieee802.3_llc] <protocol_value>
delete dot1v_protocol_group	group_id <id>
show dot1v_protocol_group	{group_id <id>}
config port dot1v	ports [<portlist> all] [add protocol_group group_id <id> [vlan <vlan_name 32> vlanid <vlanid>] delete protocol_group [group_id <id> all]]
show port dot1v	{ports <portlist>}

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

create dot1v_protocol_group

Purpose	Used to create a protocol group.
Syntax	create dot1v_protocol_group group_id <id>
Description	This command will create a protocol group. This group is to be configured using the config dot1v_protocol_group command where users may set the parameters for this group. After being configured, this group may be attached to a port or range of ports using the config port dot1v command.
Parameters	<i>group_id <id></i> – Enter an integer from 1 to 16 to identify the protocol VLAN group being created here.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create a protocol group:

```
DGS-3450:admin# create dot1v_protocol_group group_id 1
Command: create dot1v_protocol_group group_id 1

Success.

DGS-3450:admin#
```

config dot1v_protocol_group

Purpose	Used to configure the parameters for a protocol VLAN group.
Syntax	config dot1v_protocol_group group_id <id> [add delete] protocol [ethernet_2 ieee802.3_snap ieee802.3_llc] <protocol_value>
Description	This command will configure a protocol template for a group. Users may set the frame type to be added or deleted, along with the appropriate <i>protocol_value</i> in hexadecimal form. After being configured, this group may be attached to a port or range of ports using the config port dot1v command.
Parameters	<p><i>group_id <id></i> – Enter an integer from 1 to 16 to identify the protocol VLAN group being configured here.</p> <p><i>add delete</i> – Choose whether to add or delete the protocol to this group. This protocol is identified using the following <i>protocol</i> parameter.</p> <p><i>protocol</i> – Choose the appropriate frame type to be added to this group. This frame type will be identified by the switch by examining the packet header of incoming packets and matching it to the <i>protocol_value</i> stated here. This frame type must be followed by the correct <i>protocol_value</i>. The user has three choices:</p> <ul style="list-style-type: none"> • <i>ethernet_2</i> – Choose this parameter if you wish this protocol group to employ the Ethernet2 frame type. This frame type is identified by the 16-bit (2 octet) IEEE802.3 type field in the packet header, which is to be stated using the following <i>protocol_value</i>. • <i>ieee802.3_snap</i> – Choose this parameter if you wish this protocol group to employ the Sub Network Access Protocol (SNAP) frame type. This frame type is identified by the 16-bit (2 octet) IEEE802.3 type field in the packet header, which is to be stated using the following <i>protocol_value</i>. • <i>ieee802.3_llc</i> – Choose this parameter if you wish this protocol group to employ the Link Logical Control (LLC) frame type. This frame type is identified by the 2-octet IEEE802.3 Link Service Access Point (LSAP) pair field in the packet header, which is to be stated using the following <i>protocol_value</i>. The first octet defines the Destination Service Access Point value and the second octet is the Source Service Access Point (SSAP) value. <p><i><protocol_value></i> – Enter the corresponding protocol value of the protocol identified in the previous field. This value must be stated in a hexadecimal form.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure a protocol template:

```
DGS-3450:admin# config dot1v_protocol_group group_id 1 add protocol ethernet_2 86DD
Command: config dot1v_protocol_group group_id 1 add protocol ethernet_2 86DD

Success.

DGS-3450:admin#
```


delete dot1v_protocol_group

Purpose	Used to delete a protocol VLAN group.
Syntax	delete dot1v_protocol_group group_id <id>
Description	This command will delete a protocol VLAN group.
Parameters	<i>group_id <id></i> – Enter an integer from 1 to 16 to identify the protocol VLAN group being deleted here.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete a protocol VLAN group:

```
DGS-3450:admin# delete dot1v_protocol_group group_id 1
Command: delete dot1v_protocol_group group_id 1

Success.

DGS-3450:admin#
```

show dot1v_protocol_group

Purpose	Used to display the configurations for a protocol VLAN group.
Syntax	show dot1v_protocol_group {group_id <id>}
Description	This command will display the configurations of a protocol VLAN group.
Parameters	<i>group_id <id></i> – Enter an integer from 1 to 16 to identify the protocol VLAN group to be displayed. Entering this command without the <i>group_id</i> parameter will display the configurations for all configured protocol VLAN groups.
Restrictions	None.

Example usage:

To display the configurations for a protocol VLAN group:

```
DGS-3450:admin# show dot1v_protocol_group group_id 1
Command: show dot1v_protocol_group group_id 1

Protocol Group ID      Frame Type      Protocol Value
-----
1                      EthernetII     86DD

Total Entries: 1

DGS-3450:admin#
```

config port dot1v

Purpose	Used to bind a VLAN with a protocol template on one or more ports.
Syntax	config port dot1v ports [<portlist> all] [add protocol_group group_id <id> [vlan <vlan_name 32> vlanid <vlanid>] delete protocol_group [group_id <id> all]]
Description	This command will bind a VLAN with a protocol template on one or more ports. When an ingress untagged packet is identified by the <i>protocol_value</i> stated using the config dot1v_protocol_group command, the switch will assign a pre-configured VLAN and a priority for these ingress untagged packets in order to properly reach their destination.
Parameters	<p><i>ports</i> – Use this parameter to specify ports.</p> <ul style="list-style-type: none"> <i><portlist></i> – Use this parameter to assign a port or group of ports. <i>all</i> – Use this parameter to specify all ports on the system. <p><i>add protocol_group group_id <id></i> – Enter an integer from 1 to 16 to identify the protocol VLAN group being assigned to the ports or range of ports configured in the previous field.</p> <p><i>vlan</i> – Use this parameter bind a VLAN with a specific protocol template using either of the following parameters:</p> <ul style="list-style-type: none"> <i>vlan_name 32</i> – Identify the VLAN name for which to add a tag to ingress untagged packets. <i>vlanid</i> - Identify the VID for which to add a tag to ingress untagged packets. <p><i>delete protocol_group</i> – Use this parameter to remove this protocol VLAN group's association with the ports stated in this command, by using the following parameters:</p> <ul style="list-style-type: none"> <i>group_id <id></i> – Enter this parameter with its corresponding group number, to remove this pre-defined protocol group from the ports specified here. <i>all</i> – Use this parameter to remove all protocol VLAN groups from the ports specified in this command.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To bind a VLAN with a protocol template:

```
DGS-3450:admin# config port dot1v ports 1:6-1:8 add protocol_group group_id 1 vlan
building1
Command: config port dot1v ports 1:6-1:8 add protocol_group group_id 1 vlan building1

Success.

DGS-3450:admin#
```

show port dot1v

Purpose	Used to display the bound protocol template on a specific port or ports.
Syntax	show port dot1v {ports <portlist>}
Description	This command will display the protocol VLAN group and VLAN for individual ports.
Parameters	<i>ports <portlist></i> – Enter the port or group of ports for which to display the protocol VLAN group settings. Entering this command without this parameter will display all ports and their corresponding protocol VLAN group settings.
Restrictions	None.

Example usage:

To configure the ports for a protocol VLAN group:

```
DGS-3450:admin# show port dot1v ports 1:6-1:8
```

```
Command: show port dot1v ports 1:6-1:8
```

```
Port: 1:6
```

Protocol Group ID	VLAN Name
-----	-----
1	building1

```
Port: 1:7
```

Protocol Group ID	VLAN Name
-----	-----
1	building1

```
Port: 1:8
```

Protocol Group ID	VLAN Name
-----	-----
1	building1

```
Total Entries: 3
```

```
DGS-3450:admin#
```

QUALITY OF SERVICE (QoS) COMMANDS

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

Command	Parameters
config bandwidth_control	[<portlist> all] {rx_rate [no_limit <value 64-10000000>] tx_rate [no_limit <value 64-10000000>]}
show bandwidth_control	{<portlist>}
config scheduling	{ports [<portlist> all]} <class_id 0-6> [max_packet <value 0-15>]
config scheduling_mechanism	{ports [<portlist> all]} [strict weight_fair]
show scheduling	{<portlist>}
show scheduling_mechanism	{<portlist>}
config 802.1p user_priority	{ports [<portlist> all]} <priority 0-7> <class_id 0-6>
show 802.1p user_priority	{<portlist>}
config 802.1p default_priority	[<portlist> all] <priority 0-7>
show 802.1p default_priority	{<portlist>}
enable hol_prevention	
disable hol_prevention	
show hol_prevention	
config per_queue bandwidth_control	{ports [<portlist> all]} <cos_id_list 0-6> {{min_rate [no_limit <value 64-10000000 >]} max_rate [no_limit <value 64-10000000 >]}(1)
show per_queue bandwidth_control	{<portlist>}

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

config bandwidth_control

Purpose	Use to configure the port bandwidth limit control.
Syntax	config bandwidth_control [<portlist> all] {rx_rate [no_limit <value 64-10000000>] tx_rate [no_limit <value 64-10000000>]}
Description	This command sets the maximum limit for port bandwidth.
Parameters	<p><i>portlist</i> - Specifies the range of ports to be configured.</p> <p><i>rx_rate</i> - Specifies the limitations to apply to the receive data rate.</p> <p><i>no_limit</i> - Indicates there is no limit on the amount of bandwidth that can be received on the configured ports.</p> <p>An integer value from 64 to 10000000 sets the maximum limit in Kbits/sec. The actual bandwidth will be an adjusted value based on the user specified bandwidth. The actual limit may be equal to the user specified limit, but will not exceed it. The actual limit recognized by the device, will be displayed when the command is executed. Actual rate = (inputted rate/ minimum granularity) * minimal granularity</p> <p><i>tx_rate</i> - Specifies the limitation applied to the transmit data rate.</p> <p><i>no_limit</i> - Indicates that there is no limit on the port TX bandwidth.</p> <p>An integer value from 64 to 10000000 sets a maximum limit in Kbits/sec. The actual</p>

config bandwidth_control

bandwidth will be an adjusted value based on the user specified bandwidth. The actual limit may be equal to the user specified limit, but will not exceed it. The actual limit recognized by the device, will be displayed when the command is executed. Actual rate = (inputted rate/ minimum granularity) * minimal granularity

Restrictions Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the transmit bandwidth rate on port 1:1-1:10 to be 100 Kbits/sec:

```
DGS-3450:admin# config bandwidth_control 1:1-1:10 tx_rate 100
Command: config bandwidth_control 1:1-1:10 tx_rate 100
```

The setting value is not an integer multiple of granularity 64. The closest value 64 is chosen.

Success.

```
DGS-3450:admin#
```

show bandwidth_control

Purpose	Used to display the port bandwidth control table.
Syntax	show bandwidth_control {<portlist>}
Description	The show bandwidth_control command displays the port bandwidth configuration. The bandwidth can also be assigned by the RADIUS server through the authentication process. If the RADIUS server has assigned the bandwidth, then the RADIUS-assigned bandwidth will be the effective bandwidth. The authentication with the RADIUS server can be either per port or per user. For per-user authentication, there may be multiple bandwidth control values assigned when there are multiple users attached to the specific port. In this case, the largest assigned bandwidth value will be applied to the effective bandwidth for this specific port. Note that only devices that support MAC-based VLANs can provide per user authentication.
Parameters	<i>portlist</i> - Specifies a range of ports to be displayed. If no parameter is specified, the system will display all ports bandwidth configurations.
Restrictions	None.

Example usage:

To display port bandwidth control table for ports 1:1-1:10:

```
DGS-3450:admin# show bandwidth_control 1:1-1:10
```

```
Command: show bandwidth_control 1:1-1:10
```

Bandwidth Control Table

Port	RX Rate (Kbit/sec)	TX Rate (Kbit/sec)	Effective RX (Kbit/sec)	Effective TX (Kbit/sec)
1:1	no_limit	64	-	128
1:2	no_limit	64	-	-
1:3	no_limit	64	64	64
1:4	no_limit	64	64	64
1:5	no_limit	64	-	-
1:6	no_limit	64	64	64
1:7	no_limit	64	-	-
1:8	no_limit	64	-	-
1:9	no_limit	64	-	-
1:10	no_limit	64	-	-

```
DGS-3450:admin#
```

config scheduling

Purpose	Used to configure the traffic scheduling mechanism for each CoS queue.
Syntax	config scheduling {ports [<portlist> all]} <class_id 0-6> [max_packet <value 0-15>]
Description	Used to configure the traffic scheduling mechanism for each CoS queue.
Parameters	<p><i>ports <portlist></i> - Specifies the range of ports to be configured.</p> <p><i>all</i> - To set all ports in the system, you may use the "all" parameter. If no parameter is specified, the system will set all ports.</p> <p><i>class_id</i> - This specifies the n+1 hardware priority queues that the config scheduling command will apply to. The four hardware priority queues are identified by a number □ from 0 to n □ with the 0 queue being the lowest priority. The determination of n is project dependent.</p> <p><i>max_packet</i> - Specifies the maximum number of packets that the hardware priority queue, specified above, will be allowed to transmit before allowing the next lowest priority queue to transmit its packets. A value between 0 and m can be specified. Determination of m is project dependent.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the traffic scheduling on CoS queue 1, with a weight value of 15, on port 1:10:

```
DGS-3450:admin# config scheduling ports 1:10 1 max_packet 15
```

```
Command: config scheduling ports 1:10 1 max_packet 15
```

```
Success.
```

```
DGS-3450:admin#
```

config scheduling_mechanism

Purpose	Used to configure the traffic scheduling mechanism for each CoS queue.
Syntax	config scheduling_mechanism {ports [<portlist> all]} [strict weight_fair]

config scheduling_mechanism

Description	There are two sets of commands that the project can be choose to implement. If the project only supports the scheduling mechanism to be set globally, the portlist parameter will not be supported. This command is used to specify how the switch handles packets in priority queues.
Parameters	<i>ports</i> <portlist> - Specifies a range of ports to be configured. <i>all</i> - To set all ports in the system, you may use the "all" parameter. If no parameter is specified, the system will set all ports. <i>strict</i> - All queues will operate in strict mode. <i>weight_fair</i> - Each queue will operate based on their settings.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the traffic scheduling mechanism for the CoS queue on port 1:1:

```
DGS-3450:admin# config scheduling_mechanism ports 1:1 strict
Command: config scheduling_mechanism ports 1:1 strict

Success.

DGS-3450:admin#
```

show scheduling

Purpose	Used to display the current traffic scheduling parameters.
Syntax	show scheduling {<portlist>}
Description	The show scheduling command displays the current traffic scheduling parameters in use on the Switch.
Parameters	<i>portlist</i> - Specifies the range of ports to be displayed. If portlist is not specified, for the projects that support the per-port scheduling configure, system will display all ports' scheduling configurations, for those projects that only support the global scheduling settings, this command will display the global setting only.
Restrictions	None.

Example usage:

To display the traffic scheduling parameters for each CoS queue on port 1:1 (take eight hardware priority queues for example):

```
DGS-3450:admin#show scheduling 1:1
```

```
Command: show scheduling 1:1
```

```
QOS Output Scheduling On Port: 1:1
```

```
Class ID  MAX. Packets
```

```
-----  -----
```

```
Class-0   1
Class-1   2
Class-2   3
Class-3   4
Class-4   5
Class-5   6
Class-6   7
```

```
DGS-3450:admin#
```

show scheduling_mechanism

Purpose	Used to show the traffic scheduling mechanism.
Syntax	show scheduling_mechanism { <portlist> }
Description	The show scheduling_mechanism command displays the traffic scheduling mechanism.
Parameters	<i>portlist</i> - Specifies a range of ports to be displayed. If no portlist is specified, for the projects that support the per-port scheduling mechanism configure, system will display all ports' scheduling mechanism configurations, for those projects that only support the global scheduling mechanism settings, this command will display the global setting only.
Restrictions	None.

Example usage:

To show the scheduling mechanism for all ports:

```
DGS-3450:admin#show scheduling_mechanism 1:1
```

```
Command: show scheduling_mechanism 1:1
```

```
Port  Mode
-----  -----
1:1   strict
```

```
DGS-3450:admin#
```

config 802.1p user_priority

Purpose	Used to map the 802.1p user priority of an incoming packet to one of the eight hardware queues available on the Switch.
Syntax	config 802.1p user_priority { ports [<portlist> all]} <priority 0-7> <class_id 0-6>
Description	The config 802.1p user_priority command is used when you want to configure the way that the switch will map an incoming packet, based on its 802.1p user priority, to one of the available hardware priority queues on the switch.
Parameters	<i>ports <portlist></i> - Specifies the range of ports to be configured. <i>all</i> - To set all ports in the system, you may use the "all" parameter. If no parameter is specified, the system will set all ports. <i>priority</i> - The 802.1p user priority you want to associate the <class_id> (the number of the hardware queue) with.

config 802.1p user_priority

class_id - The number of the switch's hardware priority queue. The switch has 7 hardware priority queues available. They are numbered between 0 (the lowest priority) and 6 (the highest priority).

Restrictions Only Administrator and Operator-level users can issue this command.

Example usage:

To configure an 802.1p user priority of 1 and a class_ID of 3 on port 1:1:

```
DGS-3450:admin# config 802.1p user_priority ports 1:1 1 3
Command: config 802.1p user_priority ports 1:1 1 3
```

Success.

```
DGS-3450:admin#
```

show 802.1p user_priority

Purpose Used to display the 802.1p user priority.

Syntax **show 802.1p user_priority {<portlist>}**

Description The show 802.1p user_priority command displays 802.1p user priority for ports.

Parameters *portlist* - Specifies the range of ports to be displayed.

If no portlist is specified, this command will display the 802.1p user priority for all ports.

Restrictions Only Administrator and Operator-level users can issue this command.

Example usage:

In the case of Project only support global configuration, display the 802.1p user priority:

```
DGS-3450:admin#show 802.1p user_priority 1:1
Command: show 802.1p user_priority 1:1
```

QOS Class of Traffic

Port 1:1

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

```
DGS-3450:admin#
```

config 802.1p default_priority

Purpose Used to configure the 802.1p default priority settings on the Switch. If an untagged packet is received by the Switch, the priority configured with this command will be written to the packet's priority field.

Syntax **config 802.1p default_priority [<portlist> | all] <priority 0-7>**

Description The configure 802.1p default_priority command allows you to specify default priority handling

config 802.1p default_priority

	of untagged packets received by the Switch. The priority value entered with this command will be used to determine the hardware priority queues that the packet will be forwarded to.
Parameters	<p><i>portlist</i> - This specifies the range of ports, which require the default priority settings configured on. That is, the range of ports which receive all untagged packets will be assigned the priority specified below. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example:</p> <p>1:3 - Specifies switch number 1, port 3.</p> <p>2:4 - Specifies switch number 2, port 4.</p> <p>1:3-2:4 - Specifies all of the ports between switch 1, port 3 and switch 2, port 4, in numerical order.</p> <p><i>all</i> - Specifies that the command will apply to all ports on the switch.</p> <p><i>priority</i> - The priority value (0 to 7) assigned to untagged packets received by the switch or a range of ports on the switch.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure an 802.1p default priority settings of 5 on all Switch ports:

```
DGS-3450:admin# config 802.1p default_priority all 5
Command: config 802.1p default_priority all 5
```

Success.

```
DGS-3450:admin#
```

show 802.1p default_priority

Purpose	Used to display the current default priority settings on the Switch.
Syntax	show 802.1p default_priority { <portlist> }
Description	<p>The command displays the current configured default priority settings on the switch.</p> <p>The default priority can also be assigned by the RADIUS server through the authentication process. Authentication with the RADIUS server can be either per port or per user. For per port authentication, the priority assigned by the RADIUS server will be the default priority of the effective port. For per user authentication, the priority assigned by RADIUS will not be the effective port default priority, as the will priority associated with MAC address will be assigned. Note that only devices supporting MAC-based VLANs can provide per user authentication.</p>
Parameters	<p><i>portlist</i> - Specifies the range of ports to be displayed.</p> <p>If no parameter is specified, all ports with an 802.1p default priority will be displayed.</p>
Restrictions	None.

Example usage:

To display the 802.1p default priority on ports 1:1-1:10:

```
DGS-3450:admin#show 802.1p default_priority 1:1-1:10
```

```
Command: show 802.1p default_priority 1:1-1:10
```

Port	Priority	Effective Priority
----	-----	-----
1:1	0	0
1:2	0	0
1:3	0	0
1:4	0	0
1:5	0	0
1:6	0	0
1:7	0	0
1:8	0	0
1:9	0	0
1:10	0	0

```
DGS-3450:admin#
```

enable hol_prevention

Purpose	Used to enable HOL prevention.
Syntax	enable hol_prevention
Description	The enable hol_prevention command enables head of line prevention on the Switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable HOL prevention on the switch:

```
DGS-3450:admin# enable hol_prevention
```

```
Command: enable hol_prevention
```

```
Success.
```

```
DGS-3450:admin#
```

disable hol_prevention

Purpose	Used to disable HOL prevention.
Syntax	disable hol_prevention
Description	The command disables head of line prevention on the Switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable HOL prevention on the Switch:

```
DGS-3450:admin# disable hol_prevention
```

```
Command: disable hol_prevention
```

```
Success.
```

```
DGS-3450:admin#
```

show hol_prevention

Purpose	Use to show the HOL prevention state.
Syntax	show hol_prevention
Description	The show hol_prevention command displays the head of line prevention state on the switch.
Parameters	None.
Restrictions	None.

Example usage:

To display the HOL prevention state on the switch:

```
DGS-3450:admin# show hol_prevention
```

```
Command: show hol_prevention
```

```
Device HOL Prevention State: Enabled
```

```
DGS-3450:admin#
```

config per_queue bandwidth_control

Purpose	Used to configure the queue bandwidth control for each port.
Syntax	config per_queue bandwidth_control {ports [<portlist> all]} <cos_id_list 0-6> {{min_rate [no_limit <value 64-10000000>]} max_rate [no_limit <value 64-10000000>]}(1)
Description	<p>The config per_queue bandwidth_control command sets the bandwidth control for each specific queue on specified ports.</p> <p>min_rate specifies the minimum guaranteed bandwidth. Specifying no limit for the minimum rate means that bandwidth will not be guaranteed.</p> <p>max_rate limits the bandwidth. When specified, packets transmitted from the queue will not exceed the specified limit even if extra bandwidth is available.</p> <p>The specification of min_rate and max_rate are effective regardless of whether the queue is operating in strict mode or in WRR mode.</p>
Parameters	<p><i>ports <portlist></i> - Specifies a range of ports to be configured.</p> <p><i>all</i> - To set all ports in the system, you may use the "all" parameter. If no parameter is specified, the system will set all ports.</p> <p><i><cos_id_list 0-6></i> - Specifies a list of priority queues. The priority queue number is ranged from 0 to 6.</p> <p><i>min_rate</i> - Specifies that one of the parameters below (no_limit or 64-10000000) will be applied to the minimum rate, which the above specified class will be allowed to receive packets at.</p> <p><i>no_limit</i> - Specifies that there will be no limit on the rate of packets received by the class specified above.</p> <p><i><value 64-10000000></i> - Specifies the packet limit, in Kbps, that the above ports will be allowed to receive.</p>

config per_queue bandwidth_control

If the specified rate does not have multiple of minimum granularity, the rate will be adjusted:
Actual rate = (inputted rate/ minimum granularity) * minimal granularity.

max_rate - Specifies that one of the parameters below (*no_limit* or 64-10000000) will be applied to the maximum rate that the class specified above will be allowed to transmit packets at.

no_limit - Specifies that there will be no limit on the rate of packets received by the above specified class.

<value 64-10000000> - Specifies the packet limit, in Kbps, that the above ports will be allowed to receive.

If the specified rate does not have multiple of minimum granularity, the rate will be adjusted:
Actual rate = (inputted rate/ minimum granularity) * minimal granularity.

Restrictions

Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the minimum rate to be 130 and the maximum rate to be 100000 on CoS bandwidth queue 1 for ports 1:1-1:10:

```
DGS-3450:admin# config per_queue bandwidth_control ports 1:1-1:10 1 min_rate 130 max_rate 100000
Command: config per_queue bandwidth_control ports 1:1-1:10 1 min_rate 130 max_rate 100000

Success.

DGS-3450:admin#
```

show per_queue bandwidth_control

Purpose	Used to display the per queue bandwidth control settings for each port.
Syntax	show per_queue bandwidth_control {<portlist>}
Description	Used to display the per queue bandwidth control settings.
Parameters	<i>portlist</i> - Specifies the range of ports to be displayed. If no parameter is specified, the system will display the CoS bandwidth configuration for all ports.
Restrictions	None.

Example usage:

To display the per queue bandwidth control table for port 1:10:

```
DGS-3450:admin# show per_queue bandwidth_control 1:10
```

```
Command: show per_queue bandwidth_control 1:10
```

```
Queue Bandwidth Control Table On Port: 1:10
```

Queue	Min_Rate (64Kbit/sec)	Max_Rate (64Kbit/sec)
0	640	no_limit
1	640	no_limit
2	640	no_limit
3	640	no_limit
4	640	no_limit
5	no_limit	no_limit
6	no_limit	no_limit

```
DGS-3450:admin#
```

REMOTE COPY PROTOCOL (RCP) COMMANDS

RCP is a UNIX Remote Shell service which allows files to be copied between a server and client. RCP is an application that operates above the TCP protocols, and uses port number 514 as the TCP destination port.

The RCP application uses client server architecture and the client can be any machine running the RCP client application.

A Switch that supports the RCP client allows users to copy firmware images, configurations and log files between the Switch and RCP Server.

Switches that do not support a file system should still be able to run an RCP client to copy firmware images, configurations and logs between the switch and RCP server.

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

Command	Parameters
config rcp server	{ipaddress <ipaddr> username <username 15>}
config rcp server clear	[ipaddr username both]
show rcp server	
download firmware_fromRCP	[[username <username 15>] {<ipaddr>} src_file <path_filename 64> rcp:<string 128>] {unit [<unit_id 1-12> all]} {image_id <int 1-2>}
download cfg_fromRCP	[[username <username>] [{<ipaddr>}] src_file <path_filename 64> rcp: <string 128>] {config_id <int 1-2>}
upload cfg_toRCP	[[username <username>] [{ <ipaddr>}] dest_file <path_filename 64> rcp: <string 128>] {config_id <int 1-2>} {[include exclude begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}} {[include exclude begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}} {[include exclude begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}}}]}
upload log_toRCP	[[username <username 15>]{<ipaddr>} dest_file <path_filename 64> rcp:<string 128>]
upload attack_log_toRCP	[[username <username 15>]{<ipaddr>} dest_file <path_filename 64> rcp:<string 128>] {unit <unit_id 1-12>}

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

config rcp server

Purpose	Configure the global RCP server information.
Syntax	config rcp server {ipaddress <ipaddr> username <username 15>}
Description	This command is used to configure the global RCP server information. This global RCP Server setting can be used when the Server or remote user name is not specified. ONLY one RCP server can be configured for each system. If a user does not specify the RCP Server in the CLI command, and the global RCP Server was not configured, the Switch will ask the user to input the Server IP address or remote user name while executing the RCP commands.
Parameters	<i>ipaddress</i> - The IP address or IPv6 address of the global RCP Server. By default, the server is unspecified. <i>username</i> - The remote user name for logging into the global RCP Server. By default, the global server's remote user name is unspecified.
Restrictions	Only Administrator level users can issue this command.

Example usage:

To configure the global RCP Server:

```
DGS-3450:admin# config rcp server ipaddress 172.18.212.106 username rcp_user
Command: config rcp server ipaddress 172.18.212.106 username rcp_user

Success.

DGS-3450:admin#
```

config rcp server clear

Purpose	This command is used to clear the RCP global server information.
Syntax	config rcp server clear [ipaddr username both]
Description	This command is used to configure the global RCP server information. This global RCP Server setting can be used when the Server or remote user name is not specified. ONLY one RCP server can be configured for each system. If a user does not specify the RCP Server in the CLI command, and the global RCP Server was not configured, the Switch will ask the user to input the Server IP address or remote user name while executing the RCP commands.
Parameters	<i>ipaddress</i> - The IP address or IPv6 address of the global RCP Server. By default, the server is unspecified. <i>username</i> - The remote user name for logging into the global RCP Server. By default, the global server's remote user name is unspecified. <i>both</i> - Both the RCP Server IP address and remote user name.
Restrictions	Only Administrator level users can issue this command.

Example usage:

To configure the global RCP Server:

```
DGS-3450:admin# config rcp server clear username
Command: config rcp server clear username

Success.

DGS-3450:admin# config rcp server clear both
Command: config rcp server clear both

Success.

DGS-3450:admin#
```

show rcp server

Purpose	Used to display the global RCP server configured on the switch.
Syntax	show rcp server
Description	This command displays the global RCP server information.
Parameters	None.
Restrictions	Only Administrator level users can issue this command.

Example usage:

To display the global RCP Server configuration:

```
DGS-3450:admin#show rcp server
Command: show rcp server

RCP Server Address      : 172.18.212.106
RCP Server Username    : rcp_user

DGS-3450:admin#
```

download firmware_fromRCP

Purpose	This command is used to download firmware from RCP server.
Syntax	download firmware_fromRCP [{ username <username 15> } {<ipaddr>} src_file <path_filename 64> [rcp :<string 128>] { unit [unit_id 1-12> all]} { image_id <int 1-2>}
Description	This command is used to download a firmware image file from an RCP server.
Parameters	<p><i>username</i> - The remote user name on the RCP Server.</p> <p><i>ipaddr</i> - The IP address of the RCP server.</p> <p><i>path_filename</i> - The pathname specifies the pathname on the RCP server or local.</p> <p>Note: If user specifies the relative file path, the path search strategy is depending on the server system. For some system, will search the current user working directory firstly, then the environment paths.</p> <p><i>unit</i> - Specifies which unit on the stacking system. If it is not specified, it refers to the master unit.</p> <p><i>all</i> - When all is specified, the boot_up firmware image on all units will be updated.</p> <p><i>image_id</i> - Specifies which firmware image. It is no need to support this argument when only one firmware image is supported. If not specified, it refers to the boot_up image.</p> <p><i>rcp</i>: <string 128> - Syntax: rcp: username@ipaddr/directory/filename Example for FULL path: user_name@10.1.1.1/home/user_name/desxxxx.had Example for relative path: user_name@10.1.1.1./desxxxx.had Example for omitted user name in rcp string: 10.1.1.1./desxxxx.had.</p> <p>Note: No SPACE in the whole <string>.</p>
Restrictions	Only Administrator level users can issue this command.

Example usage:

To download firmware from RCP:

```
DGS-3450:admin# download firmware_fromRCP username rcp_user 172.18.212.106 src_file
/home/DGS-XXXX.had
Command: download firmware_fromRCP username rcp_user 172.18.212.106 src_file /home/DGS-
XXXX.had

Connecting to server..... Done.
Download firmware..... Done. Do not power off!
Please wait, programming flash..... Done.
Saving current settings to NV-RAM..... Done.

DGS-3450:admin#
```

To download firmware form RCP using string:

```
DGS-3450:admin# download firmware_fromRCP rcp: rcp_user@10.1.1.1/home/rcp_user/DGS-XXXX.had
Command: download firmware_fromRCP rcp: rcp_user@10.1.1.1/home/rcp_user/DGS-XXXX.had

Connecting to server..... Done.
Download firmware..... Done. Do not power off!
Please wait, programming flash..... Done.
Saving current settings to NV-RAM..... Done.

DGS-3450:admin#
```

To download firmware from RCP Server using rcp string without user name specified, and global RCP Server was not configured:

```
DGS-3450:admin# download firmware_fromRCP rcp: 10.1.1.1 DGS-XXXX.had
Command: download firmware_fromRCP rcp: 10.1.1.1 DGS-XXXX.had

Using RCP Server Username : rcp_user

Connecting to server..... Done.
Download firmware..... Done. Do not power off!
Please wait, programming flash..... Done.
Saving current settings to NV-RAM..... Done.

DGS-3450:admin#
```

To download firmware from RCP using global configured server:

```
DGS-3450:admin# download firmware_fromRCP src_file /home/DGS-XXXX.had
Command: download firmware_fromRCP src_file /home/DGS-XXXX.had

Using RCP Server IP: 172.18.212.106
Using RCP Server Username : rcp_user

Connecting to server..... Done.
Download firmware..... Done. Do not power off!
Please wait, programming flash..... Done.
Saving current settings to NV-RAM..... Done.
Please wait, the switch is rebooting...

DGS-3450:admin#
```

To download firmware from RCP without specifies the RCP Server and remote user:

```
DGS-3450:admin# download firmware_fromRCP src_file /home/DGS-XXXX.had
Command: download firmware_fromRCP src_file /home/DGS-XXXX.had

No RCP Server IP Configured.
Would you like to specify a RCP Server IP? (N) 172.18.211.106
No RCP Server Username Configured
Would you like to specify a RCP Server Username? (N) rcp_user

Connecting to server..... Done.
Download firmware..... Done. Do not power off!
Please wait, programming flash..... Done.
Saving current settings to NV-RAM..... Done.
Please wait, the switch is rebooting...

DGS-3450:admin#
```

To download firmware from RCP without specifies the RCP Server and remote user, and the global RCP server was not configured:

```
DGS-3450:admin# download firmware_fromRCP src_file DGS-XXXX.had
Command: download firmware_fromRCP src_file DGS-XXXX.had

No RCP Server IP configured.
Would you like to specify a RCP Server IP?(N)

RCP: copy file aborted!
Fail!

DGS-3450:admin#
```

To download DGS-XXXX.had from Global RCP Server and save with default file path & name:

```
DGS-3450:admin# download firmware_fromRCP src_file DGS-XXXX.had
Command: download firmware_fromRCP src_file DGS-XXXX.had

Using RCP Server IP: 172.18.212.106
Using RCP Server Username : rcp_user

Connecting to server..... Done.
Download firmware..... Done. Do not power off!
Please wait, programming flash..... Done.
Saving current settings to NV-RAM..... Done.

DGS-3450:admin#
```

download cfg_fromRCP

Purpose	Download configuration file from the RCP server.
Syntax	download cfg_fromRCP [{username <username>}] [{ipaddr}] src_file <path_filename 64> rcp: <string 128>] {config_id <int 1-2>}
Description	This command is used to download a configuration file from an RCP server.
Parameters	<i>username</i> - The remote user name on the RCP Server. <i>ipaddr</i> - The IP address of the RCP server. <i>path_filename</i> - The pathname specifies the pathname on the RCP server or local RCP client.

download cfg_fromRCP

Note: If a user specifies the relative file path, the path search strategy will depend on the server system. For some systems, the current user working directory will be searched first, followed by the environment paths.

config_id - Specifies the configuration file ID. There is no need to support this argument when only one CFG file is supported. If not specified, it refers to the boot_up configuration file.

rcp: <string 128> - Syntax: rcp: username@ipaddr/directory/filename

Example for FULL path: user_name@10.1.1.1/home/user_name/desxxxx.had

Example for relative path: user_name@10.1.1.1./desxxxx.had

Note: No SPACE in the whole <string>.

Restrictions

Only Administrator level users can issue this command.

Example usage:

To download a configuration file from an RCP server:

```
DGS-3450:admin# download cfg_fromRCP username rcp_user 172.18.212.106 src_file
/home/DGS-XXXX.cfg
Command: download cfg_fromRCP username rcp_user 172.18.212.106 src_file /home/DGS-
XXXX.cfg

Connecting to server..... Done.
Download configuration..... Done.

DGS-3450:admin#
```

To download a configuration using an RCP string:

```
DGS-3450:admin# download cfg_fromRCP rcp: rcp_user@172.18.212.106/home/DGS-XXXX.cfg
config_id 1
Command: download cfg_fromRCP rcp: rcp_user@172.18.212.106/home/DGS-XXXX.cfg config_id 1

Connecting to server..... Done.
Download configuration..... Done.

DGS-3450:admin#
```

upload cfg_toRCP

Purpose	Upload a configuration file from the device to an RCP server.
Syntax	upload cfg_toRCP [{username <username>} {[<ipaddr>]} dest_file <path_filename 64> rcp: <string 128>] {config_id <int 1-2>} {[include exclude begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}} {[include exclude begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}} {[include exclude begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}}}}}
Description	This command is used to upload a configuration file from the device to an RCP server. If the remote filename is not specified, the default file name will be modelname-image-id.
Parameters	<i>username</i> - The remote user name on the RCP Server. <i>ipaddr</i> - The IP address of the RCP server. <i>path_filename</i> - The pathname specifies the pathname on the RCP server or local RCP client. Note: If a user specifies the relative file path, the path search strategy will depend on the server system. For some systems, the current user working directory will be searched first, followed by the environment paths.

upload cfg_toRCP

If a user only specifies the `path_filename` parameter, only the current device configuration will be uploaded.

config_id - Specifies the configuration file ID. There is no need to support this argument when only one configuration file is supported. If not specified, it refers to the `boot_up` configuration file.

rcp: <string 128> - Syntax: `rcp: username@ipaddr/directory/filename`

Example for FULL path: `user_name@10.1.1.1/home/user_name/desxxxx.had`

Example for relative path: `user_name@10.1.1.1./desxxxx.had`

Note: No SPACES are allowed in the whole <string>.

filter_string - A filter string is enclosed by the “symbol. Therefore, the filter string itself cannot contain the “character. The filter string is case sensitive.

Restrictions

Only Administrator level users can issue this command.

Example usage:

To upload the configuration from a single-config device to an RCP server:

```
DGS-3450:admin# upload cfg_toRCP username rcp_user 172.18.212.104 dest_file /home/DGS-XXXX.cfg
Command: upload cfg_toRCP username rcp_user 172.18.212.104 dest_file /home/DGS-XXXX.cfg

Connecting to server..... Done.
Upload Configuration..... Done.

DGS-3450:admin#
```

To upload the configuration from a multi-config device to an RCP server using an RCP string:

```
DGS-3450:admin# upload cfg_toRCP rcp: rcp_user@172.18.212.104/home/DGS-XXXX.cfg config_id 1
Command: upload cfg_toRCP rcp: rcp_user@172.18.212.104/home/DGS-XXXX.cfg config_id 1

Connecting to server..... Done.
Upload configuration..... Done.

DGS-3450:admin#
```

upload log_toRCP

Purpose	Upload a log file from the device to an RCP server.
Syntax	upload log_toRCP [{ username <username 15>}{<ipaddr>} dest_file <path_filename 64> [rcp :<string 128>]
Description	This command is used to upload a system log file from the device to an RCP server. If a destination file is not specified the file name will be <code>modelname-slog</code> .
Parameters	<p><i>username</i> - The remote user name on the RCP Server.</p> <p><i>ipaddr</i> - The IP address of the RCP server.</p> <p><i>path_filename</i> - The pathname specifies the pathname on the RCP server or local RCP client.</p> <p>Note: If a user specifies the relative file path, the path search strategy will depend on the server system. For some systems, the current user working directory will be searched first, followed by the environment paths.</p>

upload log_toRCP

rcp: <string 128> - Syntax: rcp: username@ipaddr/directory/filename
 Example for FULL path: user_name@10.1.1.1/home/user_name/desxxxx.had
 Example for relative path: user_name@10.1.1.1./desxxxx.had
Note: No SPACES are allowed in the whole <string>.

Restrictions Only Administrator and Operator-level users can issue this command.

Example usage:

To upload the log from the device to an RCP server:

```
DGS-3450:admin# upload log_toRCP username rcp_user 172.18.212.104 dest_file /home/DGS-XXXX.log
Command: upload log_toRCP username rcp_user 172.18.212.104 dest_file /home/DGS-XXXX.log

Connecting to server... Done.
Upload log..... Done.

DGS-3450:admin#
```

To upload log from the device to an RCP server using an RCP string:

```
DGS-3450:admin# upload log_toRCP rcp: rcp_user@172.18.212.104/home/DGS-XXXX.log
Command: upload log_toRCP rcp: rcp_user@172.18.212.104/home/DGS-XXXX.log

Connecting to server..... Done.
Upload configuration..... Done.

DGS-3450:admin#
```

upload attack_log_toRCP

Purpose	Upload attack log file from the device to an RCP server.
Syntax	upload attack_log_toRCP [{ username <username 15>}{<ipaddr>} dest_file <path_filename 64> [rcp:<string 128>] {unit <unit_id 1-12>}
Description	This command is used to upload the system attack log file from the device to an RCP server.
Parameters	<p><i>username</i> - The remote user name on the RCP Server.</p> <p><i>ipaddr</i> - The IP address of the RCP server.</p> <p><i>path_filename</i> - The pathname specifies the pathname on the RCP server or local RCP client.</p> <p>Note: If a user specifies the relative file path, the path search strategy will depend on the server system. For some systems, the current user working directory will be searched first, followed by the environment paths</p> <p>Note: If a user only specifies the path_filename parameter for the RCP server, it will upload the master attack log file.</p> <p><i>unit</i> - Specifies which unit on the stacking system. If not specified, it refers to the master unit.</p> <p><i>rcp</i>: <string 128> - Syntax: rcp: username@ipaddr/directory/filename Example for FULL path: user_name@10.1.1.1/home/user_name/desxxxx.had Example for relative path: user_name@10.1.1.1./desxxxx.had Note: No SPACES allowed in the whole <string>.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To upload the attack log from the device to an RCP server:

```
DGS-3450:admin# upload attack_log_toRCP username rcp_user 172.18.212.104 dest_file
/home/DGS-XXXX.alog unit 2
Command: upload attack_log_toRCP username rcp_user 172.18.212.104 dest_file /home/DGS-
XXXX.alog unit 2

Connecting to server...Done.
Upload attack log.....Done.

DGS-3450:admin#
```

To upload the attack log from the device to an RCP server using an RCP string:

```
DGS-3450:admin# upload attack_log_toRCP rcp: rcp_user@172.18.212.104/home/DGS-XXXX.alog
Command: upload attack_log_toRCP rcp: rcp_user@172.18.212.104/home/DGS-XXXX.alog

Connecting to server..... Done.
Upload attack log..... Done.

DGS-3450:admin#
```

REMOTE SWITCHED PORT ANALYZER (RSPAN) COMMANDS

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

Command	Parameters
enable rspan	
disable rspan	
create rspan vlan	[vlan_name <vlan_name> vlan_id <value 1-4094>]
delete rspan vlan	[vlan_name <vlan_name> vlan_id <value 1-4094>]
config rspan vlan	[vlan_name <vlan_name> vlan_id <vlanid 1-4094>] source { [mirror_group_id <value 1-4> [add delete] ports <portlist> [rx tx both]]}
config rspan vlan	[vlan_name <vlan_name> vlan_id <vlanid 1-4094>] redirect [add delete] port <port>
show rspan	{[vlan_name <vlan_name> vlan_id <vlanid 1-4094>]}

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

enable rspan

Purpose	Used to enable the RSPAN globally.
Syntax	enable rspan
Description	<p>This command controls the RSPAN function.</p> <p>The purpose of the RSPAN function is to mirror packets to a remote switch.</p> <p>A packet travels from the switch where the monitored packet is received, passing through the intermediate switch, and then to the switch where the sniffer is attached. The first switch is also named the source switch.</p> <p>To make the RSPAN function work, the RSPAN VLAN source setting must be configured on the source switch. For the intermediate and the last switch, the RSPAN VLAN redirect setting must be configured.</p> <p>Note: RSPAN VLAN mirroring will only work when RSPAN is enabled (when one RSPAN VLAN has been configured with a source port).</p> <p>The RSPAN redirect function will work when RSPAN is enabled and at least one RSPAN VLAN has been configured with redirect ports.</p>
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

Configure RSPAN state to enable:

```
DGS-3450:admin# enable rspan
Command: enable rspan

Success.

DGS-3450:admin#
```


disable rspan

Purpose	Used to disable the RSPAN globally.
Syntax	disable rspan
Description	This command controls the RSPAN function.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

Configure RSPAN state to disabled:

```
DGS-3450:admin# disable rspan
Command: disable rspan

Success.

DGS-3450:admin#
```

create rspan vlan

Purpose	Used to create an RSPAN VLAN.
Syntax	create rspan vlan [vlan_name <vlan_name> vlan_id <value 1-4094>]
Description	This command is used to create the RSPAN VLAN. Up to 16 RSPAN VLANs can be created.
Parameters	<i>vlan_name</i> - Create the RSPAN VLAN by VLAN name. <i>vlan_id</i> - Create the RSPAN VLAN by VLAN ID.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create an RSPAN VLAN entry by VLAN name "v2":

```
DGS-3450:admin# create rspan vlan vlan_name v2
Command: create rspan vlan vlan_name v2

Success.

DGS-3450:admin#
```

To create an RSPAN VLAN entry by VLAN ID "3":

```
DGS-3450:admin# create rspan vlan vlan_id 3
Command: create rspan vlan vlan_id 3

Success.

DGS-3450:admin#
```

delete rspan vlan

Purpose	Used to delete an RSPAN VLAN.
---------	-------------------------------

delete rspan vlan

Syntax	delete rspan vlan [vlan_name <vlan_name> vlan_id <value 1-4094>]
Description	This command is used to delete RSPAN VLANs.
Parameters	<i>vlan_name</i> - Delete RSPAN VLAN by VLAN name. <i>vlan_id</i> - Delete RSPAN VLAN by VLAN ID.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete an RSPAN VLAN entry by VLAN name "v2":

```
DGS-3450:admin# delete rspan vlan vlan_name v2
Command: delete rspan vlan vlan_name v2
Success.

DGS-3450:admin#
```

To delete an RSPAN VLAN entry by VLAN ID "3":

```
DGS-3450:admin# delete rspan vlan vlan_id 3
Command: delete rspan vlan vlan_id 3
Success.

DGS-3450:admin#
```

config rspan vlan source

Purpose	Used by the source switch to configure the source setting for the RSPAN VLAN.
Syntax	config rspan vlan [vlan_name <vlan_name> vlan_id <vlanid 1-4094>] source { [mirror_group_id <value 1-4> [add delete] ports <portlist> [rx tx both]]}
Description	This command configures the source setting for the RSPAN VLAN on the source switch.
Parameters	<p><i>vlan</i> - See below:</p> <ul style="list-style-type: none"> <i>vlan_name</i> - Specify the RSPAN VLAN by VLAN name. <i>vlan_id</i> - Specify the RSPAN VLAN by VLAN ID. <p><i>source</i> - If the ports are not specified by this command, the source of RSPAN will come from the source specified by the mirror command or the flow-based source specified by an ACL. If no parameter is specified for source, it deletes the configured source parameters.</p> <ul style="list-style-type: none"> <i>add</i> - Add source ports. <i>delete</i> - Delete source ports. <i>ports <portlist></i> - Specify source portlist to add to or delete from the RSPAN source <i>rx</i> - Only monitor ingress packets. <i>tx</i> - Only monitor egress packets. <i>both</i> - Monitor both ingress and egress packets. <i>mirror_group_id</i> - The mirror group identify that specify which mirror session used for RSPAN source function. <p>If the mirror group is not specified when configuring the mirror ports, the mirror group 1 will be the default group.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure an RSPAN source entry without source target port:

```
DGS-3450:admin#config rspan vlan vlan_name vlan2 source add ports 2-5 rx
Command:config rspan vlan vlan_name vlan2 source add ports 2-5 rx

Success.

DGS-3450:admin#
```

To configure an RSPAN source entry for per flow RSPAN, without any source ports:

```
DGS-3450:admin#config rspan vlan vlan_id 2 source
Command:config rspan vlan vlan_id 2 source

Success.

DGS-3450:admin#
```

To configure an RSPAN entry on a source with mirror group ID:

```
DGS-3450:admin#config rspan vlan vlan_id 2 source mirror_group_id 3
Command:config rspan vlan vlan_id 2 source mirror_group_id 3

Success.

DGS-3450:admin#
```

config rspan vlan redirect

Purpose	Used by the intermediate or last switch to configure the output port for the RSPAN mirrored packet.
Syntax	config rspan vlan [vlan_name <vlan_name> vlan_id <vlanid 1-4094>] redirect [add delete] port <port>
Description	<p>This command is used by the intermediate or last switch to configure the output port of the RSPAN VLAN packets.</p> <p>The redirect command makes sure that the RSPAN VLAN packets can egress to the redirect ports. In addition, to this redirect command, the VLAN setting must be correctly configured to make the RSPAN VLAN work correctly. That is, for the intermediate switch, the redirect port must be tagged member port of RSPAN VLAN. For the last switch, the redirect port must be either be a tagged member port or an untagged member port of the RSPAN VLAN based on the users' requirements. If untagged membership is specified, the RSPAN VLAN tag will be removed.</p> <p>The redirect function will only work when RSPAN is enabled.</p> <p>Multiple RSPAN VLANs can be configured with the redirect setting at the same time.</p> <p>A RSPAN VLAN can be configured with the source setting and the redirect setting at the same time.</p>
Parameters	<p><i>vlan</i> - See below:</p> <ul style="list-style-type: none"> <i>vlan_name</i> - Specify the RSPAN VLAN by VLAN name. <i>vlan_id</i> - Specify the RSPAN VLAN by VLAN ID. <p><i>redirect</i> - Specify output portlist for the RSPAN VLAN packets. If the redirect port is a Link Aggregation port, there will perform the Link Aggregation behavior for RSPAN packets.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To add or delete redirect ports for special RSPAN VLAN on intermediate or destination switch:

```
DGS-3450:admin# config rspan vlan vlan_name vlan2 redirect add ports 1:18
Command: config rspan vlan vlan_name vlan2 redirect add ports 1:18

Success.

DGS-3450:admin#
```

show rspan

Purpose	Used to display RSPAN configuration.
Syntax	show rspan {[vlan_name <vlan_name> vlan_id <vlanid 1-4094>]}
Description	This command displays the RSPAN configuration.
Parameters	<i>vlan_name</i> - Specify the RSPAN VLAN by VLAN name <i>vlan_id</i> - Specify the RSPAN VLAN by VLAN ID.
Restrictions	None.

Example usage:

Display the specific settings:

```
DGS-3450:admin# show rspan vlan_id 63
Command: show rspan vlan_id 63
RSPAN : Enabled

RSPAN VLAN ID : 63
-----
Mirror Group ID : 1
Target Port     : 1:1
Source Ports
RX              : 1:2-1:5
TX              : 1:2-1:5
Redirect Ports  : 9

Total RSPAN VLAN : 1
DGS-3450:admin#
```

Display all settings:

```
DGS-3450:admin# show rspan
```

```
Command: show rspan
```

```
RSPAN: Enabled
```

```
RSPAN VLAN ID: 1
```

```
-----  
Mirror Group ID   : 1
```

```
Target Port       : 1:1
```

```
Source Ports
```

```
                RX:
```

```
                TX:
```

```
RSPAN VLAN ID: 2
```

```
-----  
Redirect Ports    : 1:6
```

```
RSPAN VLAN ID: 3
```

```
-----  
Redirect Ports    : 1:7
```

```
Total RSPAN VLAN :3
```

```
DGS-3450:admin#
```

ROUTING INFORMATION PROTOCOL (RIP) COMMANDS

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

Command	Parameters
config rip	[ipif <ipif_name 12> all] {authentication [enable <password 16> disable] tx_mode [disable v1_only v1_compatible v2_only] rx_mode [v1_only v2_only v1_or_v2 disable] state [enable disable]}
enable rip	
disable rip	
show rip	{ipif <ipif_name 12>}

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

config rip

Purpose	Used to configure RIP on the Switch.
Syntax	config rip [ipif <ipif_name 12> all] {authentication [enable <password 16> disable] tx_mode [disable v1_only v1_compatible v2_only] rx_mode [v1_only v2_only v1_or_v2 disable] state [enable disable]}
Description	This command is used to configure RIP on the Switch.
Parameters	<p><i><ipif_name 12></i> – The name of the IP interface.</p> <p><i>all</i> – To configure all RIP receiving mode for all IP interfaces.</p> <p><i>authentication [enable disable]</i> – Enables or disables authentication for RIP on the Switch.</p> <ul style="list-style-type: none"> <i><password 16></i> – Allows the specification of a case-sensitive password. <p><i>tx_mode</i> – Determines how received RIP packets will be interpreted – as RIP version <i>V1 only</i>, <i>V2 Only</i>, or <i>V1 Compatible (V1 and V2)</i>. This entry specifies which version of the RIP protocol will be used to transfer RIP packets. The disabled entry prevents the reception of RIP packets.</p> <ul style="list-style-type: none"> <i>disable</i> – Prevents the transmission of RIP packets. <i>v1_only</i> – Specifies that only RIP v1 packets will be transmitted. <i>v1_compatible</i> – Specifies that only RIP v1 compatible packets will be transmitted. <i>v2_only</i> – Specifies that only RIP v2 packets will be transmitted. <p><i>rx_mode</i> – Determines how received RIP packets will be interpreted – as RIP version <i>V1 only</i>, <i>V2 Only</i>, or <i>V1 or V2</i>. This entry specifies which version of the RIP protocol will be used to receive RIP packets. The <i>disable</i> entry prevents the reception of RIP packets.</p> <ul style="list-style-type: none"> <i>v1_only</i> – Specifies that only RIP v1 packets will be transmitted. <i>v2_only</i> – Specifies that only RIP v2 packets will be transmitted. <i>v1_or_v2</i> – Specifies that only RIP v1 or v2 packets will be transmitted. <p><i>state [enable disable]</i> – Allows RIP to be enabled and disabled on the Switch.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To change the RIP receive mode for the IP interface System:

```
DGS-3450:admin# config rip ipif System rx_mode v1_only
Command: config rip ipif System rx_mode v1_only

Success.

DGS-3450:admin#
```

enable rip

Purpose	Used to enable RIP.
Syntax	enable rip
Description	This command is used to enable RIP on the Switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example Usage:

To enable RIP:

```
DGS-3450:admin# enable rip
Command: enable rip

Success.

DGS-3450:admin#
```

disable rip

Purpose	Used to disable RIP.
Syntax	disable rip
Description	This command is used to disable RIP on the Switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable RIP:

```
DGS-3450:admin# disable rip
Command: disable rip

Success.

DGS-3450:admin#
```

show rip

Purpose	Used to display the RIP configuration and statistics for the Switch.
Syntax	show rip {ipif <ipif_name 12>}
Description	This command will display the RIP configuration and statistics for a given IP interface or for all IP interfaces.
Parameters	<i>ipif <ipif_name 12></i> – The name of the IP interface for which to display the RIP configuration and settings. If this parameter is not specified, the show rip command will display the global RIP configuration for the Switch.
Restrictions	None.

Example usage:

To display RIP configuration:

```
DGS-3450:admin# show rip
Command: show rip

RIP Global State : Disabled

RIP Interface Settings

Interface      IP Address      TX Mode    RX Mode      Authen-      State
-----
System        10.90.90.90/8   Disabled   Disabled     Disabled     Disabled

Total Entries : 1
DGS-3450:admin#
```

Example usage:

To display RIP configurations by IP interface:

```
DGS-3450:admin# show rip ipif System
Command: show rip ipif System

RIP Interface Settings

Interface Name: System          IP Address: 10.53.13.33/8 (Link Up)
Interface Metric: 1             Administrative State: Disabled
TX Mode: V2 Only                RX Mode: V1 or V2
Authentication: Disabled

Total Entries: 1

DGS-3450:admin#
```


SAFEGUARD ENGINE COMMANDS

Periodically, malicious hosts on the network will attack the Switch by utilizing packet flooding (ARP Storm) or other methods. These attacks may increase the CPU utilization beyond its capability. To alleviate this problem, the Safeguard Engine function was added to the Switch's software.

The Safeguard Engine can help the overall operability of the Switch by minimizing the workload of the Switch while the attack is ongoing, thus making it capable to forward essential packets over its network in a limited bandwidth. When the Switch either (a) receives too many packets to process or (b) exerts too much memory, it will enter an Exhausted mode.

When in this mode, the Switch will perform the following tasks to minimize the CPU usage:

1. It will limit bandwidth of receiving ARP packets. The user may implement this in two ways, by using the **config safeguard_engine** command.
 - a. When strict is chosen, the Switch will stop receiving ARP packets not destined for the Switch. This will eliminate all unnecessary ARP packets while allowing the essential ARP packets to pass through to the Switch's CPU.
 - b. When fuzzy is chosen, the Switch will minimize the ARP packet bandwidth received by the switch by adjusting the bandwidth for all ARP packets, whether destined for the Switch or not. The Switch uses an internal algorithm to filter ARP packets through, with a higher percentage set aside for ARP packets destined for the Switch.
2. It will limit the bandwidth of IP packets received by the Switch. The user may implement this in two ways, by using the **config safeguard_engine** command.
 - a. When strict is chosen, the Switch will stop receiving all unnecessary broadcast IP packets, even if the high CPU utilization is not caused by the high reception rate of broadcast IP packets.
 - b. When fuzzy is chosen, the Switch will minimize the IP packet bandwidth received by the Switch by adjusting the bandwidth for all IP packets, by setting a acceptable bandwidth for both unicast and broadcast IP packets. The Switch uses an internal algorithm to filter IP packets through while adjusting the bandwidth dynamically.

IP packets may also be limited by the Switch by configuring only certain IP addresses to be accepted. This method can be accomplished through the CPU Interface Filtering mechanism explained in the previous section. Once the user configures these acceptable IP addresses, other packets containing different IP addresses will be dropped by the Switch, thus limiting the bandwidth of IP packets. To keep the process moving fast, be sure not to add many conditions on which to accept these acceptable IP addresses and their packets, this limiting the CPU utilization.

Once in Exhausted mode, the packet flow will decrease by half of the level that caused the Switch to enter Exhausted mode. After the packet flow has stabilized, the rate will initially increase by 25% and then return to a normal packet flow.



NOTICE: When the Safeguard Engine is enabled, the Switch will allot bandwidth to various traffic flows (ARP, IP) using the FFP (Fast Filter Processor) metering table to control the CPU utilization and limit traffic. This may limit the speed of routing traffic over the network.

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

Command	Parameters
config safeguard_engine	{state [enable disable] utilization {rising <value 20-100> falling <value 20-100>} trap_log [enable disable] mode [strict fuzzy]}
show safeguard_engine	

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

config safeguard_engine

Purpose	To config ARP storm control for system.
Syntax	config safeguard_engine {state [enable disable] utilization {rising <value 20-100> falling <value 20-100>} trap_log [enable disable] mode [strict fuzzy]}
Description	Use this command to configure Safeguard Engine to minimize the effects of an ARP storm.
Parameters	<p><i>state [enable disable]</i> – Select the running state of the Safeguard Engine function as enable or disable.</p> <p><i>utilization</i> – Select this option to trigger the Safeguard Engine function to enable based on the following determinates:</p> <ul style="list-style-type: none"> <i>rising <value 20-100></i> – The user can set a percentage value of the rising CPU utilization which will trigger the Safeguard Engine function. Once the CPU utilization rises to this percentage, the Safeguard Engine mechanism will initiate. <i>falling <value 20-100></i> – The user can set a percentage value of the falling CPU utilization which will trigger the Safeguard Engine function to cease. Once the CPU utilization falls to this percentage, the Safeguard Engine mechanism will shut down. <p><i>trap_log [enable disable]</i> – Choose whether to enable or disable the sending of messages to the device's SNMP agent and switch log once the Safeguard Engine has been activated by a high CPU utilization rate.</p> <p><i>mode</i> - Used to select the type of Safeguard Engine to be activated by the Switch when the CPU utilization reaches a high rate. The user may select:</p> <ul style="list-style-type: none"> <i>strict</i> – If selected, this function will stop accepting all ARP packets not intended for the Switch, and will stop receiving all unnecessary broadcast IP packets, until the storm has subsided. <i>fuzzy</i> – If selected, this function will instruct the Switch to minimize the IP and ARP traffic flow to the CPU by dynamically allotting an even bandwidth to all traffic flows.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the safeguard engine for the Switch:

```
DGS-3450:admin# config safeguard_engine state enable utilization rising 45
Command: config safeguard_engine state enable utilization rising 45
```

Success.

```
DGS-3450:admin#
```

show safeguard_engine

Purpose	Used to display current Safeguard Engine settings.
Syntax	show safeguard_engine
Description	This will list the current status and type of the Safeguard Engine settings currently configured.
Parameters	None.
Restrictions	None.

Example usage:

To display the safeguard engine status:

```
DGS-3450:admin# show safeguard_engine
Command: show safeguard_engine

Safeguard engine state           : Disabled
Safeguard engine current status  : normal mode
=====
CPU utilization information:
Rising                          : 30%
Falling                          : 20%
Trap/Log state                  : Disabled
Mode                             : Fuzzy

DGS-3450:admin#
```

SECURE SHELL (SSH) COMMANDS

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

Command	Parameters
config ssh algorithm	[3DES AES128 AES192 AES256 Arcfour blowfish cast128 twofish128 twofish192 twofish256 MD5 SHA1 RSA DSS] [enable disable]
show ssh algorithm	
config ssh authmode	[password publickey hostbased] [enable disable]
show ssh authmode	
config ssh user	<username 15> authmode [hostbased [hostname <domain_name 32> hostname_IP <domain_name 32> <ipaddr>] password publickey]
show ssh user authmode	
config ssh server	{maxsession <int 1-8> contimeout <sec 120-600> authfail {<int 2-20> rekey [10min 30min 60min never] port < tcp_port_number 1-65535>}
enable ssh	
disable ssh	
show ssh server	

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

config ssh algorithm

Purpose	Used to config ssh server algorithm.
Syntax	config ssh algorithm [3DES AES128 AES192 AES256 Arcfour blowfish cast128 twofish128 twofish192 twofish256 MD5 SHA1 RSA DSS] [enable disable]
Description	The config ssh algorithm command config the ssh service algorithm.
Parameters	<p><i>3DES</i> - Specify ssh server encryption algorithm.</p> <p><i>blowfish</i> - Specify ssh server encryption algorithm.</p> <p><i>AES(128,192,256)</i> - Specify ssh server encryption algorithm.</p> <p><i>arcfour</i> - Specify ssh server encryption algorithm.</p> <p><i>cast128</i> - Specify ssh server encryption algorithm.</p> <p><i>twofish(128,192,256)</i> - Specify ssh server encryption algorithm.</p> <p><i>MD5</i> - Specify ssh server data integrity algorithm.</p> <p><i>SHA1</i> - Specify ssh server data integrity algorithm.</p> <p><i>DSS</i> - Specify ssh server public key algorithm.</p> <p><i>RSA</i> - Specify ssh server public key algorithm.</p> <p><i>enable</i> - Specify to enable the algorithm.</p> <p><i>disable</i> - Specify to disable the alogirthm.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable ssh server public key algorithm:

```
DGS-3450:admin# config ssh algorithm DSS enable RSA enable
Command: config ssh algorithm DSS enable RSA enable

Success.

DGS-3450:admin#
```

show ssh algorithm

Purpose	Used to show ssh server algorithm.
Syntax	show ssh algorithm
Description	The show ssh algorithm command show the ssh service algorithm.
Parameters	None.
Restrictions	None.

Example usage:

To show server algorithm:

```
DGS-3450:admin# show ssh algorithm
Command: show ssh algorithm

Encryption Algorithm
3DES      : Enabled
AES128    : Enabled
AES192    : Enabled
AES256    : Enabled
Arcfour   : Enabled
Blowfish  : Enabled
Cast128   : Enabled
Twofish128 : Enabled
Twofish192 : Enabled
Twofish256 : Enabled
MD5       : Enabled
SHA1      : Enabled
RSA       : Enabled
DSS       : Enabled

DGS-3450:admin#
```

config ssh authmode

Purpose	Used to update user authentication for ssh configuration.
Syntax	config ssh authmode [password publickey hostbased] [enable disable]
Description	The config ssh user command update the ssh user information.
Parameters	<i>password</i> - Specifies user authentication method. <i>publickey</i> - Specifies user authentication method. <i>hostbased</i> - Specifies user authentication method. <i>enable</i> - Enable user authentication method. <i>disable</i> - Disable user authentication method.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To config user authentication method:

```
DGS-3450:admin# config ssh authmode publickey enable
Command: config ssh authmode publickey enable

Success.

DGS-3450:admin#
```

show ssh authmode

Purpose	Used to show user authentication method.
Syntax	show ssh authmode
Description	The show ssh authmode command show the user authentication method.
Parameters	None.
Restrictions	None.

Example usage:

To show user authentication method:

```
DGS-3450:admin# show ssh authmode
Command: show ssh authmode

The SSH authmode
Password : Enabled
Publickey : Enabled
Hostbased : Enabled

DGS-3450:admin#
```

config ssh user

Purpose	Used to update user information for ssh configuration.
Syntax	config ssh user <username 15> authmode [hostbased [hostname <domain_name 32> hostname_IP <domain_name 32> <ipaddr>] password publickey]
Description	The config ssh user command update the ssh user information.
Parameters	<p><i>username</i> - Specifies the User name.</p> <p><i>publickey</i> - Specifies user authentication method.</p> <p><i>password</i> - Specifies user authentication method.</p> <p><i>hostbased</i> - Specifies user authentication method.</p> <p><i>hostname</i> - Specifies host domain name.</p> <p><i>hostname_ip</i> - Specifies host domain name and ipaddress.</p> <p><i>domain_name</i> - Specifies host name if configuration hostbased mode.</p> <p><i>ipaddr</i> - Specifies host ip address if configuring hostbased mode.</p>
Restrictions	Only Administrator level users can issue this command.

Example usage:

To update user "test" authmode:

```
DGS-3450:admin# config ssh user test publickey
Command: config ssh user test publickey

Success.

DGS-3450:admin#
```

show ssh user authmode

Purpose	Used to show ssh user information.
Syntax	show ssh user authmode
Description	The show ssh user command show the ssh user information.
Parameters	None.
Restrictions	Only Administrator level users can issue this command.

Example usage:

To show user information about ssh configuration:

```
DGS-3450:admin# show ssh user authmode
Command: show ssh user authmode

Current Accounts
Username      Authenticaiton
-----
test         publickey

Total Entries : 1

DGS-3450:admin#
```

config ssh server

Purpose	Used to configure the SSH server.
Syntax	config ssh server {maxsession <int 1-8> contimeout <sec 120-600> authfail {<int 2-20> rekey [10min 30min 60min never] port < tcp_port_number 1-65535>}
Description	The config ssh server command config the SSH server general information.
Parameters	<p><i>maxsession</i> - Specifies ssh server max session at the same time.</p> <p><i>contimeout</i> - Specifies ssh server connection timeout.</p> <p><i>authfail</i> - Specifies user max fail attempts.</p> <p><i>10/30/60 min</i> - Specifies time to re-generate session key.</p> <p><i>never</i> - Do not re-generate session key.</p> <p><i>port</i> - Specifies the TCP port used to communication between ssh client and server. The default value is 22.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To config ssh server maxsession is 3:

```
DGS-3450:admin# config ssh server maxsession 3
Command: config ssh server maxsession 3

Success.

DGS-3450:admin#
```

enable ssh

Purpose	Used to enable the SSH server.
Syntax	enable ssh
Description	The enable ssh command enables ssh server services. When enabling ssh, telnet will be disabled.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable the SSH server:

```
DGS-3450:admin# enable ssh
Command: enable ssh

Success.

DGS-3450:admin#
```

disable ssh

Purpose	Used to disable the SSH server service.
Syntax	disable ssh
Description	The disable ssh command disables ssh server services.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable the SSH server service:

```
DGS-3450:admin# disable ssh
Command: disable ssh

Success.

DGS-3450:admin#
```

show ssh server

Purpose	Used to show the SSH server.
Syntax	show ssh server
Description	The show ssh server command show the ssh server general information.

show ssh server

Parameters	None.
Restrictions	None.

Example usage:

To show the SSH server:

```
DGS-3450:admin# show ssh server
Command: show ssh server
```

The SSH server configuration

```
max Session           : 3
Connection timeout    : 300
Authfail attempts     : 2
Rekey timeout         : 60min
TCP Port Number       : 23
```

```
DGS-3450:admin#
```

SECURE SOCKETS LAYER (SSL) COMMANDS

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

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

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

Command	Parameters
enable ssl	{ciphersuite {RSA_with_RC4_128_MD5 RSA_with_3DES_EDE_CBC_SHA DHE_DSS_with_3DES_EDE_CBC_SHA RSA_EXPORT_with_RC4_40_MD5}}
disable ssl	{ciphersuite {RSA_with_RC4_128_MD5 RSA_with_3DES_EDE_CBC_SHA DHE_DSS_with_3DES_EDE_CBC_SHA RSA_EXPORT_with_RC4_40_MD5}}
config ssl cachetimeout	<value 60-86400>
show ssl	{certificate}
show ssl cachetimeout	
download ssl certificate	<ipaddr> certfilename <path_filename 64> keyfilename <path_filename 64>

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

enable ssl

Purpose	To enable the SSL function on the Switch.
---------	---

enable ssl

Syntax	enable ssl {ciphersuite {RSA_with_RC4_128_MD5 RSA_with_3DES_EDE_CBC_SHA DHE_DSS_with_3DES_EDE_CBC_SHA RSA_EXPORT_with_RC4_40_MD5}}
Description	This command will enable SSL on the Switch by implementing any one or combination of listed ciphersuites on the Switch. Entering this command without a parameter will enable the SSL status on the Switch. Enabling SSL will disable the web-manager on the Switch.
Parameters	<p><i>ciphersuite</i> – A security string that determines the exact cryptographic parameters, specific encryption algorithms and key sizes to be used for an authentication session. The user may choose any combination of the following:</p> <ul style="list-style-type: none"> • <i>RSA_with_RC4_128_MD5</i> – This ciphersuite combines the RSA key exchange, stream cipher RC4 encryption with 128-bit keys and the MD5 Hash Algorithm. • <i>RSA_with_3DES_EDE_CBC_SHA</i> – This ciphersuite combines the RSA key exchange, CBC Block Cipher 3DES_EDE encryption and the SHA Hash Algorithm. • <i>DHE_DSS_with_3DES_EDE_CBC_SHA</i> – This ciphersuite combines the DSA Diffie Hellman key exchange, CBC Block Cipher 3DES_EDE encryption and SHA Hash Algorithm. • <i>RSA_EXPORT_with_RC4_40_MD5</i> – This ciphersuite combines the RSA Export key exchange, stream cipher RC4 encryption with 40-bit keys. <p>The ciphersuites are enabled by default on the Switch, yet the SSL status is disabled by default. Enabling SSL with a ciphersuite will not enable the SSL status on the Switch.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable SSL on the Switch for all ciphersuites:

```
DGS-3450:admin# enable ssl
Command:enable ssl
```

Note: Web will be disabled if SSL is enabled.
Success.

```
DGS-3450:admin#
```



NOTE: Enabling SSL on the Switch will enable all ciphersuites. To utilize a particular ciphersuite, the user must eliminate other ciphersuites by using the `disable ssl` command along with the appropriate ciphersuites.



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

disable ssl

Purpose	To disable the SSL function on the Switch.
Syntax	disable ssl {ciphersuite {RSA_with_RC4_128_MD5 RSA_with_3DES_EDE_CBC_SHA DHE_DSS_with_3DES_EDE_CBC_SHA RSA_EXPORT_with_RC4_40_MD5}}
Description	This command will disable SSL on the Switch and can be used to disable any one or combination of listed ciphersuites on the Switch.
Parameters	<p><i>ciphersuite</i> – A security string that determines the exact cryptographic parameters, specific encryption algorithms and key sizes to be used for an authentication session. The user may choose any combination of the following:</p> <ul style="list-style-type: none"> • <i>RSA_with_RC4_128_MD5</i> – This ciphersuite combines the RSA key exchange, stream cipher RC4 encryption with 128-bit keys and the MD5 Hash Algorithm. • <i>RSA_with_3DES_EDE_CBC_SHA</i> – This ciphersuite combines the RSA key exchange, CBC Block Cipher 3DES_EDE encryption and the SHA Hash Algorithm. • <i>DHE_DSS_with_3DES_EDE_CBC_SHA</i> – This ciphersuite combines the DSA Diffie Hellman key exchange, CBC Block Cipher 3DES_EDE encryption and SHA Hash Algorithm. • <i>RSA_EXPORT_with_RC4_40_MD5</i> – This ciphersuite combines the RSA Export key exchange, stream cipher RC4 encryption with 40-bit keys.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable the SSL status on the Switch:

```
DGS-3450:admin# disable ssl
```

```
Command: disable ssl
```

```
Success.
```

```
DGS-3450:admin#
```

To disable ciphersuite RSA_EXPORT_with_RC4_40_MD5 only:

```
DGS-3450:admin# disable ssl ciphersuite RSA_EXPORT_with_RC4_40_MD5
```

```
Command: disable ssl ciphersuite RSA_EXPORT_with_RC4_40_MD5
```

```
Success.
```

```
DGS-3450:admin#
```

config ssl cachetimeout

Purpose	Used to configure the SSL cache timeout.
Syntax	config ssl cachetimeout <value 60-86400>
Description	This command will set the time between a new key exchange between a client and a host using the SSL function. A new SSL session is established every time the client and host go through a key exchange. Specifying a longer timeout will allow the SSL session to reuse the master key on future connections with that particular host, therefore speeding up the negotiation process.
Parameters	<value 60-86400> – Enter a timeout value between 60 and 86400 seconds to specify the total time an SSL key exchange ID stays valid before the SSL module will require a new, full SSL negotiation for connection. The default cache timeout is 600 seconds
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To set the SSL cachetimeout for 7200 seconds:

```
DGS-3450:admin# config ssl cachetimeout 7200
Command: config ssl cachetimeout 7200

Success.

DGS-3450:admin#
```

show ssl cachetimeout

Purpose	Used to show the SSL cache timeout.
Syntax	show ssl cachetimeout
Description	Entering this command will allow the user to view the SSL cache timeout currently implemented on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To view the SSL cache timeout on the Switch:

```
DGS-3450:admin# show ssl cachetimeout
Command: show ssl cachetimeout

Cache timeout is 600 second(s).

DGS-3450:admin#
```

show ssl

Purpose	Used to view the SSL status and the certificate file status on the Switch.
Syntax	show ssl {certificate}
Description	This command is used to view the SSL status on the Switch.
Parameters	<i>{certificate}</i> – Use this parameter to display the SSL certificate file information currently implemented on the Switch.
Restrictions	None.

Example usage:

To view the SSL status on the Switch:

```
DGS-3450:admin# show ssl
Command: show ssl

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

DGS-3450:admin#
```

Example usage:

To view certificate file information on the Switch:

```
DGS-3450:admin# show ssl certificate
Command: show ssl certificate

Loaded with RSA Certificate!

DGS-3450:admin#
```

download ssl certificate

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

Example usage:

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

```
DGS-3450:admin# download ssl certificate 10.53.13.94 certfilename c:/cert.der keyfilename
c:/pkey.der
Command: download ssl certificate 10.53.13.94 certfilename c:/cert.der keyfilename
c:/pkey.der

Certificate Loaded Successfully!

DGS-3450:admin#
```

sFLOW COMMANDS

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

Command	Parameters
create sflow flow_sampler	ports [<portlist> all] analyzer_server_id < value 1-4> {rate <value 0-65535> tx_rate <value 0-65535> maxheadersize <value 18-256>}
config sflow flow_sampler	ports [<portlist> all] {rate <value 0-65535> tx_rate <value 0-65535> maxheadersize < value 18-256 >}(1)
delete sflow flow_sampler	ports [<portlist> all]
create sflow counter_poller	ports [<portlist> all] analyzer_server_id < value 1-4> {interval [disable <sec 20-120>]}
config sflow counter_poller	ports [<portlist> all] interval [disable <sec 20-120>]
delete sflow counter_poller	ports [<portlist> all]
create sflow analyzer_server	< value 1-4 > owner<name 16> {timeout [<sec 1-2000000> infinite] collectoraddress [<ipaddr> <ipv6addr>] collectorport <udp_port_number 1-65535> maxdatagramsize < value m-n>}
config sflow analyzer_server	< value 1-4 > {timeout [<sec 1-2000000 > infinity] collectoraddress [<ipaddr> <ipv6addr>] collectorport <udp_port_number 1-65535> maxdatagramsize < value 300-1400 >}(1)
delete sflow analyzer_server	< value 1-4 >
enable sflow	
disable sflow	
show sflow	
show sflow flow_sampler	
show sflow counter_poller	
show sflow analyzer_server	

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

create sflow flow_sampler

Purpose	Used to create the sFlow flow_sampler.
Syntax	create sflow flow_sampler ports [<portlist> all] analyzer_server_id < value 1-4> {rate <value 0-65535> tx_rate <value 0-65535> maxheadersize <value 18-256>}
Description	Used to create the sFlow flow_sampler. By configuring the sampling function for a port, a sample packet received by this port will be encapsulated and forwarded to analyzer server at the specified interval.
Parameters	<p><i>ports</i> - Specifies the list of ports to be configured.</p> <p><i>analyzer_server_id</i> - Specifies the ID of a server analyzer where the packet will be forwarded.</p> <p><i>rate</i> - The sampling rate for packet Rx sampling.</p> <p><i>tx_rate</i> - The sampling rate for packet Tx sampling.</p> <p><i>maxheadersize</i> - The maximum number of leading bytes in the packet which has been sampled that will be encapsulated and forwarded to the server. If not specified, the default</p>

create sflow flow_sampler

value is 128

Restrictions Only Administrator and Operator-level users can issue this command.

Example usage:

Create sFlow flow sampler:

```
DGS-3450:admin# create sflow flow_sampler ports 1 analyzer_server_id 1 rate 1
maxheadersize 18
Command: create sflow flow_sampler ports 1 analyzer_server_id 1 rate 1 maxheadersize 18
```

Success.

DGS-3450:admin#

config sflow flow_sampler

Purpose	Used to config the sFlow flow_sampler parameters.
Syntax	config sflow flow_sampler ports [<portlist> all] {rate <value 0-65535> tx_rate <value 0-65535> maxheadersize <value 18-256>}(1)
Description	Configures the sFlow flow sampler parameters. In order to change the analyzer_server_id, first delete the flow_sampler and create a new one.
Parameters	<p><i>ports</i> - Specifies the list of ports to be configured.</p> <p><i>rate</i> - The sampling rate for packet Rx sampling.</p> <p><i>tx_rate</i> - The sampling rate for packet Tx sampling.</p> <p><i>maxheadersize</i> - The maximum number of leading bytes in the packet which has been sampled that will be encapsulated and forwarded to the server. If not specified, the default value is 128.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

Configure the sFlow sampler the rate of port 1 to be 0:

```
DGS-3450:admin# config sflow flow_sampler ports 1 rate 0 tx_rate 1
Command: config sflow flow_sampler ports 1 rate 0 tx_rate 1
```

Success.

DGS-3450:admin#

delete sflow flow_sampler

Purpose	Used to delete the sFlow flow_sampler.
Syntax	delete sflow flow_sampler ports [<portlist> all]
Description	Used to delete the sFlow flow_sampler.
Parameters	<i>ports</i> - Specifies the list of ports to be configured.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

Delete the sFlow sampler port 1:

```
DGS-3450:admin# delete sflow flow_sampler ports 1
Command: delete sflow flow_sampler ports 1

Success.

DGS-3450:admin#
```

create sflow counter_poller

Purpose	Used to create the sFlow counter_poller:
Syntax	create sflow counter_poller ports [<portlist> all] analyzer_server_id <value 1-4> {interval [disable <sec 20-120>]}
Description	This command is used to create the sFlow counter poller. The poller function instructs the switch to forward statistics counter information with respect to a port. The counters are RFC 2233 counters.
Parameters	<i>analyzer_server_id</i> - The analyzer_server_id is the id of a analyzer_server, <i>interval</i> - The maximum number of seconds between successive statistic counters information. If set to 0, the counter-poller is disabled. If interval is not specified, its default value is 0.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

Create sFlow counter poller, which sample port 1 to analyzer server 1:

```
DGS-3450:admin# create sflow counter_poller ports 1 analyzer_server_id 1
Command: create sflow counter_poller ports 1 analyzer_server_id 1

Success.

DGS-3450:admin#
```

config sflow counter_poller

Purpose	Used to config the sFlow counter_poller parameters.
Syntax	config sflow counter_poller ports [<portlist> all] interval [disable <sec 20-120>]
Description	This command is used to configure the sFlow counter_poller parameters. If the user wants the change the analyzer_server_id, he needs to delete the counter_poller and creates a new one.
Parameters	<i>interval</i> - The maximum number of seconds between successive samples of the counters. If set it 0, the counter-sample is disabled.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

Configure the interval of sFlow counter poller port 1 to be 0:

```
DGS-3450:admin# config sflow counter_poller ports 1 interval disable
Command: config sflow counter_poller ports 1 interval disable

Success.

DGS-3450:admin#
```

delete sflow counter_poller

Purpose	Used to delete the sFlow counter poller.
Syntax	delete sflow counter_poller ports [<portlist> all]
Description	Delete the sFlow counter_poller from the specified port.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

Delete sFlow counter poller on port 1:

```
DGS-3450:admin# delete sflow counter_poller ports 1
Command: delete sflow counter_poller ports 1

Success.

DGS-3450:admin#
```

create sflow analyzer_server

Purpose	Used to create the analyzer server.
Syntax	create sflow analyzer_server < value 1-4 > owner<name 16> {timeout [<sec m-n> infinite] collectoraddress [<ipaddr> <ipv6addr>] collectorport <udp_port_number 1-65535> maxdatagramsize < value m-n>}
Description	Creates the analyzer_server. You can specify more than one analyzer_server with the same IP address but with different UDP port numbers. You can have up to four unique combinations of IP address and UDP port number.
Parameters	<p><i>owner</i> - The entity making use of this sFlow analyzer_server. When owner is set or modified, the timeout value will become 400 automatically.</p> <p><i>timeout</i> - The length of time before the server is timed out. When the analyzer_server times out, all of the flow_samplers and counter_pollers associated with this analyzer_server will be deleted. If not specified, its default value is 400.</p> <p><i>collectoraddress</i> - The IP address of the analyzer_server. If this is set to 0 or not specified, the IPv4 address is 0.0.0.0 and the entry is not active. It is not only IPv4 address, but also IPv6 address.</p> <p><i>collectorport</i> - The destination UDP port for sending the sFlow datagrams. If not specified, the default value is 6364.</p> <p><i>maxdatagramsize</i> - The maximum number of data bytes that can be packed in a single sample datagram. If not specified, the default value is 1400.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create the analyzer_server:

```
DGS-3450:admin# create sflow analyzer_server 2 owner monitor timeout infinite collect
oraddress 10.0.0.1 collectorport 65524 maxdatagramsize 300
Command: create sflow analyzer_server 2 owner monitor timeout infinite collector
address 10.0.0.1 collectorport 65524 maxdatagramsize 300

Success.

DGS-3450:admin#
```

config sflow analyzer_server

Purpose	Used to config the analyzer server information.
Syntax	config sflow analyzer_server <value 1-4> {timeout [<sec 1-2000000 > infinity] collectoraddress [<ipaddr> <ipv6addr>] collectorport <udp_port_number 1-65535> maxdatagramsize < value 300-1400 >}(1)
Description	Configures the receiver information. You can specify more than one collector with the same IP address if the UDP port numbers are unique.
Parameters	<p><i>timeout</i> - The time (in seconds) remaining before the sample is released and stops sampling. When the analyzer_server times out, all of the flow_samplers and counter_pollers associated with this analyzer_server will be deleted.</p> <p><i>collectoraddress</i> - The IP address of the server. If not specified or set a 0 address, sFlow packets will not be sent to this server.</p> <p><i>collectorport</i> - The destination port for sending sFlow datagrams</p> <p><i>maxdatagramsize</i> - The maximum number of data bytes that can be packed in a single sample datagram.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

Configure the sFlow analyzer server to be 10.90.90.90:

```
DGS-3450:admin# config sflow analyzer_server 1 collectoraddress 10.90.90.90
Command: config sflow analyzer_server 1 collectoraddress 10.90.90.90

Success.

DGS-3450:admin#
```

delete sflow_analyzer_server

Purpose	Used to delete the analyzer_server.
Syntax	delete sflow analyzer_server < value 1-4 >
Description	Used to delete the analyzer_server.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete the analyzer_server:

```
DGS-3450:admin# delete sflow analyzer_server 1
Command: delete sflow analyzer_server 1

Success.

DGS-3450:admin#
```

enable sflow

Purpose	Used to enable the sFlow function.
Syntax	enable sflow
Description	Enable the sFlow function.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

Enable sFlow:

```
DGS-3450:admin# enable sflow
Command: enable sflow

Success.
DGS-3450:admin#
```

disable sflow

Purpose	Used to disable the sFlow function.
Syntax	disable sflow
Description	Disable the sFlow function.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable the sFlow function:

```
DGS-3450:admin# disable sflow
Command: disable sflow

Success.

DGS-3450:admin#
```

show sflow

Purpose	Show the sFlow information.
Syntax	show sflow
Description	This command is used to show the sFlow information. sFlow Address: The IPv4 address associated with this agent. sFlow AddressV6: The IPv6 address associated with this agent.

show sflow

	sFlow State: The current state of the sFlow agent.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To show the sFlow information:

```
DGS-3450:admin# show sflow
Command: show sflow

sFlow Version      : V5
sFlow Address      : 10.90.90.90
sFlow AddressV6    : FE80::285:43FF:FE26:3101
sFlow State        : Enabled

DGS-3450:admin#
```

show sflow flow_sampler

Purpose	Used to display the sFlow flow_sampler information of ports which have been created.
Syntax	show sflow flow_sampler
Description	This command is used to show the sFlow flow_sampler configured for ports. The actual value rate is 256 times the displayed rate value. There are two types of rates. The Configured Rate is configured by the user. In order to limit the number of packets sent to the CPU when the rate of traffic to the CPU is high, the sampling rate will be decreased. This is specified as the active rate.
Parameters	None.
Restrictions	None.

Example usage:

To show the sFlow flow_sampler information of ports which have been created:

```
DGS-3450:admin# show sflow flow_sampler
Command: show sflow flow_sampler

  Port      Analyzer  Configured  Configured  Active  Active  Max Header
  ---      -
  Server ID  Rx Rate    Tx Rate     Rx Rate    Tx Rate  Size
  ---      -
  10        1          1           2          0        0       20

Total Entries: 1

DGS-3450:admin#
```

show sflow flow_poller

Purpose	Used to display the sFlow counter_poller information of ports which have been created.
Syntax	show sflow counter_poller
Description	This command is used to show the sFlow counter_pollers which have been configured for

show sflow flow_poller

	port.
Parameters	None.
Restrictions	None.

Example usage:

To show the sFlow counter_poller information of ports which have been created:

```
DGS-3450:admin# show sflow counter_poller
Command: show sflow counter_poller

  Port      Analyzer Server ID      Polling Interval (secs)
  ----      -
  1         1                        disable

Total Entries: 1

DGS-3450:admin#
```

show sflow analyzer_server

Purpose	Used to display the sFlow analyzer server information.
Syntax	show sflow analyzer_server
Description	This command is used to show the sFlow analyzer_server information. The Timeout field specifies the time configured by user. The Current Countdown Time is the current time remaining before the server timeout.
Parameters	None.
Restrictions	None.

Example usage:

To show the sFlow flow_sampler information of ports which have been created:

```
DGS-3450:admin# show sflow analyzer_server
Command: show sflow analyzer_server

sFlow Analyzer_server Information
-----
Server ID           : 1
Owner               : 1
Timeout             : Infinite
Current Countdown Time : Infinite
Collector Address   : 10.0.0.1
Collector Port      : 655
Max Datagram Size   : 301

Total Entries: 1

DGS-3450:admin#
```

STACKING COMMANDS

Stacking protocol is a special communication mechanism between devices. It is responsible for allowing multiple devices to combine together, working in the same configuration. To users, these devices work as a whole.

Stacking devices can provide more network bandwidth and reliability for users. A device down will not influence other devices in the same stacking topology.

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

Command	Parameters
config stacking_mode	[disable enable]
show stacking_mode	
config box_priority current_box_id	<value 1-12> priority <value 1-63>
config box_id current_box_id	<value 1-12> new_box_id [auto <value 1-12>]
show stack_information	
show stack_device	
config stacking force_master_role state	[enable disable]

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

config stacking_mode

Purpose	Used to configure the stacking mode.
Syntax	config stacking_mode [disable enable]
Description	The config stacking_mode command configures the state of the stacking function. By default stacking mode is disabled. Administrators need to specifically configure the stacking mode to make the switch stackable. The user can only change the stacking mode when the Switch is operating in standalone mode.
Parameters	<i>stacking_mode</i> - Used to enable or disable the switch's stacking capability.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable stacking mode:

```
DGS-3450:admin# config stacking_mode enable
Command: config stacking_mode enable
```

```
Changing the stacking mode may cause the device to restart. Do you still want to
continue?(y/n) y
Please wait, the switch is rebooting...
```

show stacking_mode

Purpose	Used to display the current stacking mode.
Syntax	show stacking_mode
Description	The show stacking_mode command displays the current stacking mode.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To display the stacking mode:

```
DGS-3450:admin# show stacking_mode
Command: show stacking_mode

Stacking mode   : Enabled

DGS-3450:admin#
```

config box_priority

Purpose	Used to configure the box priority of the switch.
Syntax	config box_priority current_box_id <value 1-12> priority <value 1-63>
Description	The config box_priority command configures the box priority of the switch, which determines the box that will become the master. A lower number means a higher priority. The new priority will take effect after the user reboots the switch.
Parameters	<i>current_box_id</i> - Specifies the switch being configured. The range is 1-12 <i>priority</i> - Specifies the priority assigned to the box, with a lower number meaning a higher priority. The range is 1-63.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the box priority of the Switch to have an ID of 1 and a priority value of 1:

```
DGS-3450:admin# config box_priority current_box_id 1 priority 1
Command: config box_priority current_box_id 1 priority 1

Success.

DGS-3450:admin#
```

config box_id

Purpose	Used to configure the box ID. Users can use this command to reassign box IDs.
Syntax	config box_id current_box_id <value 1-12> new_box_id [auto <value 1-12>]
Description	The config box_id command configures the box ID. By default, the box ID is automatically assigned by the system based topology election results. Administrators can assign box IDs statically. The new box ID will take effect after the unit reboots. Each unit in the Switch stack must have a unique box ID. If there are duplicate IDs, the stack system will not stack properly.
Parameters	<i>current_box_id</i> - Specifies the switch being configured. The parameter range is 1-12.

config box_id

new_box_id - Specifies the new ID that will be assigned to the box. The parameter range is 1-12.

auto - Allows the box ID to be assigned automatically by the stack system. The new box ID will take effect after the next reboot.

Restrictions Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the Switch that has a current box ID of 1 to have an automatic ID assigned by the Switch:

```
DGS-3450:admin# config box_id current_box_id 1 new_box_id auto
```

```
Command: config box_id current_box_id 1 new_box_id auto
```

Success.

```
DGS-3450:admin#
```

show stack_information

Purpose Used to display the stack information.

Syntax **show stack_information**

Description The show stack_information command displays stacking information.

Parameters None.

Restrictions None.

Example usage:

To display the stack information:

```
DGS-3450:admin# show stack_information
```

```
Command: show stack_information
```

```
Topology      :Duplex_Chain
```

```
My Box ID     :3
```

```
Master ID     :3
```

```
Box Count     :1
```

```
Force Master Role: Enable
```

Box ID	User Set	Type	Exist	Prio- rity	MAC	Prom Version	Runtime Version	H/W Version
1	-	DGS-XXXXXS	No					
2	-	NOT_EXIST	No					
3	User	DGS-3450	Exist	0	00-00-11-33-66-33	1.00.B007	2.70.B56	A1
4	-	NOT_EXIST	No					
5	-	NOT_EXIST	No					
6	-	NOT_EXIST	No					
7	-	NOT_EXIST	No					
8	-	NOT_EXIST	No					

```
DGS-3450:admin#
```

show stack_device

Purpose	Used to display information about the devices in the stack.
Syntax	show stack_device
Description	The show stack_device command displays stack device information.
Parameters	None.
Restrictions	None.

Example usage:

To display the stack device information:

```
DGS-3450:admin# show stack_device
Command: show stack_device

Box ID      Box Type      H/W Version  Serial Number
-----
 1          DGS-3450     0A1          1234567890123
 3          DGS-3450     0A1          2345678901234

DGS-3450:admin#
```

config stacking force_master_role

Purpose	This command is used to configure the stacking force master role state.
Syntax	config stacking force_master_role state [enable disable]
Description	This command is used to ensure the master role is unchanged when new device add to current stacking topology. If the state is enabled, the master's priority will become zero after the stacking has stabilized.
Parameters	<i>force_master_role</i> - Used to enable or disable the switch's Stacking Force Master Role state. The default setting is disabled.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable the stacking force master role state:

```
DGS-3450:admin# config stacking force_master_role state enable
Command: config stacking force_master_role state enable

Success.

DGS-3450:admin#
```

STATIC MAC-BASED VLAN COMMANDS

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

For bridges that implement MAC-based VLAN classification, the VID associated with an Untagged or Priority-tagged Frame is determined based on the source MAC address. The each entry of VLAN_MAC table specifies a relationship for a source MAC address with a VLAN. If the source MAC address of ingress untagged or priority-tagged frame is match with the entry, the VLAN of the frame will be assigned according VLAN assignment rule in the entry.

Command	Parameters
create mac_based_vlan mac_address	<macaddr> vlan [<vlan_name 32> vlanid <vlanid 1-4094>]
delete mac_based_vlan	[mac_address <macaddr> all]
show mac_based_vlan	{mac_address <macaddr> [vlan <vlan_name 32>]}

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

create mac_based_vlan

Purpose	Used to create a static mac-based vlan entry.
Syntax	create mac_based_vlan mac_address <macaddr> vlan [<vlan_name 32> vlanid <vlanid 1-4094>]
Description	<p>This command only needs to be supported by the model which supports mac-based VLAN. The user can use this command to create a static mac-based VLAN entry.</p> <p>When a static mac_based_vlan entry is created for a user, the traffic from this user will be able to be serviced under the specified VLAN regardless of the authentication function operated on this port.</p> <p>There is a global limitation of the maximum entries supported for the static mac-based entry. The maximum value is 1024.</p>
Parameters	<p><i>mac_address</i> – The MAC address.</p> <p><i>vlan</i> – The VLAN to be associated with the MAC address.</p> <p><i>vlanid</i> - The VLAN ID to be associated with the MAC address.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage

To create mab_local:

```
DGS-3450:admin# create mac_based_vlan mac_address 00-00-00-00-00-01 vlan default
Command: create mac_based_vlan mac_address 00-00-00-00-00-01 vlan default

Success.

DGS-3450:admin#
```

delete mac_based_vlan

Purpose	Used to delete the static MAC-based VLAN entry.
Syntax	delete mac_based_vlan [mac_address <macaddr> all]
Description	Use this command to delete a database entry. If the mac_address and vlan is not specified, all static entries associated with the port will be removed.
Parameters	<i>mac_address</i> – The MAC address.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage

To delete a static mac-based-vlan entry:

```
DGS-3450:admin# delete mac_based_vlan mac_address 00-00-00-00-00-01
Command: delete mac_based_vlan mac mac_address 00-00-00-00-00-01

Success.

DGS-3450:admin#
```

show mac_based_vlan

Purpose	Used to show the static or dynamic MAC-based VLAN entry.
Syntax	show mac_based_vlan {mac_address <macaddr> [vlan <vlan_name 32>]}
Description	User can use this command to display the static or dynamic MAC-Based VLAN entry.
Parameters	<i>mac_address</i> – Specifies the entry that you would like to display. <i>vlan</i> – Specifies the VLAN to be associated with the MAC address that you would like to display.
Restrictions	None.

Example usage

To display the static MAC-based VLAN entry:

```
DGS-3450:admin# show mac_based_vlan
Command: show mac_based_vlan

MAC Address          VLAN      Status      Type
-----
00-80-e0-14-a7-57    200       Active      Static
00-80-c2-33-c3-45    200       Inactive    Mac based access control
00-80-c2-33-c3-45    300       Active      JWAC
00-80-c2-33-c3-90    400       Active      WAC
00-a2-44-17-32-98    500       Active      Multiple Authentication
00-a2-44-17-32-97    500       Active      802.1x
Total Entries : 6

DGS-3450:admin#
```

SUBNET VLAN COMMANDS

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

Command	Parameters
create subnet_vlan	[network <network_address> ipv6network <ipv6networkaddr>] [vlan <vlan_name 32> vlanid <vlanid 1-4094>] {priority <value 0-7>}
delete subnet_vlan	[network <network_address> ipv6network <ipv6networkaddr>] vlan <vlan_name 32> vlanid <vidlist> all]
show subnet_vlan	{[network <network_address> ipv6network <ipv6networkaddr>] vlan <vlan_name 32> vlanid <vidlist>]}
config vlan_precedence ports	<portlist> [mac_based_vlan subnet_vlan]
show vlan_precedence ports	{<portlist>}

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

create subnet_vlan

Purpose	Use this command to create a subnet VLAN entry.
Syntax	create subnet_vlan [network <network_address> ipv6network <ipv6networkaddr>] [vlan <vlan_name 32> vlanid <vlanid 1-4094>] { priority <value 0-7>}
Description	The user can use this command to create a subnet VLAN entry. A subnet VLAN entry is an IP subnet-based VLAN classification rule. If an untagged or priority-tagged IP packet is received on a port, its source IP address will be used to match the subnet VLAN entries. If the source IP is in the subnet of an entry, the packet will be classified to the VLAN defined for this subnet.
Parameters	<i>network</i> - To specify an IPv4 network address. The format is ipaddress/prefix length. <i>ipv6network</i> - To specify an IPv6 network address. The format is ipaddress/prefix length. The prefix length of IPv6 network address shall not be greater than 64. <i>vlan</i> - The vlan to be associated with the subnet. You can specify a vlan name or vlan ID. The vlan must be existed static vlan. <i>priority</i> - The priority to be associated with the subnet. Its range is 0-7.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

This example shows how to create a subnet VLAN entry:

```
DGS-3450:admin# create subnet_vlan network 172.168.1.1/24 vlan v2 priority 2
Command: create subnet_vlan source_ip 172.168.1.1/24 vlan v2 priority 2

Success.

DGS-3450:admin#
```

This example shows how to create an IPv6 subnet VLAN entry:

```
DGS-3450:admin# create subnet_vlan ipv6network fe80::250:baff::0/64 vlan v2 priority 2
Command: create subnet_vlan ipv6network fe80::250:baff::0/64 vlan v2 priority 2

Success.

DGS-3450:admin#
```

delete subnet_vlan

Purpose	Use this command to delete subnet vlan entry.
Syntax	delete subnet_vlan [network <network_address> ipv6network <ipv6networkaddr>] vlan <vlan_name 32> vlanid <vidlist> all]
Description	This command is used to delete subnet vlan entry from switch. You can delete subnet vlan entry by IP subnet or vlan, or delete all subnet vlan entries.
Parameters	<p><i>network</i> - To specify an IPv4 network address or IPv6 network address. The format is ipaddress / prefix length.</p> <p><i>ipv6network</i> - To specify an IPv6 network address. The format is ipaddress / prefix length. The prefix length of IPv6 network address shall not be greater than 64.</p> <p><i>vlan</i> - If specify the vlan, all subnet vlan entries that associated with this vlan will be deleted.</p> <p><i>vidlist</i> - Specifies a list of VLANs by VLAN ID.</p> <p><i>all</i> - If specify all, all subnet vlan entries will be deleted.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

This example shows how to delete a subnet VLAN entry:

```
DGS-3450:admin# delete subnet_vlan network 172.168.1.1/24
Command:delete subnet_vlan network 172.168.1.1/24

Success.

DGS-3450:admin#
```

This example shows how to delete all subnet VLAN entries:

```
DGS-3450:admin# delete subnet_vlan all
Command:delete subnet_vlan all

Success.

DGS-3450:admin#
```

show subnet_vlan

Purpose	Use this command to display subnet vlan entry information.
Syntax	show subnet_vlan {[network <network_address> ipv6network <ipv6networkaddr>] vlan <vlan_name 32> vlanid <vidlist>]}
Description	This command is used to display subnet vlan entry information.
Parameters	<p><i>network</i> - To specify an IPv4 network address. If network address is not specified, all subnet vlan entries will be displayed.</p> <p><i>ipv6network</i> - To specify an IPv6 network address. If network address is not specified, all subnet vlan entries will be displayed.</p>

show subnet_vlan

vlan - If specify the vlan, all subnet vlan entries that associated with this vlan will be displayed. If no parameter is specified, all subnet vlan entries will be displayed.
vidlist - Specifies a list of VLANs by VLAN ID.

Restrictions None.

Example usage:

This example shows how to show a specified subnet VLAN entry:

```
DGS-3450:admin# show subnet_vlan network 172.168.1.1/24
Command:show subnet_vlan network 172.168.1.1/24

IP Address/Subnet Mask          VLAN      Priority
-----
172.168.1.1/24                  10        1

DGS-3450:admin#
```

This example shows how to display a specified IPv6 subnet VLAN entry:

```
DGS-3450:admin# show subnet_vlan network fe80::250:baff::0/64
Command: show subnet_vlan network fe80::250:baff::0/64

IP Address/Subnet Mask          VLAN      Priority
-----
fe80::250:baff::0/64           10        1

DGS-3450:admin#
```

This example shows how to show all subnet VLAN entries:

```
DGS-3450:admin# show subnet_vlan
Command:show subnet_vlan

IP Address/Subnet Mask          VLAN      Priority
-----
172.168.1.1/24                  10        2
172.18.211.1/255.255.255.0      20        3
172.18.211.6/24                 5         1
fe80::250:baff::0/64           10        2

Total entry:4

DGS-3450:admin#
```

config vlan_precedence ports

Purpose	Use this command to configure the vlan classification precedence.
Syntax	config vlan_precedence ports <portlist> [mac_based_vlan subnet_vlan]
Description	This command is used to configure vlan classification precedence on each port. You can specify the order of MAC-based VLAN classification and subnet VLAN classification. If a port's VLAN classification is MAC-based precedence, MAC-based VLAN classification will process at first. If MAC-based VLAN classification fails, the subnet VLAN classification will be executed.

config vlan_precedence ports

	If a port's VLAN classification is subnet VLAN precedence, the subnet VLAN classification will process at first. If subnet VLAN classification fails, the MAC-based VLAN classification will be executed.
Parameters	<p><i>portlist</i> - A range of ports to configure.</p> <p><i>mac_based_vlan</i> - If the parameter is specified, the MAC-based VLAN classification is precedence than subnet VLAN classification.</p> <p><i>subnet_vlan</i> - If the parameter is specified, the subnet VLAN classification is precedence than MAC-based VLAN classification.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

This example shows how to configure subnet VLAN classification precedence on port 1:

```
DGS-3450:admin# config vlan_precedence 1 subnet_vlan
Command: config vlan_precedence 1 subnet_vlan

Success.

DGS-3450:admin#
```

show vlan_precedence ports

Purpose	Use this command to show vlan classification precedence.
Syntax	show vlan_precedence ports {<portlist>}
Description	This command is used to show vlan classification precedence.
Parameters	<i>portlist</i> - A range of ports will display. If no parameters is specified, all ports vlan classification precedence will display.
Restrictions	None.

Example usage:

This example shows how to display VLAN classification precedence on ports 1-3:

```
DGS-3450:admin# show vlan_precedence
Command: show vlan_precedence

Port      VLAN Precedence
-----  -----
1         MAC-Based VLAN
2         Subnet VLAN
3         MAC-Based VLAN

Total entry: 3

DGS-3450:admin#
```


SWITCH PORT COMMANDS

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

Command	Parameters
config ports	[<portlist> all] {medium_type [fiber copper]} { speed[auto {capability_advertised {10_half 10_full 100_half 100_full 1000_full } } 10_half 10_full 100_half 100_full 1000_full {[master slave]}] auto_negotiation restart_an flow_control [enable disable] learning [enable disable] state [enable disable] [description <desc 1-32> clear_description]}
show ports	{<portlist>} {[description err_disabled auto_negotiation details media_type]}

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

config ports

Purpose	Used to configure the Switch's Ethernet port settings.
Syntax	config ports [<portlist> all] { medium_type [fiber copper]} { speed [auto { capability_advertised {10_half 10_full 100_half 100_full 1000_full } } 10_half 10_full 100_half 100_full 1000_full { master slave }]] auto_negotiation restart_an flow_control [enable disable] learning [enable disable] state [enable disable] [description <desc 1-32> clear_description]
Description	This command allows for the configuration of the Switch's Ethernet ports. Only the ports listed in the <portlist> will be affected.
Parameters	<p><i>all</i> – Configure all ports on the Switch.</p> <p><portlist> – Specifies a port or range of ports to be configured. The beginning and end of the port list range are separated by a dash.</p> <p><i>medium_type</i> [fiber copper] – This applies only to the Combo ports. If configuring the Combo ports this defines the type of transport medium used.</p> <p><i>speed</i> – Allows the user to adjust the speed for a port or range of ports. The user has a choice of the following:</p> <ul style="list-style-type: none"> • <i>auto</i> – Enables auto-negotiation for the specified range of ports. • [10 100 1000] – Configures the speed in Mbps for the specified range of ports. Gigabit ports are statically set to 1000 and cannot be set to slower speeds. • [half full] – Configures the specified range of ports as either full-duplex or half-duplex. • [master slave] – The master setting (1000M/Full_M) will allow the port to advertise capabilities related to duplex, speed and physical layer type. The master setting will also determine the master and slave relationship between the two connected physical layers. This relationship is necessary for establishing the timing control between the two physical layers. The timing control is set on a master physical layer by a local source. The slave setting (1000M/Full_S) uses loop timing, where the timing comes from a data stream received from the master. If one connection is set for 1000M/Full_M, the other side of the connection must be set for 1000M/Full_S. Any other configuration will result in a link down status for both ports. <p><i>flow_control</i> [enable disable] – Enable or disable flow control for the specified ports.</p> <p><i>learning</i> [enable disable] – Enables or disables the MAC address learning on the specified range of ports.</p> <p><i>state</i> [enable disable] – Enables or disables the specified range of ports. If the specific ports are in an error-disabled state configuring their state to enable will recover these ports from disabled to enabled state.</p> <p><i>description</i> <desc 1-32> – Enter an alphanumeric string of no more than 32 characters to describe a selected port interface.</p> <p><i>clear_description</i> – Enter this command to clear the port description of the selected port(s).</p>
Restrictions	Only Administrator and Operator-level users can issue this command.



NOTE: Gigabit Ethernet ports are statically set to 1 Gbps, and their speed cannot be modified. The DGS-3400 series fiber ports only support 1000M_full.

Example usage:

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

```
DGS-3450:admin# config ports 1:1-1:3 speed 10_full learning enable state enable
flow_control enable
Command: config ports 1:1-1:3 speed 10_full learning enable state enable flow_control
enable

Success.

DGS-3450:admin#
```

To configure the speed of ports 1 to 3 of unit 1 to be auto, capability advertised with half duplex and full duplex ports:

```
DGS-3450:admin# config ports 1:1-1:3 speed auto capability_advertised 10_half 10_full
Command: config ports 1:1-1:3 speed auto capability_advertised 10_half 10_full

Success.

DGS-3450:admin#
```

show ports

Purpose	Used to display the current configuration of a range of ports.
Syntax	show ports {<portlist>} [{description err_disabled auto_negotiation details media_type}]
Description	This command is used to display the current configuration of a range of ports.
Parameters	<p><i><portlist></i> – Specifies a port or range of ports to be displayed. The beginning and end of the port list range are separated by a dash.</p> <p><i>{description}</i> – Adding this parameter to the show ports command indicates that a previously entered port description will be included in the display.</p> <p><i>err_disabled</i> – Choosing this parameter will display ports that have been disconnected due to an error on the port, such as a Loopback Detection.</p> <p><i>auto_negotiation</i> – Choosing this parameter will display the port auto-negotiation information in the display.</p> <p><i>details</i> - Displays the port detailed information</p> <p><i>media_type</i> - Displays port transceiver type.</p>
Restrictions	None.

Example usage:

To display the configuration of all ports on a switch:

DGS-3450:admin# show ports

Command: show ports

Port	Port State	Settings Speed/Duplex/FlowCtrl	Connection Speed/Duplex/FlowCtrl	Address Learning
1:1	Enabled	Auto/Disabled	Link Down	Enabled
1:2	Enabled	Auto/Disabled	Link Down	Enabled
1:3	Enabled	Auto/Disabled	Link Down	Enabled
1:4	Enabled	Auto/Disabled	Link Down	Enabled
1:5	Enabled	Auto/Disabled	Link Down	Enabled
1:6	Enabled	Auto/Disabled	Link Down	Enabled
1:7	Enabled	Auto/Disabled	Link Down	Enabled
1:8	Enabled	Auto/Disabled	Link Down	Enabled
1:9	Enabled	Auto/Disabled	Link Down	Enabled
1:10	Enabled	Auto/Disabled	Link Down	Enabled
1:11	Enabled	Auto/Disabled	Link Down	Enabled
1:12	Enabled	Auto/Disabled	Link Down	Enabled
1:13	Enabled	Auto/Disabled	Link Down	Enabled
1:14	Enabled	Auto/Disabled	Link Down	Enabled
1:15	Enabled	Auto/Disabled	Link Down	Enabled
1:16	Enabled	Auto/Disabled	Link Down	Enabled
1:17	Enabled	Auto/Disabled	Link Down	Enabled
1:18	Enabled	Auto/Disabled	Link Down	Enabled
1:19	Enabled	Auto/Disabled	Link Down	Enabled

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

To display the configuration of all ports on the Switch, with a description:

DGS-3450:admin# show ports description

Command: show ports description

Port	Port State	Settings Speed/Duplex/FlowCtrl	Connection Speed/Duplex/FlowCtrl	Address Learning
1:1	Enabled	Auto/Disabled	Link Down	Enabled
	Description:			
1:2	Enabled	Auto/Disabled	Link Down	Enabled
	Description:			
1:3	Enabled	Auto/Disabled	Link Down	Enabled
	Description:			
1:4	Enabled	Auto/Disabled	Link Down	Enabled
	Description:			
1:5	Enabled	Auto/Disabled	Link Down	Enabled
	Description:			
1:6	Enabled	Auto/Disabled	Link Down	Enabled
	Description:			
1:7	Enabled	Auto/Disabled	Link Down	Enabled
	Description:			
1:8	Enabled	Auto/Disabled	Link Down	Enabled
	Description:			
1:9	Enabled	Auto/Disabled	Link Down	Enabled
	Description:			

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

To display the Error Disabled ports:

```
DGS-3450:admin# show ports err_disabled
Command : show ports err_disabled

Port      Port      Connection status      Reason
  State

-----
1:2      Enabled  Err-disabled          Storm control
          Desc: Port 2
1:8      Enabled  Err-disabled          Storm control
          Desc: Port 8

DGS-3450:admin#
```

To display the Error Disabled ports:

```
DGS-3450:admin# show ports err_disabled
Command : show ports err_disabled

Port      Port      Connection status      Reason
  State

-----
1:2      Enabled  Err-disabled          Storm control
          Desc: Port 2
1:8      Enabled  Err-disabled          Storm control
          Desc: Port 8

DGS-3450:admin#
```

To display the auto_negotiation ports:

```
DGS-3450:admin# show ports 1:1-1:3 auto_negotiation
Command: show ports 1:1-1:3 auto_negotiation

Port : 1:1
-----
Auto Negotiation      : Enabled
Capability Bits       : 1000M_Full
Capability Advertised Bits : 1000M_Full
Capability Received Bits  :

Port : 1:2
-----
Auto Negotiation      : Enabled
Capability Bits       : 1000M_Full
Capability Advertised Bits : 1000M_Full
Capability Received Bits  :

Port : 1:3
-----
Auto Negotiation      : Enabled
Capability Bits       : 1000M_Full
Capability Advertised Bits : 1000M_Full
Capability Received Bits  :

DGS-3450:admin#
```


SYSLOG OR TRAP SOURCE-INTERFACE COMMANDS

The syslog or trap source-interface function is used for selecting a fixed interface as the source interface to send syslog or trap message. It also provides a mechanism to select a certain IP address from the specified interface as the source address to send the message. The servers beyond different networks receive the syslog or trap message always come from a fixed source IP address, it is helpful to use the source IP address to identify the switch.

The Syslog or Trap Source-Interface commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameters
config syslog source_ipif	[<ipif_name> {<ipaddr>} none]
show syslog source_ipif	
config trap source_ipif	[<ipif_name> {<ipaddr> <ipv6addr>} none]
show trap source_ipif	

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

config syslog source_ipif

Purpose	Configure syslog source IP interface.
Syntax	config syslog source_ipif [<ipif_name> {<ipaddr>} none]
Description	This command is used to configure syslog source IP interface.
Parameters	<i>ipif_name</i> - IP interface name. If only specify this parameter, the least IPv4 address and the smallest IPv6 address of ipif_name will be used as source IP addresses. <i>none</i> - For clear the configured source IP interface. <i>ipaddr</i> - Specify the IPv4 address.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

Configure syslog source IP interface:

```
DGS-3450:admin# config syslog source_ipif ipif3 14.0.0.5
Command: config syslog source_ipif ipif3 14.0.0.5
```

Success

```
DGS-3450:admin#
```

To clear the configured source IP interface for syslog:

```
DGS-3450:admin# config syslog source_ipif none
Command: config syslog source_ipif none
```

Success

```
DGS-3450:admin#
```

show syslog source_ipif

Purpose	Show syslog source IP interface.
Syntax	show syslog source_ipif
Description	This command is used to display the syslog source IP interface.
Parameters	None.
Restrictions	None.

Example usage:

Show syslog source IP interface:

```
DGS-3450:admin# show syslog source_ipif
Command: show syslog source_ipif

Syslog Source IP Interface Configuration:

IP Interface           : ipif3
IPv4 Address           : 14.0.0.3

DGS-3450:admin#
```

config trap source_ipif

Purpose	Configure trap source IP interface.
Syntax	config trap source_ipif [<ipif_name> {<ipaddr> <ipv6addr>} none]
Description	This command is used to configure trap source IP interface.
Parameters	<i>ipif_name</i> - IP interface name. If only specify this parameter, the least IPv4 address and the smallest IPv6 address of ipif_name will be used as source IP addresses. <i>none</i> - For clearing the configured source IP interface. <i>ipaddr</i> - IPv4 address. <i>ipv6addr</i> - IPv6 address.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

Configure trap source IP interface:

```
DGS-3450:admin# config trap source_ipif inter4
Command: config trap source_ipif inter4

Success

DGS-3450:admin#
```

To clear the configured trap source IP interface:


```
DGS-3450:admin# config trap source_ipif none
Command: config trap source_ipif none

Success

DGS-3450:admin#
```

show trap source_ipif

Purpose	Show trap source IP interface.
Syntax	show trap source_ipif
Description	This command is used to display the trap source IP interface.
Parameters	None.
Restrictions	None.

Example usage:

Show trap source IP interface:

```
DGS-3450:admin# show trap source_ipif
Command: show trap source_ipif

Trap Source IP Interface Configuration:

IP Interface           : ipif4
IPv4 Address           : None
IPv6 address           : 3000::52

DGS-3450:admin#
```

SYSTEM LOG COMMANDS

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

Command	Parameters
clear log	
show log	{{[index <value_list> severity {emergency alert critical error warning notice informational debug <level_list 0-7>}]}}
enable syslog	
disable syslog	
show syslog	
config syslog host	<index 1-4> [severity [emergency alert critical error warning notice informational debug <level 0-7>] facility [local0 local1 local2 local3 local4 local5 local6 local7] udp_port <udp_port_number> ipaddress <ipaddr> state [enable disable]](1)
create syslog host	<index 1-4> {severity [emergency alert critical error warning notice informational debug all <level 0-7>] facility [local0 local1 local2 local3 local4 local5 local6 local7] udp_port <udp_port_number> ipaddress<ipaddr> state [enable disable]}
delete syslog host	[<index 1-4> all]
show syslog host	{<index 1-4>}
config log_save_timing	[time_interval <min 1-65535> on_demand log_trigger]
show log_save_timing	
show attack_log	{unit <unit_id 1-12>} {index <value_list>}
clear attack_log	{unit <unit_id 1-12> all}
upload attack_log_toTFTP	[<ipaddr> <ipv6addr> <domain_name 255>] dest_file <path_filename 64> {unit <unit_id 1-12>}
upload attack_log_toRCP	{{username <username 15>} {<ipaddr>} dest_file <path_filename 64> rcp: <string 128>] {unit <unit_id 1-12>}

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

clear log

Purpose	Used to clear the switch's history log.
Syntax	clear log
Description	This command clears the switch's history log.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To clear the switch's history log:

```
DGS-3450:admin# clear log
Command: clear log

Success.

DGS-3450:admin#
```

show log

Purpose	Used to display the switch's history log.																								
Syntax	show log {[index <value_list> severity {emergency alert critical error warning notice informational debug <level_list 0-7>}]}																								
Description	This command displays the switch's history log. When the log is empty, the prompt message "Log is empty." will be displayed.																								
Parameters	<p><i>index</i> - The show log command will display the history log between the log number of X and Y. For example, showing log index 1-5 will display the history log from 1 to 5. If no parameter is specified, all history log entries will be displayed.</p> <table border="0"> <tr> <td><i>severity</i></td> <td><i>emergency</i></td> <td>Severity level 0</td> </tr> <tr> <td></td> <td><i>alert</i></td> <td>Severity level 1</td> </tr> <tr> <td></td> <td><i>critical</i></td> <td>Severity level 2</td> </tr> <tr> <td></td> <td><i>error</i></td> <td>Severity level 3</td> </tr> <tr> <td></td> <td><i>warning</i></td> <td>Severity level 4</td> </tr> <tr> <td></td> <td><i>notice</i></td> <td>Severity level 5</td> </tr> <tr> <td></td> <td><i>informational</i></td> <td>Severity level 6</td> </tr> <tr> <td></td> <td><i>debug</i></td> <td>Severity level 7</td> </tr> </table> <p><i>level_list</i> - Specifies a list of severity levels to be displayed. If there is more than one severity level, please separate them by comma. The level number is from 0 to 7.</p>	<i>severity</i>	<i>emergency</i>	Severity level 0		<i>alert</i>	Severity level 1		<i>critical</i>	Severity level 2		<i>error</i>	Severity level 3		<i>warning</i>	Severity level 4		<i>notice</i>	Severity level 5		<i>informational</i>	Severity level 6		<i>debug</i>	Severity level 7
<i>severity</i>	<i>emergency</i>	Severity level 0																							
	<i>alert</i>	Severity level 1																							
	<i>critical</i>	Severity level 2																							
	<i>error</i>	Severity level 3																							
	<i>warning</i>	Severity level 4																							
	<i>notice</i>	Severity level 5																							
	<i>informational</i>	Severity level 6																							
	<i>debug</i>	Severity level 7																							
Restrictions	None.																								

Example usage:

To display the switch's history log:

```
DGS-3450:admin# show log index 1-3
Command: show log index 1-3
```

Index	Date	Time	Level	Log Text
3	2008-10-17	15:00:14	INFO(1)	CLI(1):Successful login through Console (User name: Anonymous)
2	2008-10-17	10:50:36	WARN(3)	CLI(3):Console session timed out (Username: Anonymous)
1	2008-10-16	15:19:17	CRIT(5)	SNMP(2):SNMP request received from 10.0.0.27 with invalid community string!

```
DGS-3450:admin#
```

enable syslog

Purpose	Used to enable the sending of syslog messages.
Syntax	enable syslog
Description	This command enables the sending of syslog messages.

enable syslog

Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable the sending of syslog messages:

```
DGS-3450:admin# enable syslog
Command: enable syslog
```

Success.

```
DGS-3450:admin#
```

disable syslog

Purpose	Used to disable the sending of syslog messages.
Syntax	disable syslog
Description	This command disables the sending of syslog messages.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable the sending of syslog messages:

```
DGS-3450:admin# disable syslog
Command: disable syslog
```

Success.

```
DGS-3450:admin#
```

show syslog

Purpose	Used to display the syslog protocol global state.
Syntax	show syslog
Description	This command displays the syslog protocol global state.
Parameters	None.
Restrictions	None.

Example usage:

To display the syslog protocol global state:

```
DGS-3450:admin# show syslog
Command: show syslog

Syslog Global State: Enabled

DGS-3450:admin#
```

config syslog host

Purpose	Used to configure the syslog host configurations.																																								
Syntax	config syslog host <index 1-4> [severity [emergency alert critical error warning notice informational debug <level 0-7>] facility [local0 local1 local2 local3 local4 local5 local6 local7] udp_port <udp_port_number> ipaddress <ipaddr> state [enable disable]](1)																																								
Description	<p>This command configures the syslog host configurations. The user can choose and report a specific level of messages to a specific host. When the user chooses a specific level for a specific host, messages which are at that severity level or higher will be reported to the specified host.</p> <p>When the specified host doesn't exist, the prompt message, "The entry does not exist." will be displayed and this configuration will fail.</p> <p>When the IP address is invalid, the prompt message, "Invalid IP address." will be displayed and this configuration will fail.</p> <p>The prompt message, "The IP address has already been configured." will be prompted to the user when configuring syslog hosts with "all" option and just assigning one IP address to those hosts. This configuration will fail.</p> <p>When the specified IP address already exists, the prompt message, "The host IP address already exists." will be displayed and this configuration will fail.</p>																																								
Parameters	<p><i>host</i> - The host index or all hosts.</p> <table border="0"> <tr> <td style="padding-right: 20px;"><i>severity</i> -</td> <td style="padding-right: 20px;"><i>emergency</i></td> <td>Severity level 0</td> </tr> <tr> <td></td> <td><i>alert</i></td> <td>Severity level 1</td> </tr> <tr> <td></td> <td><i>critical</i></td> <td>Severity level 2</td> </tr> <tr> <td></td> <td><i>error</i></td> <td>Severity level 3</td> </tr> <tr> <td></td> <td><i>warning</i></td> <td>Severity level 4</td> </tr> <tr> <td></td> <td><i>notice</i></td> <td>Severity level 5</td> </tr> <tr> <td></td> <td><i>informational</i></td> <td>Severity level 6</td> </tr> <tr> <td></td> <td><i>debug</i></td> <td>Severity level 7</td> </tr> </table> <p><i>facility</i> - 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 below. This facility setting will be put in the syslog packet when it is sent to a specific syslog server.</p> <table border="0"> <tr> <td style="padding-right: 20px;"><i>local0</i></td> <td>user-defined facility</td> </tr> <tr> <td><i>local1</i></td> <td>user-defined facility</td> </tr> <tr> <td><i>local2</i></td> <td>user-defined facility</td> </tr> <tr> <td><i>local3</i></td> <td>user-defined facility</td> </tr> <tr> <td><i>local4</i></td> <td>user-defined facility</td> </tr> <tr> <td><i>local5</i></td> <td>user-defined facility</td> </tr> <tr> <td><i>local6</i></td> <td>user-defined facility</td> </tr> <tr> <td><i>local7</i></td> <td>user-defined facility</td> </tr> </table> <p><i>udp_port</i> - The UDP port number.</p> <p><i>ipaddr</i> - Specify the IP address for the host.</p> <p><i>ipv6addr</i> - Specify the IPv6 address for the host.</p>	<i>severity</i> -	<i>emergency</i>	Severity level 0		<i>alert</i>	Severity level 1		<i>critical</i>	Severity level 2		<i>error</i>	Severity level 3		<i>warning</i>	Severity level 4		<i>notice</i>	Severity level 5		<i>informational</i>	Severity level 6		<i>debug</i>	Severity level 7	<i>local0</i>	user-defined facility	<i>local1</i>	user-defined facility	<i>local2</i>	user-defined facility	<i>local3</i>	user-defined facility	<i>local4</i>	user-defined facility	<i>local5</i>	user-defined facility	<i>local6</i>	user-defined facility	<i>local7</i>	user-defined facility
<i>severity</i> -	<i>emergency</i>	Severity level 0																																							
	<i>alert</i>	Severity level 1																																							
	<i>critical</i>	Severity level 2																																							
	<i>error</i>	Severity level 3																																							
	<i>warning</i>	Severity level 4																																							
	<i>notice</i>	Severity level 5																																							
	<i>informational</i>	Severity level 6																																							
	<i>debug</i>	Severity level 7																																							
<i>local0</i>	user-defined facility																																								
<i>local1</i>	user-defined facility																																								
<i>local2</i>	user-defined facility																																								
<i>local3</i>	user-defined facility																																								
<i>local4</i>	user-defined facility																																								
<i>local5</i>	user-defined facility																																								
<i>local6</i>	user-defined facility																																								
<i>local7</i>	user-defined facility																																								

config syslog host

state - The syslog protocol is used for the transmission of event notification messages across networks to a host. The option enables or disables the host to receive such messages.

Restrictions

Only Administrator and Operator-level users can issue this command.

Example usage:

To configure syslog host configuration:

```
DGS-3450:admin# config syslog host all severity all facility local0
Command: config syslog host all severity all facility local0
```

Success.

```
DGS-3450:admin#
```

create syslog host

Purpose

Used to create a new syslog host.

Syntax

```
create syslog host <index 1-4> {severity [ emergency | alert | critical | error | warning |
notice | informational | debug] all | <level 0-7>} | facility [ local0 | local1 | local2 | local3 |
local4 | local5 | local6 | local7] | udp_port <udp_port_number> | ipaddress<ipaddr> |
state [ enable | disable]}
```

Description

This command creates a new syslog host. The user can choose and report specific levels of messages to a specific host. When the user chooses a specific level for a specific host, messages which are at that severity level or higher will be reported to that host.

When the IP address is invalid, the prompt message, "Invalid IP address," will be displayed and this configuration will fail.

When the specified IP address already exists, the prompt message, "The host IP address already exists," will be displayed and this configuration will fail.

When the specified host already exists, the prompt message, "The entry already exists," will be displayed and this configuration will fail.

Parameters

host - The host index or all hosts

<i>severity</i>	<i>emergency</i>	Severity level 0
	<i>alert</i>	Severity level 1
	<i>critical</i>	Severity level 2
	<i>error</i>	Severity level 3
	<i>warning</i>	Severity level 4
	<i>notice</i>	Severity level 5
	<i>informational</i>	Severity level 6
	<i>debug</i>	Severity level 7
	<i>all</i>	Severity level All

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. The facilities that have been designated are shown below.

<i>local0</i>	user-defined facility
<i>local1</i>	user-defined facility
<i>local2</i>	user-defined facility
<i>local3</i>	user-defined facility
<i>local4</i>	user-defined facility

create syslog host

local5 user-defined facility
local6 user-defined facility
local7 user-defined facility

udp_port - The UDP port number.

state - The syslog protocol is used for the transmission of event notification messages across networks to a host. This option enables or disables the hosts that will receive such messages.

ipaddress – Specify the IP address used here.

Restrictions Only Administrator and Operator-level users can issue this command.

Example usage:

To create a new syslog host:

```
DGS-3450:admin# create syslog host 1 ipaddress 10.90.90.1 severity all facility local0
Command: create syslog host 1 ipaddress 10.90.90.1 severity all facility local0
```

Success.

```
DGS-3450:admin#
```

delete syslog host

Purpose Used to delete the syslog host(s).

Syntax **delete syslog host [<index 1-4> | all]**

Description This command deletes the syslog host(s).

When the specified host doesn't exist, the prompt message, "The entry does not exist," will be displayed and this configuration will fail.

Parameters *host [<index 1-4> | all]* - Host index or all hosts.

Restrictions Only Administrator and Operator-level users can issue this command.

Example usage:

To delete a syslog host:

```
DGS-3450:admin# delete syslog host 4
Command: delete syslog host 4
```

Success.

```
DGS-3450:admin#
```

show syslog host

Purpose Used to display syslog host configurations.

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

Description This command displays the syslog host configurations.

Parameters *index* - The host index.

If no parameter is specified, all hosts will be displayed.

show syslog host

Restrictions None.

Example usage:

To display syslog host configurations:

```
DGS-3450:admin# show syslog host
Command: show syslog host

Syslog Global State: Disabled

Host 1
  IP Address       : 10.1.1.2
  Severity         : Warning
  Facility         : Local0
  UDP port         : 514
  Status           : Disabled

Host 2
  IP Address       : 3000:501:100:ffff:101:202:303:1
  Severity         : Emergency
  Facility         : Local0
  UDP port         : 514
  Status           : Disabled

Host 3
  IP Address       : 10.21.13.1
  Severity         : All
  Facility         : Local0
  UDP port         : 514
  Status           : Disabled

Total Entries : 3

DGS-3450:admin#
```

config log_save_timing

Purpose	Used to configure the method for saving the log.
Syntax	config log_save_timing [time_interval <min 1-65535> on_demand log_trigger]
Description	This command is used to set the method for saving the log.
Parameters	<p><i>time_interval</i> - Save log to flash every xxx minutes. (If no new log events occur in this period, don't save.)</p> <p><i>on_demand</i> - Save log to flash whenever the user enters the "save log" or "save all" command. The default setting is on_demand.</p> <p><i>log_trigger</i> - Save log to flash whenever a new log event arrives.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the method for saving a log as on demand:


```
DGS-3450:admin# config log_save_timing on_demand
Command: config log_save_timing on_demand

Success.

DGS-3450:admin#
```

show log_save_timing

Purpose	Used to show the method for saving the log.
Syntax	show log_save_timing
Description	To show the method for saving the log.
Parameters	None.
Restrictions	None.

Example usage:

To show the timing method used for saving the log:

```
DGS-3450:admin# show log_save_timing
Command: show log_save_timing

Saving log method: on_demand

DGS-3450:admin#
```

show attack_log

Purpose	Displays the attack log messages.
Syntax	show attack_log {unit <unit_id 1-n>} {index <value_list>}
Description	Displays the attack log messages. The attack log message refers to log messages driven by modules such as DOS and the IP-MAC-port binding module. This type of log message may generate a large amount of messages and quickly cause the system to run out of system log storage. Therefore, for this type of log messages only the first log that is generated each minute can be stored in the system log, with the rest of them being stored in a separate table named attack log.
Parameters	<p>When the attack log is empty, the prompt message, "Log is empty," will be displayed.</p> <p><i>unit</i> - The attack log messages on the specified unit will be displayed. If unit ID is specified, then this unit will be referred to as the master unit.</p> <p><i>index</i> - The list of index numbers of the entries that need to be displayed. For example, show attack_log index 1-5 will display the attack log messages from 1 to 5.</p> <p>If no parameter is specified, all entries in the attack log will be displayed.</p>
Restrictions	None.

Example usage:

To show dangerous messages on the master:

```
DGS-3450:admin# show attack_log index 1
```

```
Command: show attack_log index 1
```

Index	Date	Time	Level	Log Text
1	2008-10-17	15:00:14	CRIT(2)	Land attack is blocked from (IP: 10.72.24.1 Port: 7)

```
DGS-3450:admin#
```

clear attack_log

Purpose	Used to clear the attack log.
Syntax	clear attack_log {unit <unit_id 1-n> all}
Description	Used to clear the attack log.
Parameters	<i>unit</i> - The attack log messages on the specified unit will be cleared. If specified, this unit will be referred to as the master unit.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To clear the master's attack log:

```
DGS-3450:admin# clear attack_log
```

```
Command: clear attack_log
```

```
Success.
```

```
DGS-3450:admin#
```

upload attack_log_toTFTP

Purpose	Used to upload the attack log on a unit.
Syntax	upload attack_log_toTFTP [<ipaddr> <ipv6addr> <domain_name 255>] dest_file <path_filename 64> {unit <unit_id 1-12>}
Description	To upload the attack log stored on a unit. When the attack log is empty, the prompt message, "Log is empty," will be displayed.
Parameters	<i>unit</i> - The attack log messages on the specified unit will be uploaded to the TFTP server. If specified, this unit will be referred to as the master unit. <i><ipaddr></i> - The IPv4 address of the TFTP server. <i><ipv6addr></i> - The IPv6 address of the TFTP server. <i><domain_name 255></i> - The domain name of the TFTP server. <i>dest_file</i> - The destination file name. <i><path_filename 64></i> - Specifies the path name on the TFTP server to hold the attack log.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To upload the master's dangerous log:

```
DGS-3450:admin# upload attack_log_toTFTP 10.9.68.9 dest_file test
Command: upload attack_log_toTFTP 10.9.68.9 dest_file test

Success.

DGS-3450:admin#
```

upload attack_log_toRCP

Purpose	Used to upload the attack log file from the device to an RCP server.
Syntax	upload attack_log_toRCP [{username <username 15>} {<ipaddr>} dest_file <path_filename 64> rcp: <string 128>] {unit <unit_id 1-12>}
Description	This command is used to upload the attack log file from the device to an RCP server.
Parameters	<p><i>username</i> - The remote user name on the RCP Server.</p> <p><i><ipaddr></i> - The IPv4 address of the RCP server.</p> <p><i>path_filename</i> - The pathname specifies the pathname on the RCP server or local device.</p> <p>Note: If a user specifies the relative file path, the path search strategy will depend on the server system. For some systems, it will search the current user working directory first, and then search the environment paths.</p> <p><i>dest_file</i> – Specify the destination file here.</p> <p><i>rcp: <string 128></i> - Syntax: rcp: username@ipaddr/directory/filename</p> <p>Example for FULL path: user_name@10.1.1.1/home/user_name/desxxxx.had</p> <p>Example for relative path: user_name@10.1.1.1./desxxxx.had</p> <p>Note: Do not use any blank spaces in the <string>.</p> <p><i>unitid</i> - The attack log messages on the specified unit will be uploaded to the RCP server. If specified, this unit will be referred to as the master unit.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To upload the attack log from the device to an RCP server:

```
DGS-3450:admin# upload attack_log_toRCP username rcp_user 172.18.212.104 /home/DGS-XXXX.log unit 2
Command: upload attack_log_toRCP username rcp_user 172.18.212.104 /home/DGS-XXXX.log unit 2

Connecting to server..... Done.
Upload Attack log..... Done.

DGS-3450:admin#
```

TECHNICAL SUPPORT COMMANDS

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

Command	Parameters
show tech_support	
upload tech_support_toTFTP	<ipaddr> <path_filename 64>

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

show tech_support

Purpose	Used to show the information of technique's support.
Syntax	show tech_support
Description	<p>This command is especially used by the technical support personnel to dump the device overall operation information. The information is project dependent and includes the following information.</p> <ul style="list-style-type: none"> • Basic System information • system log • Running configuration • Layer 1 information • Layer 2 information • Layer 3 information • Application • OS status • Controller's status <p>This command can be interrupted by Ctrl - C or ESC when it is executing.</p>
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To show the information of technique's support:

```
DGS-3450:admin# show tech_support
```

```
Command: show tech_support
```

```
#-----
#                               DGS-3450 Gigabit Ethernet Switch
#                               Technical Support Information
#
#                               Firmware: Build 2.70.B56
#                               Copyright(C) 2010 D-Link Corporation. All rights reserved.
#-----
```

```
***** Basic System Information *****
```

```
[SYS 2000-5-6 23:36:27]
```

```
Boot Time           : 6 May 2000 23:29:19
RTC Time            : 2000/05/06 23:36:27
Boot PROM Version   : Build 1.00-B13
Firmware Version    : Build 2.70.B56
Hardware Version     : A2
Serial number        : H2FT29C000004
MAC Address          : 00-26-5A-87-41-15
```

```
[STACKING 2000-5-6 23:36:27]
```

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

upload tech_support_toTFTP

Purpose	Used to upload the information of technique's support.
Syntax	upload tech_support_toTFTP <ipaddr> <path_filename 64>
Description	<p>The upload tech_support_toTFTP command is used to upload the information of technique's support to TFTP server. The information is project dependent and includes the following information.</p> <ul style="list-style-type: none"> • Basic System information • system log • Running configuration • Layer 1 information • Layer 2 information • Layer 3 information • Application • OS status • Controller's status <p>This command can be interrupted by Ctrl - C or ESC when it is executing.</p>
Parameters	<p><i>ipaddr</i> - Specifies the IP address of TFTP server.</p> <p><i>path_filename</i> - Specifies the file name to store the information of technique's support in TFTP server. The max size of the file name is 64.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To upload the information of technique's support:

```
DGS-3450:admin# upload tech_support_to_TFTP 10.0.0.66 tech_report.txt
Command: upload tech_support_to_TFTP 10.0.0.66 tech_report.txt

Connecting to server..... Done.
Upload techsupport file..... Done.

Success.

DGS-3450:admin#
```

TELNET CLIENT COMMANDS

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

Command	Parameters
telnet	[<ipaddr> <domain_name 255>] {tcp_port(1) <value 0-65535>}

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

telnet

Purpose	Used to initiate a Telnet client session with a specific Telnet server.
Syntax	telnet [<ipaddr> <domain_name 255>] {tcp_port(1) <value 1-65535>}
Description	The Telnet command establishes a single Telnet client connection with a specified server. The parameters specified by the command will only be used for the establishment of this specific session. They will not affect the establishment of other sessions.
Parameters	<p><i>ipaddr</i> - The IP address of the Telnet server.</p> <p><i>domain_name</i> - Specify the domain name of the Telnet server.</p> <p><i>tcp_port</i> - Specifies the Telnet server port number to be connected. If not specified, the default port is 23.</p>
Restrictions	None.

Example usage:

Telnet to a Switch by specifying the IP address:

```
DGS-3450:admin# telnet 10.90.90.90
Command: telnet 10.90.90.90
```

```
DGS-XXXX Fast Ethernet Switch Command Line Interface
```

```
Firmware: Build 2.70.B56
```

```
Copyright(C) 2006-2010 D-Link Corporation. All rights reserved.
```

```
UserName:
```

Telnet to a host by specifying the domain name and the server port:

```
DGS-3450:admin# telnet ctrl.iplanet.org tcp_port 2323
Command: telnet ctrl.iplanet.org tcp_port 2323
```

```
Login:
```

TFTP CLIENT COMMANDS

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

Command	Parameters
download firmware_fromTFTP	[<ipaddr> <ipv6addr> <domain_name 255>] src_file <path_filename 64> {[unit < unitid 1-12> all]} {image_id <int 1-2>}
download cfg_fromTFTP	[<ipaddr> <ipv6addr> <domain_name 255>] src_file <path_filename 64> {[<config_id 1-2> increment]}
upload cfg_toTFTP	[<ipaddr> <ipv6addr> <domain_name 255>] dest_file <path_filename 64> {config_id <int 1-2>} {[include exclude begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}} {[include exclude begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}} {[include exclude begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}}}}
upload log_toTFTP	[<ipaddr> <ipv6addr> <domain_name 255>] dest_file <path_filename 64>
upload attack_log_toTFTP	[<ipaddr> <ipv6addr> <domain_name 255>] dest_file <path_filename 64> {unit <unit_id 1-12>}

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

download firmware_fromTFTP

Purpose	Used to download the firmware image from TFTP server.
Syntax	download firmware_fromTFTP [<ipaddr> <ipv6addr> <domain_name 255>] src_file <path_filename 64> {[unit < unitid 1-12> all]} {image_id <int 1-2>}
Description	This command is used to download a firmware image file from the TFTP server.
Parameters	<p><i>ipaddr</i> - The IP address of the TFTP server.</p> <p><i>ipv6addr</i> - The IPV6 address of the TFTP server.</p> <p><i>domain_name</i> - The domain name of the TFTP server.</p> <p><i>src_file</i> - Used to identify the parameter "path_filename".</p> <p><i>unit</i> - Specifies which unit on the stacking system. If it is not specified, it refers to the master unit.</p> <p><i>all</i> - When all is specified, the firmware image on all units will be updated.</p> <p><i>image_id</i> - Specifies the firmware image ID. If image ID is not specified, it refers to the boot_up image.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To download firmware from TFTP:


```
DGS-3450:admin# download firmware_fromTFTP 10.54.71.1 src_file px.had
Command: download firmware_fromTFTP 10.54.71.1 src_file px.had

Connecting to server..... Done.
Download firmware..... Done. Do not power off!
Please wait, programming flash..... Done.

DGS-3450:admin#
```

download cfg_fromTFTP

Purpose	Used to download configuration file from the TFTP server.
Syntax	download cfg_fromTFTP [<ipaddr> <ipv6addr> <domain_name 255>] src_file <path_filename 64> {[<config_id 1-2> increment]}
Description	This command is used to download a configuration file from a TFTP server.
Parameters	<p><i>ipaddr</i> - The IP address of the TFTP server.</p> <p><i>ipv6addr</i> - The IPV6 address of the TFTP server.</p> <p><i>domain_name</i> - The domain name of the TFTP server.</p> <p><i>src_file</i> - Used to identify the parameter "path_filename".</p> <p><i>path_filename</i> - The pathname specifies the pathname on the TFTP server. It can be a relative pathname or an absolute pathname.</p> <p><i>config_id</i> - Specifies the configuration file ID. If <i>cfg_id</i> is not specified, it refers to the boot_up configuration file.</p> <p><i>increment</i> - This argument is only required for system which does not have file system and only support one configuration file since the download of a configuration will automatically apply the setting to the system. If increment is specified, then the existing configuration will not be cleared before applying of the new configuration. If it is not specified, then the existing configuration will be cleared before applying of the new configuration.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To download configuration from TFTP:

```
DGS-3450:admin# download cfg_fromTFTP 10.54.71.1 src_file cfg01.txt
Command: download cfg_fromTFTP 10.54.71.1 src_file cfg01.txt

Connecting to server..... Done.
Download configuration..... Done.

DGS-3450:admin#
```

upload cfg_toTFTP

Purpose	Used to upload a configuration file from device to TFTP server. This command is required to be supported when file system is not supported on device's FLASH EPROM.
Syntax	upload cfg_toTFTP [<ipaddr> <ipv6addr> <domain_name 255>] dest_file <path_filename 64> {config_id <int 1-2>} {[include exclude begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}} {[include exclude begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}} {[include exclude begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}}}}}
Description	This command is used to upload a configuration file from the device to the TFTP server.
Parameters	<i>ipaddr</i> - The IP address of the TFTP server.

upload cfg_toTFTP

ipv6addr - The IPV6 address of the TFTP server.
domain_name - The domain name of the TFTP server.
dest_file - Used to identify the parameter "path_filename".
path_filename - The pathname specifies the pathname on the TFTP server. It can be a relative pathname or an absolute pathname.
config_id - Specifies the configuration file ID. If *config_id* is not specified, it refers to the boot_up configuration file.
filter_string - A filter string is enclosed by symbol. Thus, the filter string itself cannot contain the character. The filter string is case sensitive.

Restrictions Only Administrator and Operator-level users can issue this command.

Example usage:

To upload configuration from TFTP:

```
DGS-3450:admin# upload cfg_toTFTP 10.48.74.121 dest_file C:\test
Command: upload cfg_toTFTP 10.48.74.121 dest_file C:\test

Connecting to server... Done.
Upload Configuration... Done.

DGS-3450:admin#
```

upload log_toTFTP

Purpose	Used to upload a log file from device to TFTP server. This command is required to be supported when file system is not supported on device's FLASH EPROM.
Syntax	upload log_toTFTP [<ipaddr> <ipv6addr> <domain_name 255>] dest_file <path_filename 64>
Description	This command is used to upload a log file from device to TFTP server.
Parameters	<i>ipaddr</i> - The IP address of the TFTP server. <i>ipv6addr</i> - The IPV6 address of the TFTP server. <i>domain_name</i> - The domain name of the TFTP server. <i>dest_file</i> - Used to identify the parameter "path_filename". <i>path_filename</i> - The pathname specifies the pathname on the TFTP server. It can be a relative pathname or an absolute pathname.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To upload a log file from TFTP server:

```
DGS-3450:admin# upload log_toTFTP 10.48.74.121 dest_file C:\LOG
Command: upload log_toTFTP 10.48.74.121 dest_file C:\LOG

Connecting to server... Done.
Upload log... Done.

DGS-3450:admin#
```

upload attack_log_toTFTP

Purpose	Used to upload the attack log on a unit.
Syntax	upload attack_log_toTFTP [<ipaddr> <ipv6addr> <domain_name 255>] dest_file <path_filename 64> {unit <unit_id 1-12>}
Description	This command is used to upload the attack log on a unit.
Parameters	<p><i>ipaddr</i> - The IP address of the TFTP server.</p> <p><i>ipv6addr</i> - The IPV6 address of the TFTP server.</p> <p><i>domain_name</i> - The domain name of the TFTP server.</p> <p><i>dest_file</i> - Used to identify the parameter "path_filename".</p> <p><i>path_filename</i> - Specifies the path name on the TFTP server to hold the attack log.</p> <p><i>unit</i> - The attack log messages on the specified unit will be uploaded to the TFTP server. If it is not specified, it refers to the master unit.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To upload the master's dangerous log:

```
DGS-3450:admin# upload attack_log 10.90.90.1 dest_file C:\alert.txt
Command: upload attack_log 10.90.90.1 dest_file C:\alert.txt

Success.

DGS-3450:admin#
```

TIME AND SNTP COMMANDS

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

Command	Parameters
config sntp	{primary <ipaddr> secondary <ipaddr> poll-interval <int 30-99999>}
show sntp	
enable sntp	
disable sntp	
config time	<date ddmthyyyy> <time hh:mm:ss>
config time_zone	{operator [+ -] hour <gmt_hour 0-13> min <minute 0-59>}
config dst	[disable repeating {s_week <start_week 1-4,last> s_day <start_day sun-sat> s_mth <start_mth 1-12> s_time <start_time hh:mm> e_week <end_week 1-4,last> e-day <end_day sun-sat> e_mth <end_mth 1-12> e_time <end_time hh:mm> offset [30 60 90 120]} annual {s_date <start_date 1-31> s_mth <start_mth 1-12> s_time <start_time hh:mm> e_date <end_date 1-31> e_mth <end_mth 1-12> e_time <end_time hh:mm> offset [30 60 90 120]}]
show time	

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

config sntp

Purpose	Used to setup SNTP service.
Syntax	config sntp {primary <ipaddr> secondary <ipaddr> poll-interval <int 30-99999>}
Description	Use this command to configure SNTP service from an SNTP server. SNTP must be enabled for this command to function (See <i>enable sntp</i>).
Parameters	<p><i>primary</i> – This is the primary server the SNTP information will be taken from.</p> <ul style="list-style-type: none"> • <ipaddr> – The IP address of the primary server. <p><i>secondary</i> – This is the secondary server the SNTP information will be taken from in the event the primary server is unavailable.</p> <ul style="list-style-type: none"> • <ipaddr> – The IP address for the secondary server. <p><i>poll-interval <int 30-99999></i> – This is the interval between requests for updated SNTP information. The polling interval ranges from 30 to 99,999 seconds.</p>
Restrictions	Only Administrator and Operator-level users can issue this command. SNTP service must be enabled for this command to function (enable sntp).

Example usage:

To configure SNTP settings:

```
DGS-3450:admin# config sntp primary 10.1.1.1 secondary 10.1.1.2 poll-interval 30
Command: config sntp primary 10.1.1.1 secondary 10.1.1.2 poll-interval 30

Success.

DGS-3450:admin#
```

show sntp

Purpose	Used to display the SNTP information.
Syntax	show sntp
Description	This command will display SNTP settings information including the source IP address, time and poll interval.
Parameters	None.
Restrictions	None.

Example usage:

To display SNTP configuration information:

```
DGS-3450:admin# show sntp
Command: show sntp

Current Time Source      : System Clock
SNTP                     : Disabled
SNTP Primary Server     : 10.1.1.1
SNTP Secondary Server   : 10.1.1.2
SNTP Poll Interval      : 720 sec

DGS-3450:admin#
```

enable sntp

Purpose	To enable SNTP server support.
Syntax	enable sntp
Description	This will enable SNTP support. SNTP service must be separately configured (see config sntp). Enabling and configuring SNTP support will override any manually configured system time settings.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command. SNTP settings must be configured for SNTP to function (config sntp).

Example usage:

To enable the SNTP function:

```
DGS-3450:admin# enable sntp
Command: enable sntp

Success.

DGS-3450:admin#
```

disable sntp

Purpose	To disable SNTP server support.
Syntax	disable sntp
Description	This will disable SNTP support. SNTP service must be separately configured (see config sntp).
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example:

To disable SNTP support:

```
DGS-3450:admin# disable sntp
Command: disable sntp

Success.

DGS-3450:admin#
```

config time

Purpose	Used to manually configure system time and date settings.
Syntax	config time <date ddmthyyy> <time hh:mm:ss>
Description	This will configure the system time and date settings. These will be overridden if SNTP is configured and enabled.
Parameters	<i>date</i> – Express the date using two numerical characters for the day of the month, three alphabetical characters for the name of the month, and four numerical characters for the year. For example: 03aug2003. <i>time</i> – Express the system time using the format hh:mm:ss, that is, two numerical characters each for the hour using a 24-hour clock, the minute and second. For example: 19:42:30.
Restrictions	Only Administrator and Operator-level users can issue this command. Manually configured system time and date settings are overridden if SNTP support is enabled.

Example usage:

To manually set system time and date settings:

```
DGS-3450:admin# config time 30jun2003 16:30:30
Command: config time 30jun2003 16:30:30

Success.

DGS-3450:admin#
```

config time_zone

Purpose	Used to determine the time zone used in order to adjust the system clock.
Syntax	config time_zone {operator [+ -] hour <gmt_hour 0-13> min <minute 0-59>}
Description	This will adjust system clock settings according to the time zone. Time zone settings will adjust SNTP information accordingly.
Parameters	<i>operator</i> – Choose to add (+) or subtract (-) time to adjust for time zone relative to GMT. <i>hour</i> – Select the number of hours different from GMT. <i>min</i> – Select the number of minutes difference added or subtracted to adjust the time zone.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure time zone settings:

```
DGS-3450:admin# config time_zone operator + hour 2 min 30
Command: config time_zone operator + hour 2 min 30
```

Success.

```
DGS-3450:admin#
```

config dst

Purpose	Used to enable and configure time adjustments to allow for the use of Daylight Savings Time (DST).
Syntax	config dst [disable repeating {s_week <start_week 1-4,last> s_day <start_day sun-sat> s_mth <start_mth 1-12> s_time start_time hh:mm> e_week <end_week 1-4,last> e_day <end_day sun-sat> e_mth <end_mth 1-12> e_time <end_time hh:mm> offset [30 60 90 120]} annual {s_date start_date 1-31> s_mth <start_mth 1-12> s_time <start_time hh:mm> e_date <end_date 1-31> e_mth <end_mth 1-12> e_time <end_time hh:mm> offset [30 60 90 120]}]
Description	DST can be enabled and configured using this command. When enabled this will adjust the system clock to comply with any DST requirement. DST adjustment effects system time for both manually configured time and time set using SNTP service.
Parameters	<i>disable</i> – Disable the DST seasonal time adjustment for the Switch. <i>repeating</i> – Using repeating mode will enable DST seasonal time adjustment. Repeating mode requires that the DST beginning and ending date be specified using a formula. For example, specify to begin DST on Saturday during the second week of April and end DST on Sunday during the last week of October. <i>annual</i> – Using annual mode will enable DST seasonal time adjustment. Annual mode requires that the DST beginning and ending date be specified concisely. For example, specify to begin DST on April 3 and end DST on October 14.

config dst

- s_week* – Configure the week of the month in which DST begins.
- <start_week 1-4,last>* – The number of the week during the month in which DST begins where 1 is the first week, 2 is the second week and so on, last is the last week of the month.
- e_week* – Configure the week of the month in which DST ends.
- *<end_week 1-4,last>* – The number of the week during the month in which DST ends where 1 is the first week, 2 is the second week and so on, last is the last week of the month.
- s_day* – Configure the day of the week in which DST begins.
- *<start_day sun-sat>* – The day of the week in which DST begins expressed using a three character abbreviation (sun, mon, tue, wed, thu, fri, sat)
- e_day* – Configure the day of the week in which DST ends.
- *<end_day sun-sat>* – The day of the week in which DST ends expressed using a three character abbreviation (sun, mon, tue, wed, thu, fri, sat)
- s_mth* – Configure the month in which DST begins.
- *<start_mth 1-12>* – The month to begin DST expressed as a number.
- e_mth* – Configure the month in which DST ends.
- *<end_mth 1-12>* – The month to end DST expressed as a number.
- s_time* – Configure the time of day to begin DST.
- *<start_time hh:mm>* - Time is expressed using a 24-hour clock, in hours and minutes.
- e_time* – Configure the time of day to end DST.
- *<end_time hh:mm>* – Time is expressed using a 24-hour clock, in hours and minutes.
- s_date* – Configure the specific date (day of the month) to begin DST.
- *<start_date 1-31>* – The start date is expressed numerically.
- e_date* – Configure the specific date (day of the month) to begin DST.
- *<end_date 1-31>* – The end date is expressed numerically.
- offset [30 | 60 | 90 | 120]* – Indicates number of minutes to add or to subtract during the summertime. The possible offset times are 30, 60, 90, and 120. The default value is 60.

Restrictions Only Administrator and Operator-level users can issue this command.

Example usage:

To configure daylight savings time on the Switch:

```
DGS-3450:admin# config dst repeating s_week 2 s_day tue s_mth 4 s_time 15:00 e_week 2
e_day wed e_mth 10 e_time 15:30 offset 30
Command: config dst repeating s_week 2 s_day tue s_mth 4 s_time 15:00 e_week 2 e_day wed
e_mth 10 e_time 15:30 offset 30

Success.

DGS-3450:admin#
```


show time

Purpose	Used to display the current time settings and status.
Syntax	show time
Description	This will display system time and date configuration as well as display current system time.
Parameters	None.
Restrictions	None.

Example usage:

To show the time currently set on the Switch's System clock:

```
DGS-3450:admin# show time
Command: show time

Current Time Source   : System Clock
Boot Time             : 27 Nov 2008  09:33:16
Current Time          : 27 Nov 2008  16:17:45
Time Zone             : GMT +00:00
Daylight Saving Time  : Disabled
  Offset in minutes   : 60
  Repeating           : From : Apr 1st  Sun 00:00
                     : To   : Oct last Sun 00:00
  Annual              : From : 29 Apr 00:00
                     : To   : 12 Oct 00:00

DGS-3450:admin#
```

TIME RANGE COMMANDS

The Time Range commands are used in conjunction with the Access Profile commands listed in the previous chapter to determine a starting point and an ending point, based on days of the week, when an Access Profile configuration will be enabled on the Switch. Once configured here, the time range are to be applied to an access profile rule using the **config access_profile profile_id** command.



NOTE: The Time Range commands are based on the time settings of the Switch. Make sure to configure the time for the Switch appropriately for these commands using commands listed in the Time and SNTP Commands chapter later in this manual.

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

Command	Parameters
config time_range	<range_name 32> [hours start_time <time hh:mm:ss> end_time <time hh:mm:ss> weekdays <daylist> delete]
show time_range	

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

config time_range

Purpose	Used to configure a time range in which an access profile rule is to be enabled.
Syntax	config time_range <range_name 32> [hours start_time <time hh:mm:ss> end_time <time hh:mm:ss> weekdays <daylist> delete]
Description	This command is to be used in conjunction with an access profile rule to determine a period of time when an access profile and an associated rule are to be enabled on the Switch. Remember, this time range can only be applied to one period of time and also, it is based on the time set on the Switch.
Parameters	<p><i>range_name 32</i> – Enter a name of no more than 32 alphanumeric characters that will be used to identify this time range on the Switch. This range name will be used in the config access_profile profile_id command to identify the access profile and associated rule to be enabled for this time range.</p> <p><i>hours</i> – This parameter is used to set the time in the day that this time range is to be set using the following parameters:</p> <ul style="list-style-type: none"> <i>start_time <time hh:mm:ss></i> – Use this parameter to identify the starting time of the time range, in hours, minutes and seconds, based on the 24-hour time system. <i>end_time <time hh:mm:ss></i> – Use this parameter to identify the ending time of the time range, in hours, minutes and seconds, based on the 24-hour time system. <p><i>weekdays</i> – Use this parameter to determine the days of the week to set this time range.</p> <ul style="list-style-type: none"> <i><daylist></i> – The user may set the days of the week here to set this time range in the three letter format (mon, tue, wed...). To specify a day range, separate the daylist using a dash (mon-fri would mean Monday through Friday). To specify a list of days in a week, separate the daylist using a comma, with no spaces (mon,tue,fri would mean Monday, Tuesday and Friday). <p><i>delete</i> – Use this parameter to delete a previously configured time range from the system.</p>

config time_range

Restrictions	Only Administrator and Operator-level users can issue this command.
--------------	---

Example usage:

To configure the time range time1 to be between 6:30 a.m. and 9:40 p.m., Monday to Friday:

```
DGS-3450:admin# config time_range time1 hours start_time 6:30:00 end_time 21:40:00
weekdays mon-fri
Command: config time_range time1 hours start_time 6:30:00 end_time 21:40:00 weekdays mon-
fri

Success.

DGS-3450:admin#
```

show time_range

Purpose	To view the current configurations of the time range set on the Switch.
Syntax	show time_range
Description	This command is used to display the currently configured time range(s) set on the Switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To view the current time range settings.

```
DGS-3450:admin# show time_range
Command: show time_range

Time Range information
-----
Range name      : time1
Weekdays       : Mon, Tue, Wed, Thu, Fri
Start time      : 06:30:00
End time        : 21:40:00

Total entries: 1

DGS-3450:admin#
```

TRACE ROUTE COMMANDS

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

Command	Parameters
tracert	[<ipaddr> <domain_name 255>] {ttl <value 1-60> port <value 30000-64900> timeout <sec 1-65535> probe <value 1-9>}
tracert6	<ipv6addr> {ttl <value 1-60> port <value 30000-64900> timeout <sec 1-65535> probe <value 1-9>}

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

tracert

Purpose	This command is used to trace the routed path between the switch and a destination end station.
Syntax	tracert [<ipaddr> <domain_name 255>] {ttl <value 1-60> port <value 30000-64900> timeout <sec 1-65535> probe <value 1-9>}
Description	To track the route of an IP packet, tracert launches UDP probe packets with a small TTL (time to live) and then listens for an ICMP "time exceeded" reply from a gateway. Probes start with a TTL of one and increase by one until either an ICMP "port unreachable" is returned, indicating that the packet reached the host, or the maximum number of hops is exceeded. At each TTL setting, one probe packet is launched (the number can be changed by specifying the parameter "probe") and tracert prints a line showing the round trip time and the address of the gateway of each probe, or time out of each probe. If there is no response within the 5 seconds timeout interval, an asterisk (*) is printed for that probe.
Parameters	<p><i>ipaddr</i> - IP address of the destination end station.</p> <p><i><domain_name 255></i> - The domain name of the destination end station.</p> <p><i>ttl <value 1-60></i> - The time to live value of the trace route request. This is the maximum number of routers that a trace route packet can cross, while seeking the network path between two devices. The range for the TTL is 1 to 60 hops.</p> <p><i>port <value 30000-64900></i> - Specify the destination UDP port number. The UDP port range is from 30000 to 64900.</p> <p><i>timeout <sec 1-65535></i> - Define the timeout period while waiting for a response from the remote device. A value of 1 to 65535 seconds can be specified. The default is 5 seconds.</p> <p><i>probe <value 1-9></i> - Specify the number of probe packets for each TTL. The default is 1.</p> <p>Note: The probe will be terminated once the destination is reached.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To trace the routed path between the switch and 10.48.74.121:

```
DGS-3450:admin# traceroute 10.48.74.121 probe 3
Command: traceroute 10.48.74.121 probe 3

<10 ms      10.12.73.254
<10 ms      10.12.73.254
<10 ms      10.12.73.254
<10 ms      10.19.68.1
<10 ms      10.19.68.1
*           Request timed out.
<10 ms      10.48.74.121

Trace complete.
DGS-3450:admin#
```

To trace the routed path between the switch and intra.example.com:

```
DGS-3450:admin# traceroute intra.example.com timeout 10
Command: traceroute intra.example.com timeout 10

<10 ms      10.12.73.254
<10 ms      10.19.68.1
<10 ms      intra.example.com [10.48.74.100]

Trace complete.
DGS-3450:admin#
```

traceroute6

Purpose	This command is used to trace the IPv6 routed path between the switch and a destination end station.
Syntax	traceroute6 <ipv6addr> {ttl <value 1-60> port <value 30000-64900> timeout <sec 1-65535> probe <value 1-9>}
Description	To track the route of an IPv6 packet, traceroute6 launches UDP probe packets with a small TTL (time to live) and then listens for an ICMP "time exceeded" reply from a gateway. Probes start with a TTL of one and increase by one until either an ICMP "port unreachable" is returned, indicating that the packet reached the host, or the maximum number of hops is exceeded. At each TTL setting, one probe are launched (the number can be changed by specifying the parameter "probe") and traceroute prints a line showing the round trip time and the address of the gateway of each probe, or time out of each probe. If there is no response within the 5 seconds timeout interval, an asterisk (*) is printed for that probe.
Parameters	<p><i>ipv6addr</i> - IPv6 address of the destination end station.</p> <p><i>tll</i> <value 1-60> - The time to live value of the trace route request. This is the maximum number of routers that a trace route v6 packet can cross, while seeking the network path between two devices. The range for the TTL is 1 to 60 hops.</p> <p><i>port</i> <value 30000-64900> - Specify the destination UDP port number. The UDP port range is from 30000 to 64900.</p> <p><i>timeout</i> <sec 1-65535> - Define the timeout period while waiting for a response from the remote device. A value of 1 to 65535 seconds can be specified. The default is 5 seconds.</p> <p><i>probe</i> <value 1-9> - Specify the number of probe packets for each hop. The default is 1.</p> <p>Note: The probe will be terminated once the destination is reached.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To trace the IPv6 routed path between the switch and 3000::1:

```
DGS-3450:admin# traceroute6 3000::1 probe 3
```

```
Command: traceroute6 3000::1 probe 3
```

```
<10 ms      1345:142::11
<10 ms      1345:142::11
<10 ms      1345:142::11
<10 ms      2011:14::100
<10 ms      2011:14::100
*           Request timed out.
<10 ms      3000::1
```

```
Trace complete.
```

```
DGS-3450:admin#
```

To trace the IPv6 routed path between the switch and 1210:100::11 with port 40000:

```
DGS-3450:admin# traceroute6 1210:100::11 port 40000
```

```
Command: traceroute6 1210:100::11 port 40000
```

```
<10 ms      3100::25
<10 ms      4130::100
<10 ms      1210:100::11
```

```
Trace complete.
```

```
DGS-3450:admin#
```

TRAFFIC CONTROL COMMANDS

There are two modes used for packet storm control on the Switch, Drop mode and Shutdown mode. Drop mode is hardware-based (chip-based) and Shutdown mode is a function of software. The two modes are incompatible with each other, therefore it is necessary to determine which method is best suited to the network environment where it is used.

Drop mode

The Drop mode storm control function is used to configure three chip-based hardware tables for state and a single threshold value (threshold value is the same for all three tables). If the threshold value is exceeded on a port, the Switch will drop all packets on the port. In Drop mode, some parameters such as “time interval” and “count down,” as well as the CLI command, “config traffic control auto_recover_time” are software-based functions and therefore not applicable for Drop mode traffic control.

Shutdown mode

Shutdown mode is a software-based storm control function. When shutdown mode is used, the state of the hardware tables used for Drop mode are set to disable. Shutdown mode does not support DLF storm control. All configurations except the port state are saved in the software table. The CPU receives the port state from the counter table (updated at 2 second intervals). If a counter is exceeded on a port, the CPU is shutdown. All packets, except BPDU packets, on the port are dropped. If the port remains in shutdown status for a configurable period (the count down value), the port enters shutdown forever status. The port link is down and remains disabled until either the configurable recover timer is timed out or the CLI command “config ports [<portlist> | all] state enable” is manually entered.

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

Command	Parameters
config traffic control	[<portlist> all] {broadcast [enable disable] multicast [enable disable] [dlf unicast] [enable disable] action [drop shutdown] threshold <value 0-255000 > countdown [<min 0> <min 3-30> disable] time_interval <sec 5-600>}
config traffic trap	[none storm_occurred storm_cleared both]
show traffic control	{<portlist>}
config traffic control auto_recover_time	[<min 0> <min 1-65535>]
config traffic control_recover	[<portlist> all]

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

config traffic control

Purpose	Used to configure broadcast/multicast packet storm control. Shutdown mode is provided to monitor the traffic rate in addition to the storm control drop mode. If traffic rate is too high, this port will be shut down.
Syntax	config traffic control [<portlist> all] { broadcast [enable disable] multicast [enable disable] [dlf unicast] [enable disable] action [drop shutdown] threshold <value 0-255000 > countdown [<min 0> <min 3-30> disable] time_interval <sec 5-600>}
Description	The config traffic control command configures broadcast/multicast/DLF storm control.
Parameters	<i>portlist</i> - Used to specify a range of ports to be configured. <i>broadcast</i> - Enable or disable broadcast storm control.

config traffic control

multicast - Enable or disable multicast storm control.

dif - Enable or disable unknown packet storm control. (Supported for drop mode only)

action - One of the two options for action are specified for storm control, shutdown of drop mode. Shutdown mode is a function of software, drop mode is implemented by the chip. If shutdown mode is specified, it is necessary to configure values for the *back_off* and *time_interval* parameters.

threshold - The upper threshold, at which point the specified storm control is triggered. The <value> is the number of broadcast/multicast packets per second received by the switch that will trigger the storm traffic control measure. The threshold is expressed as PPS (packets per second) and must be an unsigned integer.

time_interval - The sampling interval of received packet counts. The possible value will be 5-600 seconds. The parameter is not applicable if “drop” (mode) is specified for the “action” parameter.

countdown - Timer for shutdown mode. If a port enters the shutdown Rx state and this timer runs out, port will be shutdown forever. The parameter is not applicable if “drop” (mode) is specified for the “action” parameter. Default is 0 minutes. 0 disables the forever state, meaning that the port will not enter the shut down forever state.

disable – Specifies that the countdown is disabled. The port will directly shutdown when the switch detects a storm.

Restrictions

Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the parameters so that the traffic control status is enabled on ports 1-12:

```
DGS-3450:admin# config traffic control 1-12 broadcast enable action shutdown threshold 1
countdown 5 time_interval 10
Command: config traffic control 1-12 broadcast enable action shutdown threshold 1
countdown 5 time_interval 10
```

Success.

```
DGS-3450:admin#
```

config traffic trap

Purpose Used to configure trap modes.

Syntax `config traffic trap [none | storm_occurred | storm_cleared | both]`

Description **Occurred Mode:** This trap is sent when a packet storm is detected by the packet storm mechanism.
Cleared Mode: This trap is sent when the packet storm is cleared by the packet storm mechanism.

Parameters *none* - No trap state is specified for storm control.
storm_occurred - Occurred mode is enabled and cleared mode is disabled.
storm_cleared - Occurred mode is disabled and cleared mode is enabled.
both - Both occurred and cleared modes are enabled.

Restrictions

Only Administrator and Operator-level users can issue this command.

Example usage:

To enable both the occurred mode and cleared mode traffic control traps:


```
DGS-3450:admin# config traffic trap both
Command: config traffic trap both

Success.

DGS-3450:admin#
```

show traffic control

Purpose	Used to display the current traffic control settings.
Syntax	show traffic control { <portlist>}
Description	The show traffic control command displays the current traffic control settings.
Parameters	<i>portlist</i> - Used to specify the range of ports to be shown. If no parameter is specified, the system will display the packet storm control configuration for all ports.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To display the traffic control parameters for ports 1 to 10:

```
DGS-3450:admin# show traffic control 1-10
Command: show traffic control 1-10

Traffic Control Trap           : [None]
Traffic Control Auto Recover Time : 5 Minutes

Port Thres  Broadcast Multicast Unicast  Action  Count  Time  Shutdown
  hold      Storm    Storm    Storm   down   down  Interval Forever
-----
1    1      Enabled  Disabled Disabled Shutdown 5    10
2    1      Enabled  Disabled Disabled Shutdown 5    10
3    1      Enabled  Disabled Disabled Shutdown 5    10
4    1      Enabled  Disabled Disabled Shutdown 5    10
5    1      Enabled  Disabled Disabled Shutdown 5    10
6    1      Enabled  Disabled Disabled Shutdown 5    10
7    1      Enabled  Disabled Disabled Shutdown 5    10
8    1      Enabled  Disabled Disabled Shutdown 5    10
9    1      Enabled  Disabled Disabled Shutdown 5    10
10   1      Enabled  Disabled Disabled Shutdown 5    10

DGS-3450:admin#
```

config traffic control auto_recover_time

Purpose	Used to configure the traffic auto recover time used to specify the time allowed for a port to recover from shutdown forever status.
Syntax	config traffic control auto_recover_time [<min 0> <min 1-65535>]
Description	Configure all ports' auto recover time from shutdown forever state.
Parameters	<i>minutes</i> - The time allowed for auto recovery from shutdown for a port. The default value is 0, so no auto recovery is possible; the port remains in shutdown forever mode. This requires manual entry of the CLI command "config ports [<portlist> all] state enable" to return the port to a forwarding state. The default value is 0, which means disable auto recover mode, shutdown forever.

config traffic control auto_recover_time

Restrictions	Only Administrator and Operator-level users can issue this command.
--------------	---

Example usage:

To configure the auto recover time to 5 minutes:

```
DGS-3450:admin# config traffic control auto_recover_time 5
Command: config traffic control auto_recover_time 5

Success.

DGS-3450:admin#
```

config traffic control_recover

Purpose	Used to configure traffic control recover for any or all ports.
Syntax	config traffic control_recover [<portlist> all]
Description	Configuring a port for traffic control recover will require an administrator to restart the specified ports if storm control shuts down the port or ports. That is, if a storm triggers the action shutdown for a port, it will remain in the shutdown even if the threshold falls below the value that triggers the storm control action.
Parameters	<i><portlist></i> - Enter the list of ports to be configured here. <i>all</i> - Specifies that all the ports will be included in the configuration.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

TRAFFIC SEGMENTATION COMMANDS

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

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

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

config traffic_segmentation

Purpose	Used to configure traffic segmentation on the Switch.
Syntax	config traffic_segmentation [<portlist> all] forward_list [null all <portlist>]
Description	The config traffic_segmentation command is used to configure traffic segmentation on the Switch.
Parameters	<p><portlist> – Specifies a port or range of ports that will be configured for traffic segmentation. The beginning and end of the port list range are separated by a dash. Non-contiguous portlist entries are separated by a comma. (ex: 1-3,7-9)</p> <p>forward_list – Specifies a range of ports that will receive forwarded frames from the ports specified in the portlist, above.</p> <ul style="list-style-type: none"> • <i>null</i> – No ports are specified. • <i>all</i> – All ports are specified. • <portlist> – Specifies a range of ports for the forwarding list. This list must be on the same Switch previously specified for traffic segmentation (i.e. following the <portlist> specified above for config traffic_segmentation). The beginning and end of the port list range are separated by a dash. Non-contiguous portlist entries are separated by a comma. (ex:1-3,7-9)
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure ports 1 through 5 to be able to forward frames to port 6 through 10:

```
DGS-3450:admin# config traffic_segmentation 1-5 forward_list 6-10
Command: config traffic_segmentation 1-5 forward_list 6-10

Success.

DGS-3450:admin#
```

show traffic_segmentation

Purpose	Used to display the current traffic segmentation configuration on the Switch.
Syntax	show traffic_segmentation {<portlist>}
Description	The show traffic_segmentation command is used to display the current traffic segmentation configuration on the Switch.
Parameters	<i><portlist></i> – Specifies a port or range of ports for which the current traffic segmentation configuration on the Switch will be displayed. The beginning and end of the port list range are separated by a dash. Non-contiguous portlist entries are separated by a comma. (ex: 1-3,7-9)
Restrictions	The port lists for segmentation and the forward list must be on the same Switch.

Example usage:

To display the current traffic segmentation configuration on the Switch.

```
DGS-3450:admin# show traffic_segmentation
Command: show traffic_segmentation

Traffic Segmentation Table
Port  Forward Portlist
-----
1:1   1:1-1:25
1:2   1:1-1:25
1:3   1:1-1:25
1:4   1:1-1:25
1:5   1:1-1:25
1:6   1:1-1:25
1:7   1:1-1:25
1:8   1:1-1:25
1:9   1:1-1:25
1:10  1:1-1:25
1:11  1:1-1:25
1:12  1:1-1:25
1:13  1:1-1:25
1:14  1:1-1:25
1:15  1:1-1:25
1:16  1:1-1:25
1:17  1:1-1:25
1:18  1:1-1:25
CTRL+C  ESC q Quit  SPACE n Next Page  Enter Next Entry  a All
```

TRUSTED HOST COMMANDS

Trusted Host is a security feature which denies an illegal network address to access the switch.

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

Command	Parameters
create trusted_host	[<ipaddr> network <network_address>]
delete trusted_host	[ipaddr <ipaddr> network <network_address> all]
show trusted_host	

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

create trusted_host

Purpose	Used to create the trusted host.
Syntax	create trusted_host [<ipaddr> network <network_address>]
Description	The create trusted host command creates the trusted host. The switch allows you to specify up to three IP addresses that are allowed to manage the switch via in-band SNMP or Telnet based management software. These IP addresses must be members of the Management VLAN. If no IP addresses are specified, then there is nothing to prevent any IP address from accessing the switch, provided the user knows the Username and Password.
Parameters	<p>When the access interface is not specified, the trusted host will be created for all interfaces.</p> <p><i>ipaddr</i> - The IP address of the trusted host.</p> <p><i>network</i> - The network address of the trusted network. The form of network address is xxx.xxx.xxx.xxx/y.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create a trusted host:

```
DGS-3450:admin# create trusted_host 10.48.74.121
Command: create trusted_host 10.48.74.121

Success.

DGS-3450:admin#
```

delete trusted_host

Purpose	Used to delete a trusted host entry made using the create trusted_host command above.
Syntax	delete trusted_host [ipaddr <ipaddr> network <network_address> all]
Description	The delete trusted_host command is used to delete a trusted host entry made using the create trusted_host command above.
Parameters	<p><i>ipaddr</i> - The IP address of the trusted host.</p> <p><i>network</i> - The network address of the trusted network.</p>

delete trusted_host

all - All trusted hosts will be deleted.

Restrictions Only Administrator and Operator-level users can issue this command.

Example usage:

To delete the trusted host:

```
DGS-3450:admin# delete trusted_host 10.48.74.121
Command: delete trusted_host 10.48.74.121

Success.

DGS-3450:admin#
```

show trusted_host

Purpose	Used to display a list of trusted hosts entered on the switch using the create trusted_host command above.
Syntax	show trusted_host
Description	The show trusted host command displays the trusted hosts.
Parameters	None.
Restrictions	None.

Example usage:

To display a trusted host:

```
DGS-3450:admin# show trusted_host
Command: show trusted_host

Management Stations

IP Address
-----
10.48.93.100
10.51.17.1
10.50.95.90

Total Entries : 3

DGS-3450:admin#
```

UNICAST ROUTE COMMANDS

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

Command	Parameters
create iproute	[default <network_address>] <ipaddr> {<metric 1-65535>} {[primary backup]}
delete iproute	[default <network_address>] <ipaddr>
show iproute	{[<network_address> <ipaddr>]} {[static rip hardware]}
config route preference	[static default rip] <value 1-999>
show route preference	{[local static default rip]}
create route redistribute dst rip	src [local static] {metric <value 0-16>}
delete route redistribute	[dst rip src [static local]]
config route redistribute dst rip	src [local static] {metric <value 0-16>}
show route redistribute	{dst rip src [static local]}

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

create iproute

Purpose	Used to create an IP route entry to the switch's IP routing table.
Syntax	create iproute [default <network_address>]<ipaddr> {<metric 1-65535>} {[primary backup]}
Description	<p>Use this command to create an IP static route.</p> <p>Selecting "primary" or "backup" means the newly created route is a floating static route.</p> <p>If none of the following, "primary", or "backup" is selected, the static route will:</p> <ol style="list-style-type: none"> 1. be primary if there is no primary route that has the same destination; 2. be backup if there has been a primary route that has the same destination. 3. fail to create if there have been a primary route and a backup route that have the same destination.
Parameters	<p><i>default</i> - Create an IP default route (0.0.0.0/0).</p> <p><i>network_address</i> - The IP address and net mask of the destination of the route. The address and the mask can be set by the traditional format (for example, 10.1.2.3/255.0.0.0 or in CIDR format, 10.1.2.3/16).</p> <p><i>ipaddr</i> - The IP address for the next hop router.</p> <p><i>metric</i> - The default setting is 1.</p> <p><i>primary</i> - Specify the route as the primary route to the destination.</p> <p><i>backup</i> - Specify the route as the backup route to the destination.</p>
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To add a floating static route and a static multipath route:

```
DGS-3450:admin# create iproute 10.48.74.121/255.0.0.0 10.1.1.254 primary
Command: create iproute 10.48.74.121/8 10.1.1.254 primary

Success.

DGS-3450:admin#
```

delete iproute default

Purpose	Used to delete an IP route entry from the switch's IP routing table.
Syntax	delete iproute [default <network_address>] <ipaddr>
Description	Use this command to delete an IP static route.
Parameters	<i>default</i> - Deletes an IP default route (0.0.0.0/0). <i>network_address</i> - The IP address and net mask of the destination of the route. The address and the mask can be set by the traditional format (for example, 10.1.2.3/255.0.0.0 or in CIDR format, 10.1.2.3/16). <i>ipaddr</i> - Specify the next hop IP address of the route need to be deleted.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete an IP static route:

```
DGS-3450:admin# delete iproute 10.48.74.121/255.0.0.0 10.1.1.254
Command: delete iproute 10.48.74.121/8 10.1.1.254

Success.

DGS-3450:admin#
```

show iproute

Purpose	Used to display the switch's current IP routing table.
Syntax	show iproute {[<network_address> <ipaddr>]} {[static rip hardware]}
Description	Use this command to display the switch's IP routing table.
Parameters	<i>network_address</i> - Specify the destination network address of the route to be displayed. <i>ipaddr</i> - Specify the destination IP address of the route to be displayed. The longest prefix matched route will be displayed. <i>static</i> - Specify to display only static routes. One static route may be active or inactive. <i>rip</i> - Specify to display only RIP routes. <i>hardware</i> - Specify to display only the routes that have been written into the chip.
Restrictions	None.

Example usage:

To display the contents of the IP routing table:

DGS-3450:admin# show iproute

Command: show iproute

Routing Table

IP Address/Netmask	Gateway	Interface	Cost	Protocol
10.1.1.0/24	0.0.0.0	System	1	Local
192.168.1.0/24	0.0.0.0	ip1	1	Local

Total Entries : 2

DGS-3450:admin# show iproute static

Command: show iproute static

Routing Table

IP Address/Netmask	Gateway	Cost	Protocol	Backup	Status
0.0.0.0/0	101.1.1.101	1	Default	Backup	Inactive
12.1.0.0/16	61.1.1.61	1	Static	Backup	Inactive
12.1.0.0/16	101.1.1.101	1	Static	Primary	Inactive
123.0.0.0/8	101.1.1.7	2	Static	Primary	Active

Total Entries : 4

DGS-3450:admin# show iproute hardware

Command: show iproute hardware

Routing Table

IP Address/Netmask	Gateway	Interface
0.0.0.0/0	10.1.1.11	ip1
10.1.1.0/24	0.0.0.0	System
100.1.1.0/24	10.1.1.11	ip1
192.168.1.0/24	10.1.1.11	ip1

Total Entries : 4

DGS-3450:admin#

config route preference

Purpose	Used to configure route type preference.
Syntax	config route preference [static default rip] <value 1-999>
Description	Use this command to configure route preference. The route with smaller preference has higher priority. The preference for local routes is fixed to 0.
Parameters	<i>static</i> - Configure the preference of static route. The default value is 60. <i>default</i> - Configure the preference of default route. The default value is 1. <i>rip</i> - Configure the preference of RIP route. The default value is 100.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the route preference for static routes to 70:

```
DGS-3450:admin# config route preference static 70
Command: config route preference static 70

Success.

DGS-3450:admin#
```

show route preference

Purpose	Used to display the route preference of each route type.
Syntax	show route preference {[local static default rip]}
Description	This command is used to display route preference setting.
Parameters	<i>local</i> - Display the preference of local route. <i>static</i> - Display the preference of static route. <i>default</i> - Display the preference of default route. <i>rip</i> - Display the preference of RIP route.
Restrictions	None.

Example usage:

To display the route preference for all route types:

```
DGS-3450:admin# show route preference
Command: show route preference

Route Preference Settings

Protocol      Preference
-----
RIP           100
Static        60
Default       999
Local         0

DGS-3450:admin#
```

create route redistribute dst rip

Purpose	Used to redistribute routing information from other routing protocols to RIP.
Syntax	create route redistribute dst rip src [local static] {metric <value 0-16>}
Description	This command is used to redistribute routing information from other routing protocols to RIP. When the metric is specified as 0, the metric in the original route will become the metric of the redistributing RIP routes transparently. If the metric of the original routes is greater than 16, the route will be not redistributed.
Parameters	<i>dst</i> - Specify the target protocol. <i>src</i> - Specify the source protocol. <i>static</i> - To redistribute static routes to RIP. <i>local</i> - To redistribute local routes to RIP. <i>metric</i> - Specifies the RIP route metric value for the redistributed routes. The valid value is 0 to 16. The default value is 0.

create route redistribute dst rip

Restrictions Only Administrator and Operator-level users can issue this command.

Example usage:

To add route redistribution settings:

```
DGS-3450:admin# create route redistribute dst rip src local metric 2
Command: create route redistribute dst rip src local metric 2

Success.

DGS-3450:admin#
```

delete route redistribute

Purpose	Used to delete route redistribute configuration on the switch.
Syntax	delete route redistribute [dst rip src [static local]]
Description	This command is used to stop redistribution of routes from one source protocol to another destination protocol.
Parameters	<i>dst</i> - Specify the target protocol. <i>src</i> - Specify the source protocol.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete route redistribution settings:

```
DGS-3450:admin# delete route redistribute dst rip src local
Command: delete route redistribute dst rip src local
Success.

DGS-3450:admin#
```

config route redistribute dst rip

Purpose	Used to update the metric to be associated with the redistributed routes from a specific protocol to RIP protocol.
Syntax	config route redistribute dst rip src [local static] {metric <value 0-16>}
Description	This command is used to update the metric to be associated with the redistributed routes from a specific protocol to RIP protocol.
Parameters	<i>dst</i> - Specify the target protocol. <i>src</i> - Specify the source protocol. <i>static</i> - To redistribute static routes to RIP. <i>local</i> - To redistribute local routes to RIP. <i>metric</i> - Specifies the RIP metric value for the redistributed routes. The valid value is 0 to 16.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure route redistributions:

```
DGS-3450:admin# config route redistribute dst rip src static
Command: config route redistribute dst rip src static

Success.

DGS-3450:admin#
```

show route redistribute

Purpose	Used to display the route redistribution settings on the switch.
Syntax	show route redistribute {dst [rip] src [static local]}
Description	This command is used to display the route redistributions settings.
Parameters	<p><i>dst</i> - Specify the target protocol.</p> <p><i>rip</i> - Display the redistribution with the target protocol RIP.</p> <p><i>src</i> - Specify the source protocol.</p> <p><i>static</i> - Display the redistribution with the source static.</p> <p><i>local</i> - Display the redistribution with the source local.</p> <p>If no parameter is specified, the system will display all route redistributions.</p>
Restrictions	None.

Example usage:

To display route redistributions:

```
DGS-3450:admin# show route redistribute
Command: show route redistribute

Route Redistribution Settings

Source      Destination  Type      Metric
Protocol    Protocol
-----
LOCAL      RIP          All       2

Total Entries : 1

DGS-3450:admin#
```

UTILIZATION COMMANDS

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

Command	Parameters
show utilization	[cpu ports dram { unit <unit_id>} flash {unit <unit_id>}]

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

show utilization

Purpose	Used to display real-time port utilization statistics.
Syntax	show utilization [cpu ports dram { unit <unitid>}] flash {unit <unitid>}]
Description	The show utilization command displays real-time CPU , ports,dram or flash utilization statistics
Parameters	<p><i>ports</i> - Specifies a range of ports to be displayed. (UnitID:port number).</p> <p><i>dram</i> - To show dram memory utilization.</p> <p><i>flash</i> - To show flash memory utilization.</p> <p><i>unit</i> - Specifys the unit to be displayed. If not specified, all units will not be displayed.</p>
Restrictions	None.

Example usage:

To display the ports utilization:

DGS-3450:admin# show utilization ports

Command: show utilization ports

Port	TX/sec	RX/sec	Util	Port	TX/sec	RX/sec	Util
1:1	0	0	0	1:22	0	0	0
1:2	0	0	0	1:23	0	0	0
1:3	0	0	0	1:24	0	0	0
1:4	0	0	0	1:25	0	0	0
1:5	0	0	0	1:26	19	49	1
1:6	0	0	0	2:1	0	0	0
1:7	0	0	0	2:2	0	0	0
1:8	0	0	0	2:3	0	0	0
1:9	0	0	0	2:4	0	0	0
1:10	0	0	0	2:5	0	0	0
1:11	0	0	0	2:6	0	0	0
1:12	0	0	0	2:7	0	30	1
1:13	0	0	0	2:8	0	0	0
1:14	0	0	0	2:9	30	0	1
1:15	0	0	0	2:10	0	0	0
1:16	0	0	0	2:11	0	0	0
1:17	0	0	0	2:12	0	0	0
1:18	0	0	0	2:13	0	0	0
1:19	0	0	0	2:14	0	0	0
1:20	0	0	0	2:15	0	0	0
1:21	0	0	0	2:16	0	0	0
Port	TX/sec	RX/sec	Util	Port	TX/sec	RX/sec	Util
2:17	0	0	0				
2:18	0	0	0				
2:19	0	0	0				
2:20	0	0	0				
2:21	0	0	0				
2:22	0	0	0				
2:23	0	0	0				
2:24	0	0	0				
2:25	0	0	0				
2:26	11	2	1				

To display the CPU utilization:

DGS-3450:admin# show utilization cpu

Command: show utilization cpu

CPU utilization :

 Five seconds - 20% One minute - 10% Five minutes - 70%

Success.

DGS-3450:admin#

To display DRAM utilization:

```
DGS-3450:admin# show utilization dram
Command: show utilization dram
DRAM Utilization :
Total DRAM   : 262,144 KB
Used DRAM    : 212,568 KB
Utilization  : 81%

Success.

DGS-3450:admin#
```

To display FLASH utilization:

```
DGS-3450:admin# show utilization flash
Command: show utilization flash
FLASH Memory Utilization :
Total FLASH   : 16,384 KB
Used FLASH    : 13,440 KB
Utilization   : 82%

Success.

DGS-3450:admin#
```

WEB-BASED ACCESS CONTROL (WAC) COMMANDS

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

Command	Parameters
enable wac	
disable wac	
config wac ports	[<portlist> all] {state [enable disable] aging_time [infinite <min 1-1440>] idle_time [infinite <min 1-1440>] block_time [<sec 0-300>]}(1)
config wac method	[local radius]
config wac default_redirpath	<string 128>
config wac clear_default_redirpath	
config wac virtual_ip	{ < ipaddr > < ipv6addr > } (1)
config wac switch_http_port	< tcp_port_number 1-65535> { [http https] }
create wac user	<username 15> {[vlan <vlan_name 32> vlanid <vlanid 1-4094>]}
delete wac	[user <username 15> all_users]
config wac user	<username 15> [vlan <vlan_name 32> vlanid <vlanid 1-4094> clear_vlan]
config wac authorization attributes	{radius [enable disable] local [enable disable]}(1)
show wac	
show wac ports	{ <portlist> }
show wac user	
show wac auth_state ports	{ <portlist> }
clear wac auth_state	[ports [<portlist> all] { authenticated authenticating blocked } macaddr <macaddr>]

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

enable wac

Purpose	Used to enable WAC function.
Syntax	enable wac
Description	The enable wac command enables WAC function. WAC and JWAC are mutual exclusive function. That is, they can not be enabled at the same time.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable WAC:


```
DGS-3450:admin# enable wac
Command: enable WAC

Success.

DGS-3450:admin#
```

disable wac

Purpose	Used to disable WAC function.
Syntax	disable wac
Description	The disable wac command disables WAC function; all authentication entries related to WAC will be deleted.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable WAC:

```
DGS-3450:admin# disable wac
Command: disable wac

Success.

DGS-3450:admin#
```

config wac ports

Purpose	Used to config state and other parameters of the ports.
Syntax	config wac ports [<portlist> all] {state [enable disable] aging_time [infinite <min 1-1440>] idle_time [infinite <min 1-1440>] block_time [<sec 0-300>]}(1)
Description	The config wac ports command allows you to configure port state of WAC. The default value of aging time is 1440 minutes. The default value of idle time is infinite. The default value of block_time is 60 seconds.
Parameters	<i>portlist</i> - A port range to set their WAC state. <i>all</i> - All the Switch ports' WAC state is to be configured. <i>state</i> - To specify the port state of WAC <i>aging_time</i> - A time period during which an authenticated host will keep in authenticated state. "infinite" indicates never to age out the authenticated host on the port <i>idle_time</i> - If there is no traffic during idle time, the host will be moved back to unauthenticated state. "infinite" indicates never to check the idle state of the authenticated host on the port. <i>block_time</i> - If a host fails to pass the authentication, it will be blocked for a period specified by "block_time".
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To config state and other parameters of the ports:

```
DGS-3450:admin# config wac ports 1-9 state enable
Command: config wac ports 1-9 state enable

Success.

DGS-3450:admin#
```

config wac method

Purpose	Used to configure WAC auth method.
Syntax	config wac method [local radius]
Description	The config wac radius_protocol command allows you to specify the RADIUS protocol used by WAC to complete RADIUS authentication. WAC shares other RADIUS configuration with 802.1x, when using this command to set the RADIUS protocol, you must make sure the RADIUS server added by "config radius ..." command supports the protocol.
Parameters	<i>local</i> - The authentication will be done via the local database. <i>radius</i> - The authentication will be done via the RADIUS server.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure WAC auth method:

```
DGS-3450:admin# config wac method radius
Command: config wac method radius

Success.

DGS-3450:admin#
```

config wac default_redirpath

Purpose	Used to config WAC default redirect URL.
Syntax	config wac default_redirpath <string 128>
Description	If default redirect path is configured, the user will be redirected to the default redirect path after successful authentication. When the string is cleared, the client will not be redirected to another URL after successful authentication.
Parameters	<i>string</i> - The URL that the client will be redirected to after successful authentication. By default, the redirected path is cleared
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To config WAC default redirect URL:

```
DGS-3450:admin# config wac default_redirpath http://www.dlink.com
Command: config wac default_redirpath http://www.dlink.com

Success.

DGS-3450:admin#
```

config wac clear_default_redirpath

Purpose	Used to clear WAC default redirect URL.
Syntax	config wac clear_default_redirpath
Description	When the string is cleared, the client will not be redirected to another URL after successful authentication.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To clear WAC default redirect URL:

```
DGS-3450:admin# config wac clear_default_redirpath

Success.

DGS-3450:admin#
```

config wac virtual_ip

Purpose	Used to config the virtual IP address for WAC.
Syntax	config wac virtual_ip { < ipaddr > < ipv6addr > } (1)
Description	The virtual IP of WAC is used to accept authentication request from unauthenticated host. Only requests sent to this IP will get response correctly. This IP does not respond to ARP request or ICMP packet!
Parameters	<i>ipaddr</i> - To specify the IP address of the virtual IP. <i>ipv6addr</i> - To specify the IPv6 address of the virtual IP.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

Set IPv4 virtual IP address:

```
DGS-3450:admin# config wac virtual_ip 1.1.1.1
Command: config wac virtual_ip 1.1.1.1

Success.

DGS-3450:admin#
```

Set IPv6 virtual IP address:

```
DGS-3450:admin# config wac virtual_ip 30::20
Command: config wac virtual_ip 30::20
Success.

DGS-3450:admin#
```

config wac switch_http_port

Purpose	Used to config HTTP(s) port of the switch used by WAC.
Syntax	config wac switch_http_port < tcp_port_number 1-65535> { [http https] }
Description	The TCP port for HTTP or HTTPS is used to identify the HTTP or HTTPS packets that will be trapped to CPU for authentication processing, or to access the login page. If not specified, the default port number for HTTP is 80, and the default port number for HTTPS is 443. If no protocol specified, the protocol is HTTP. The HTTP cannot run at TCP port 443, and the HTTPS cannot run at TCP port 80.
Parameters	<i>tcp_port_number</i> - A TCP port which the WAC Switch listens to and uses to finish the authenticating process. The range of port number is 1-65535. <i>http</i> - To specify the WAC runs HTTP protocol on this TCP port <i>https</i> - To specify the WAC runs HTTPS protocol on this TCP port
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To config HTTP(s) port of the switch used by WAC:

```
Used to config HTTP(s) port of the switch used by WAC.
DGS-3450:admin# config wac switch_http_port 8888 http
Command: config wac switch_http_port 8888 http

Success.
DGS-3450:admin#
```

create wac user

Purpose	Used to create a WAC local user.
Syntax	create wac user <username 15> {[vlan <vlan_name 32> vlanid <vlanid 1-4094>]}
Description	The create wac user command allows you to create account for web-base access control. This user account is independent with login user account. If VLAN is not specified, the user will not get a VLAN assigned after the authentication.
Parameters	<i>username</i> - User account for web-base access control. <i>vlan</i> - Authentication VLAN name.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create a WAC local user:

```
DGS-3450:admin# create wac user vlan Jim
Command: create wac user vlan Jim
Enter a case-sensitive new password:**
  Enter the new password again for confirmation:**
Success.

DGS-3450:admin#
```

delete wac user

Purpose	Used to delete a WAC local user.
Syntax	delete wac [user <username 15> all_users]
Description	The delete wac user command deletes WAC users from the local DB.
Parameters	<i>user</i> - To specify the user name to be deleted <i>all_user</i> - All user accounts in local DB will be deleted.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete a WAC local user:

```
DGS-3450:admin# delete wac user 123
Command: delete wac user 123

Success.

DGS-3450:admin#
```

config wac user

Purpose	Used to configure WAC local user.
Syntax	config wac user <username 15> [vlan <vlan_name 32> vlanid <vlanid 1-4094> clear_vlan]
Description	The config wac user command updates the local user DB. Only created user can be configured
Parameters	<i>username</i> - The user name to be configured <i>vlanid</i> - Target VLAN ID for authenticated host which uses this user account to pass authentication
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure WAC local user:

```
DGS-3450:admin# config wac user Jim vlan 3
Command: config wac user Jim vlan 3

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

DGS-3450:admin#
```

config wac authorization attributes

Purpose	The enable authorization command will enable acceptance of authorized configuration.
Syntax	config wac authorization attributes {radius [enable disable] local [enable disable]}(1)
Description	Used to enable or disable acceptance of authorized configuration. When the authorization is enabled for WAC's radius, the authorized data assigned by the RADUIS server will be accepted if the global authorization network is enabled. When the authorization is enabled for WAC's local, the authorized data assigned by the local database will be accepted.
Parameters	<i>radius</i> - If specified to enable, the authorized data assigned by the RADUIS server will be accepted if the global authorization network is enabled. The default state is enabled. <i>local</i> - If specified to enable, the authorized data assigned by the local database will be accepted if the global authorization network is enabled. The default state is enabled.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

The enable authorization command will enable acceptance of authorized configuration:

```
DGS-3450:admin# config wac authorization attributes local disable
Command: config wac authorization attributes local disable

Success.

DGS-3450:admin#
```

show wac

Purpose	Used to display web authentication global setting.
Syntax	show wac
Description	This command allows the user to display the WAC global setting.
Parameters	None.
Restrictions	None.

Example usage:

Show global configuration about WAC:

```
DGS-3450:admin# show wac
Command: show wac

Web-Base Access Control
-----
State                : Enabled
Method               : RADIUS
Redirect Path        : http://tw.yaholl.com
Virtual IP           : 0.0.0.0
Virtual IPv6         : 2000::20
Switch HTTP Port     : 80 (HTTP)
RADIUS Authorization : Enabled
Local Authorization  : Enabled

DGS-3450:admin#
```

show wac ports

Purpose	Used to display web authentication port level setting.
Syntax	show wac ports { <portlist> }
Description	This command allows the user to display the port level setting.
Parameters	<i>ports</i> - A range of member ports to show the status.
Restrictions	None.

Example usage:

To show WAC port state and other parameters:

```
DGS-3450:admin# show wac ports 1-3
Command: show wac ports 1-3

Port      State      Aging Time      Idle Time      Block Time
-----
          (min)      (min)          (sec)
-----
1:1       Enabled    60              30             120
1:2       Enabled    60              30             120
1:3       Enabled    120             60             120

Success.

DGS-3450:admin#
```

show wac user

Purpose	Used to user account for web authentication.
Syntax	show wac user
Description	The show wac user command allows you to show web authentication account.
Parameters	None.
Restrictions	None.

Example usage:

To show WAC local user:

```
DGS-3450:admin# show wac user
Command: show wac user
Username      Password      VID
-----
Jim           pasx          1000

Total Entries: 1

DGS-3450:admin#
```

show wac auth_state

Purpose	Used to display the authentication state of a port.
Syntax	show wac auth_state ports { <portlist> }
Description	Used to display the authentication state for ports.
Parameters	<i>ports</i> - Specifies the list of ports whose WAC state will be displayed.
Restrictions	None.

Example usage:

To show WAC authentication information:

```
DGS-3450:admin# show wac auth_state ports 1-3
Command: show wac auth_state ports 1-3

P:Port-based  Pri:Priority
Port  MAC Address      Original State      VID Pri Aging Time/  Idle
          RX VID                                     Block Time  Time
-----
1     00-00-00-00-00-01  1     Authenticated  4004  3     Infinite 40
1     00-00-00-00-00-02  1     Authenticated  1234  -     Infinite 50
1     00-00-00-00-00-03  1     Blocked        -     -     60        -
1     00-00-00-00-00-04  1     Authenticating -     -     10        -
2     00-00-00-00-00-10(P) 1     Authenticated  1234  2     1440     20
3     00-00-00-00-00-20(P) 1     Authenticating -     -     5         -
3     00-00-00-00-00-21(P) 1     Blocked        -     -     100       -

Total Authenticating Hosts :2
Total Authenticated Hosts  :3
Total Blocked Hosts       :2

DGS-3450:admin#
```

clear wac auth_state

Purpose	Used to delete the authentication entries.
Syntax	clear wac auth_state [ports [<portlist> all] { authenticated authenticating blocked } macaddr <macaddr>]
Description	Used to clear the authentication state of a port. If the port is port-based mode, the port will return to un-authenticated state. The entire timer associated with the port will be reset. If the port is host based mode, users on this port will be cleared. The user needs to be re-authenticated to access the network.
Parameters	<i>ports</i> - Specifies the list of ports whose WAC state will be cleared.

clear wac auth_state

authenticated - Specified to clear all authenticated users for a port.

authenticating - Specified to clear all authenticating users for a port.

Restrictions

Only Administrator and Operator-level users can issue this command.

Example usage:

To delete WAC host:

```
DGS-3450:admin# clear wac auth_state ports 1-5
```

```
Command: clear wac auth_state ports 1-5
```

```
Success.
```

```
DGS-3450:admin#
```

TECHNICAL SPECIFICATIONS

Specifications listed here apply to all Switches in the DGS-3400 Series except where otherwise noted.

General	
Standards	IEEE 802.3 10BASE-T Ethernet IEEE 802.3u 100BASE-TX Fast Ethernet IEEE 802.3ab 1000BASE-T Gigabit Ethernet IEEE 802.3z 1000BASE-T (SFP "Mini GBIC") IEEE 802.3ae (10G Optional Modules) IEEE 802.1D/w/s Spanning Tree (Rapid, Multiple) IEEE 802.1P/Q VLAN IEEE 802.1p Priority Queues IEEE 802.1v Protocol VLAN IEEE 802.1X Network Access Control IEEE 802.3 Nway auto-negotiation IEEE 802.3ad Link Aggregation Control IEEE 802.3x Full-duplex Flow Control IEEE 802.1u Fast Ethernet IEEE 802.3af Power-over-Ethernet
Protocols	CSMA/CD
Data Transfer Rates:	Half-duplex Full-duplex
Ethernet	10 Mbps 20Mbps
Fast Ethernet	100Mbps 200Mbps
Gigabit Ethernet	1000Mbps 2000Mbps
Fiber Optic	SFP (Mini GBIC) Support IEEE 802.3z 1000BASE-LX (DEM-310GT transceiver) IEEE 802.3z 1000BASE-SX (DEM-311GT transceiver) IEEE 802.3z 1000BASE-SX (DEM-312GT2 transceiver) IEEE 802.3z 1000BASE-LH (DEM-314GT transceiver) IEEE 802.3z 1000BASE-ZX (DEM-315GT transceiver) WDM Single Mode Transceiver 10km (DEM-330T/R) WDM Single Mode Transceiver 40km (DEM-331T/R)
Topology	Duplex Ring, Duplex Chain
Network Cables	Cat.5 Enhanced for 1000BASE-T UTP Cat.5, Cat. 5 Enhanced for 100BASE-TX UTP Cat.3, 4, 5 for 10BASE-T EIA/TIA-568 100-ohm screened twisted-pair (STP)(100m)

Physical and Environmental

Internal Power Supply Redundant Power Supply	AC Input: 100 - 240 VAC, 50-60 Hz	
Power Consumption	DGS-3400 Series DGS-3426 (78.2 Watts) DGS-3426P (496 Watts) DGS-3427 (86.68 Watts) DGS-3450 (144.47 Watts)	Module Inserts DEM-410CX (0.015 Watts) DEM-410X (6.16 Watts)
DC Fan:	12v	
Operating Temperature	0 - 40°C	
Storage Temperature	-40 - 70°C	
Humidity	5 - 95% non-condensing	
Dimensions	441mm x 389mm x 44mm	
Weight	DGS-3400 Series DGS-3426 (5.42 kg) DGS-3426P (6 kg) DGS-3427 (5.51 kg) DGS-3450 (5.74 kg)	Module Inserts DEM-410CX (0.16 kg) DEM-410X (0.18 kg)
EMI:	CE class A, FCC Class A	
Safety:	CSA International, CB Report	

Performance

Transmission Method	Store-and-forward
Packet Buffer	0.75 MB per device
Packet Filtering / Forwarding Rate	Full-wire speed for all connections 1,488,095 pps per port (for 1000Mbps)
MAC Address Learning	Automatic update. Supports 8K MAC address.
Priority Queues	8 Priority Queues per port.
Forwarding Table Age Time	Max age: 10-1000000 seconds. Default = 300.

PASSWORD RECOVERY PROCEDURE

This chapter describes the procedure for resetting passwords on D-Link Switches. Authenticating any user who tries to access networks is necessary and important. The basic authentication method used to accept qualified users is through a local login, utilizing a Username and Password. Sometimes, passwords get forgotten or destroyed, so network administrators need to reset these passwords. This chapter explains how the Password Recovery feature can help network administrators reach this goal.

The following steps explain how to use the Password Recovery feature on D-Link devices to easily recover passwords.

Complete these steps to reset the password:

1. For security reasons, the Password Recovery feature requires the user to physically access the device. Therefore this feature is only applicable when there is a direct connection to the console port of the device. It is necessary for the user needs to attach a terminal or PC with terminal emulation to the console port of the switch.
2. Power on the Switch. After the runtime image is loaded to 100%, the Switch will allow 2 seconds for the user to press the hotkey [^] (Shift + 6) to enter the "Password Recovery Mode." Once the Switch enters the "Password Recovery Mode," all ports on the Switch will be disabled.

```

Boot Procedure1.00-B13
-----
Power On Self Test ..... 100 %

MAC Address   : 00-26-5A-87-41-15
H/W Version   : A2

Please wait, loading V2.70.B56 Runtime image ..... 100 %
    
```

```

Password Recovery Mode
>
    
```

3. In the "Password Recovery Mode" only the following commands can be used.

Command	Parameter
reset config	The reset config command resets the whole configuration back to the default values.
reboot	The reboot command exits the Reset Password Recovery Mode and restarts the switch. A confirmation message will be displayed to allow the user to save the current settings.
reset account	The reset account command deletes all the previously created accounts.
reset password {<username>}	The reset password command resets the password of the specified user. If a username is not specified, the passwords of all users will be reset.
show account	The show account command displays all previously created accounts.