

D-Link

**D-LINK DGS-1100-10/ME
METRO ETHERNET MANAGED SWITCH**

CLI REFERENCE GUIDE

V1.0

Information in this document is subject to change without notice.

© 2014 D-Link Corporation. All rights reserved.

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

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

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

FCC Warning

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

CE Mark Warning

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

Warnung!

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

Precaución!

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

Attention!

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

Attenzione!

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

VCCI Warning

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

March, 2014

Table of Contents

INTRODUCTION	1
USING THE COMMAND LINE INTERFACE	2
COMMAND SYNTAX	5
BASIC SWITCH COMMANDS.....	7
enable password encryption	8
disable password encryption	8
create account.....	9
config account.....	10
show account.....	10
delete account.....	11
show session.....	11
show switch.....	12
enable web	12
disable web.....	13
enable autoconfig	13
disable autoconfig	14
show autoconfig	14
show config	15
enable jumbo_frame.....	16
disable jumbo_frame.....	16
show jumbo_frame.....	17
save	17
reboot	18
reset system.....	18
logout	19
ping	19
ping6	20
enable telnet	21
disable telnet	21
config time_range	21
show time_range	22
MODIFY BANNER AND PROMPT COMMANDS	24
config command_prompt	24
config greeting_message.....	25
show greeting_message.....	26
SWITCH PORT COMMANDS.....	27
config ports	27
show ports	28
show duld ports	29
LOOPBACK DETECTION COMMANDS.....	30
enable loopdetect.....	30
disable loopdetect.....	30
config loopdetect mode	31
config loopdetect ports.....	31

config loopdetect.....	32
show loopdetect.....	32
PPPOE CIRCUIT ID INSERTION COMMANDS.....	34
config pppoe circuit_id_insertion state	34
config pppoe circuit_id_insertion ports.....	35
show pppoe circuit_id_insertion	36
show pppoe circuit_id_insertion ports	36
NETWORK MANAGEMENT (SNMP) COMMANDS	37
create snmp user.....	39
delete snmp user.....	39
show snmp user.....	40
create snmp view.....	40
delete snmp view.....	41
show snmp view.....	42
create snmp community	42
delete snmp community	43
show snmp community	43
config snmp engineID.....	44
create snmp group	44
delete snmp group	46
show snmp groups.....	46
show snmp global state	47
create snmp host.....	47
delete snmp host.....	48
show snmp host.....	49
create snmp v6host.....	50
delete snmp v6host.....	51
show snmp v6host.....	51
enable snmp traps.....	52
disable snmp traps.....	52
show snmp traps.....	52
enable snmp authenticate traps.....	53
disable snmp authenticate traps.....	54
config syslocation	54
config sysname.....	54
enable snmp	55
disable snmp.....	55
enable snmp fiber_port_link traps.....	56
disable snmp fiber_port_link traps.....	56
enable snmp LBD traps.....	56
disable snmp LBD traps	57
enable snmp port_security_violation traps.....	57
disable snmp port_security_violation traps.....	58
enable snmp twistedpair_port_link traps.....	58
disable snmp twistedpair_port_link traps.....	58
DOWNLOAD/UPLOAD COMMANDS	60
download.....	60

upload.....	61
DHCP RELAY COMMANDS.....	63
enable dhcp_relay	63
disable dhcp_relay.....	64
config dhcp_relay add ipif System.....	64
config dhcp_relay delete ipif System.....	65
config dhcp_relay hops	65
config dhcp_relay option_82.....	66
show dhcp_relay	67
enable dhcp_local_relay.....	67
disable dhcp_local_relay.....	68
config dhcp_local_relay.....	68
show dhcp_local_relay.....	69
enable dhcpv6_relay	69
disable dhcpv6_relay.....	69
show dhcpv6_relay	70
config dhcpv6_relay.....	70
config dhcpv6_relay hop_count.....	71
config dhcpv6_relay option_37.....	71
NETWORK MONITORING COMMANDS.....	73
show packet ports.....	73
show error ports	74
show utilization.....	75
clear counters	76
clear log.....	76
show log.....	76
save log	77
enable syslog.....	77
disable syslog.....	78
create syslog host	78
config syslog host.....	80
delete syslog host	82
show syslog host	83
cable diagnostic port	83
FORWARDING DATABASE COMMANDS.....	85
create fdb vlan.....	85
create multicast_fdb	86
config multicast_fdb	86
config fdb aging_time	87
delete fdb.....	87
show multicast_fdb	88
show fdb.....	88
config multicast port_filtering_mode.....	89
show multicast port_filtering_mode.....	90
BROADCAST STORM CONTROL COMMANDS.....	91
config traffic control	91
show traffic control	92

config traffic_control trap	92
QOS COMMANDS	94
config bandwidth_control	94
show bandwidth_control	95
config qos mode	95
show qos mode	96
config scheduling_mechanism	96
show scheduling_mechanism	97
config dscp_mapping	97
show dscp_mapping	98
RMON COMMANDS	99
enable rmon	99
disable rmon	100
create rmon alarm	100
delete rmon alarm	101
create rmon collection stats	101
delete rmon collection stats	102
create rmon collection history	102
delete rmon collection history	103
create rmon event	103
delete rmon event	104
show rmon	104
PORT MIRRORING COMMANDS	106
enable mirror	106
disable mirror	106
create mirror id	107
config mirror	107
show mirror	108
VLAN COMMANDS	110
create vlan	110
delete vlan	111
config vlan	111
show vlan	112
enable asymmetric_vlan	113
disable asymmetric_vlan	113
show asymmetric_vlan	113
enable management_vlan	114
disable management_vlan	114
config management_vlan	115
show management_vlan	115
show port_vlan pvid	116
Q-IN-Q COMMANDS	117
enable qinq	117
disable qinq	117
show qinq	118
config qinq ports	118
BASIC IP COMMANDS	120

config ipif System	120
show ipif.....	121
MAC NOTIFICATION COMMANDS	122
enable mac_notification	122
disable mac_notification	122
config mac_notification	123
config mac_notification ports	123
show mac_notification	124
show mac_notification ports	124
IGMP SNOOPING COMMANDS.....	126
enable igmp_snooping	127
disable igmp_snooping.....	127
show igmp_snooping	128
config igmp_snooping.....	128
config igmp_snooping querier	129
create igmp_snooping multicast_vlan	130
config igmp_snooping multicast_vlan	130
delete igmp_snooping multicast_vlan.....	131
config igmp_snooping multicast_vlan_group	132
config router_ports.....	132
config igmp_access_authentication ports.....	133
show igmp_access_authentication ports	133
enable igmp_snooping multicast_vlan	134
disable igmp_snooping multicast_vlan	134
show igmp_snooping multicast_vlan.....	135
show igmp_snooping multicast_vlan_group.....	136
show igmp_snooping group	136
show igmp_snooping host.....	137
show router_port	137
MLD SNOOPING COMMANDS	139
enable mld_snooping	139
disable mld_snooping	140
config mld_snooping.....	140
config mld_snooping router_ports	141
config mld_snooping querier	141
show mld_snooping	143
show mld_snooping group	143
show mld_snooping router_ports	144
show mld_snooping host.....	145
LIMITED IP MULTICAST ADDRESS COMMANDS.....	146
create mcast_filter_profile	146
config mcast_filter_profile.....	147
config mcast_filter_profile ipv6.....	147
delete mcast_filter_profile	148
show mcast_filter_profile.....	148
config limited_multicast_addr ports.....	149
show limited_multicast_addr ports	150

show max_mcast_group ports.....	150
802.1X COMMANDS	152
enable 802.1x	153
disable 802.1x	153
show 802.1x	153
show 802.1x auth_state	154
show 802.1x auth_configuration.....	155
config 802.1x auth_parameter ports.....	156
config 802.1x auth_protocol	157
config radius add.....	158
config radius delete	159
config radius.....	159
show radius	160
config 802.1x auth_mode.....	160
create 802.1x guest_vlan.....	161
delete 802.1x guest_vlan.....	161
config 802.1x guest_vlan ports	162
show 802.1x guest_vlan	162
create 802.1x user	163
show 802.1x user.....	163
delete 802.1x user	164
config 802.1x capability ports.....	164
PORT SECURITY COMMANDS	166
config port_security	166
show port_security	167
PORT PRIORITY COMMANDS	168
config port_priority	168
show port_priority.....	168
TIME AND SNTP COMMANDS	170
config sntp.....	170
show sntp	171
enable sntp	172
disable sntp.....	172
config time	173
config time_zone operator.....	173
config dst.....	174
show time	175
ARP COMMANDS.....	176
config arp_aging time	176
show arprentry.....	176
IPV6 NEIGHBOR DISCOVERY COMMANDS.....	178
create ipv6 neighbor_cache ipif	178
delete ipv6 neighbor_cache.....	179
show ipv6 neighbor_cache.....	179
config ipv6 nd ns ipif	180
show ipv6 nd	180
create ipv6route default.....	181

delete ipv6route default.....	181
show ipv6route.....	182
enable ipif_ipv6_link_local_auto System.....	182
disable ipif_ipv6_link_local_auto System.....	183
BANNER COMMANDS.....	184
config log_save_timing.....	184
show log.....	185
COMMAND HISTORY LIST COMMANDS.....	186
?.....	186
show command_history.....	187
dir.....	188
ACCESS AUTHENTICATION CONTROL COMMANDS.....	189
create authen_login method_list_name.....	190
config authen_login.....	190
delete authen_login method_list_name.....	191
show authen_login.....	192
create authen_enable method_list_name.....	193
config authen_enable.....	193
delete authen_enable method_list_name.....	195
show authen_enable.....	195
enable authen_policy.....	196
disable authen_policy.....	196
show authen_policy.....	197
config authen application.....	197
show authen application.....	198
config authen parameter.....	198
show authen parameter.....	199
create authen server_host.....	199
config authen server_host.....	200
delete authen server_host.....	201
show authen server_host.....	202
create authen server_group.....	203
config authen server_group.....	203
delete authen server_group.....	204
show authen server_group.....	204
enable admin.....	205
POWER SAVING COMMANDS.....	206
config power_saving mode.....	206
config power_saving.....	206
show power_saving.....	207
LLDP COMMANDS.....	208
enable lldp.....	208
disable lldp.....	209
config lldp message_tx_interval.....	209
config lldp message_tx_hold_multiplier.....	210
config lldp reinit_delay.....	210
config lldp tx_delay.....	211

show lldp	211
show lldp ports	212
show lldp local_ports	213
show lldp remote_ports	213
config lldp ports	214
config lldp ports	214
config lldp ports	215
config lldp ports	215
config lldp ports	216
config lldp ports	216
config lldp ports	217
config lldp ports	217
show lldp mgt_addr	218
show lldp statistics	218
TRAFFIC SEGMENTATION COMMANDS	220
config traffic_segmentation	220
show traffic_segmentation	220
ETHERNET OAM COMMANDS	222
config ethernet_oam ports (mode)	223
config ethernet_oam ports (state)	223
config ethernet_oam ports (link monitor error symbol)	224
config ethernet_oam ports (link monitor error frame)	225
config ethernet_oam ports (link monitor error frame seconds)	226
config ethernet_oam ports (link monitor error frame period)	227
config ethernet_oam ports (remote loopback)	227
config ethernet_oam ports (received remote loopback)	228
show ethernet_oam ports (status)	229
show ethernet_oam ports (configuration)	231
show ethernet_oam ports (statistics)	231
show ethernet_oam ports (event log)	232
clear ethernet_oam ports	233
SAFEGUARD COMMANDS	234
config safeguard_engine	234
show safeguard_engine	234

INTRODUCTION

The DGS-1100-10/ME consists of 8 10/100/1000Mbps ports plus 2 100/100/SFP ports.

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

This manual provides a reference for all of the commands contained in the CLI. Configuration and management of the Switch via the Web-based management agent is discussed in the Manual. For detailed information on installing hardware please refer also to the Manual.

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.

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

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.

Alternatively, users 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-1100-10/ME:5> config ipif System ipaddress 10.90.90.91/8
Command: config ipif System ipaddress 10.90.90.91/8

Success!
DGS-1100-10/ME:5>
```

Figure 1–1 Assigning an IP Address

In the above example, the Switch was assigned an IP address of 10.90.90.91 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 COMMAND LINE INTERFACE

The Switch allows a computer or terminal to perform some basic monitoring and configuration tasks by using the Command Line Interface (CLI) via TELNET protocol.



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

The command line functions are accessed over a Telnet interface. Once an IP address for the Switch has been set, A Telnet program can be used (in VT-100 compatible terminal mode) to access and control the Switch.

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

```
DGS-1100-10/ME Switch
DGS-1100-10/ME login:
```

Figure 2-1 Initial Console Screen after Logging In

Commands are entered at the command prompt, DGS-1100-10/ME:5>

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

```
DGS-1100-10/ME:5> ?
Command: ?

USEREXEC commands :
? <<command>>
cable diagnostic port [<portlist 1-10> ! all]
clear
clear counters ports <portlist 1-10>
clear ethernet_oam ports [<portlist 1-10> ! all] [<event_log ! statistics>]
clear fdb [vlan <vlan_name 20> ! port <port 1-10> ! all]
clear log
clear port_security_entry port <portlist 1-10>
cmdebug flag [<[ip] [icmp] [udp] [arp] > <enable! disable>]
cmdebug flag fdb [<[img] [info] [runtime]> <enable! disable>]
cmdebug flag led [<[read] [write] [debug] [cli] [watchdog] [path] [error]> <enable! disable>]
cmdebug killme
cmdebug lock msg
cmdebug memory
cmdebug multicast dump
cmdebug private inter mib { enable ! disable}
cmdebug sem
cmdebug sig <pid> <sig_id>
CTRL+C ESC Quit SPACE Next Page ENTER Next Entry ALL
```

Figure 2-2 The ? Command

When entering a command without its required parameters, the CLI displays the prompt: command: config account message and the options listed below.

```

DGS-1100-10/ME:5> config ipif

Command: config ipif

Next possible completions :
System

DGS-1100-10/ME:5> config mirror

Command: config mirror

Next possible completions :
id

DGS-1100-10/ME:5>

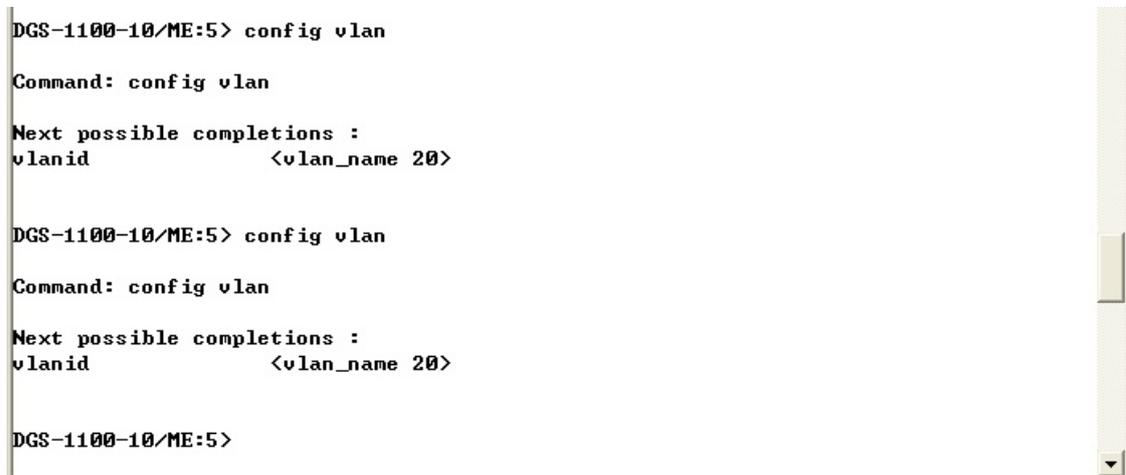
```

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, `command: config account`. Every command in the CLI has this feature, and complex commands have several layers of parameter prompting.

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

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



```

DGS-1100-10/ME:5> config vlan

Command: config vlan

Next possible completions :
vlanid          <vlan_name 20>

DGS-1100-10/ME:5> config vlan

Command: config vlan

Next possible completions :
vlanid          <vlan_name 20>

DGS-1100-10/ME:5>

```

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 `command: config account` prompt. The up arrow cursor control key was pressed to re-enter the previous command (`config account`) at the command prompt. Now the appropriate username can be entered and the `config account` command re-executed.

All commands in the CLI function in this way. In addition, the syntax of the help prompts are the same as presented in this manual: angle brackets `< >` indicate a numerical value or character string. The `< >` can also indicate a word with a number for character allowed.

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

```

DGS-1100-10/ME:5>
DGS-1100-10/ME:5>
DGS-1100-10/ME:5>
DGS-1100-10/ME:5>
DGS-1100-10/ME:5> ask

Available commands :
?                cable                clear                cmdebug
compute          config                create                debug
delete           disable               download              echo
enable           logout                npapi                 ping
ping6            reboot                reset                 rpc
save             show                  traceroute            upload

DGS-1100-10/ME:5>

```

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

```

DGS-1100-10/ME:5> show

Command: show

Next possible completions :
802.ip          802.1x          account          acct_client
arprentry      asymmetric_vlan auth_client      authen
authen_enable  authen_login    authen_policy   autoconfig
bandwidth_control  command_history config            ddp
dhcp_local_relay  dhcp_relay      dhcpv6_relay    dscp_mapping
duld           eee              error            ethernet_oam
fdb             greeting_message igmp             igmp_snooping
ipif            ipv6             ipv6route        jumbo_frame
limited_multicast_addr  lldp            log
logintimeout    loopdetect      mac_notification management
max_mcast_group mcast_filter_profile  multicast_fdb    mirror
mld_snooping    multicast        port_vlan        packet
port_priority   port_security    qinq             ports
power_saving    pppoe           router_ports     qos
radius          rmon            scheduling_mechanism  safeguard_engine
scheduling      snmp            statistics        session
snmp            syslog          time              switch
syslog          traffic_segmentation  time_range        traffic
traffic_segmentation  utilization      vlan

```

Figure 2–6 Next possible completions: Show Command

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

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 Telnet 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 account [admin oper user] <username 15>
Description	In the above syntax example, supply a username in the <username> space. Do not type the angle brackets.
Example Command	create account admin newadmin1

[square brackets]	
Purpose	Encloses a required value or set of required arguments. One value or argument can be specified.
Syntax	create account [admin oper user] <username 15>
Description	In the above syntax example, specify admin , oper or a user level account to be created. Do not type the square brackets.
Example Command	create account user newuser1

vertical bar	
Purpose	Separates two or more mutually exclusive items in a list, one of which must be entered.
Syntax	create account [admin oper user] <username 15>
Description	In the above syntax example, specify admin , oper , or user . Do not type the vertical bar.
Example Command	create account user newuser1

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

{braces}	
Purpose	Encloses an optional value or set of optional arguments.
Syntax	reset
Description	Execute "reset" will return the switch to its factory default setting.
Example command	reset Please be aware that all configurations will be reset to default value. Are you sure you want to proceed with system reset now? (Y/N)[N] N

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 displays the next command in the command history entered in the current session. This displays each command sequentially as it was entered. Use the up arrow to review previous commands.
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 (along with the appropriate parameters) in the following table.

Command	Parameter
enable password encryption	
disable password encryption	
create account	[admin operator user] <username 15>
config account	<username 15>
show account	
delete account	<username 15>
show session	
show switch	
enable web	{<tcp_port_number 1-65535>}
disable web	
enable autoconfig	
disable autoconfig	
show autoconfig	
show config	[[config_in_nvram config_id <value 1-2>] current_config] [begin exclude] <string 80>
enable jumbo_frame	
disable jumbo_frame	
show jumbo_frame	
save	[config log]
reboot	
reset system	{[include force_agree]}
logout	
ping	{times <value 0-255> timeout <sec 1-99> size <value 1-60000>}
ping6	<ipv6_addr> {size <value 1-6000> timeout <sec 1-99> times <value 1-255>}
enable telnet	{<tcp_port_number 1-65535>}
disable telnet	
config time_range	<range_name 20> [hours start_time <start_time 32> end_time <end_time 32> weekdays <daylist 32> date from_day year <start_year 2011-2029> month <start_mth 1-12> date <start_date 1-31> to_day year <end_year 2011-2029>

Command	Parameter
	month <end_mth 1-12> date <end_date 1-31> delete]
show time_range	

Each command is listed in detail as follows:

enable password encryption	
Purpose	Used to enable password encryption on a user account.
Syntax	enable password encryption
Description	The user account configuration information will be stored in the configuration file, and can be applied to the system at a time in the future. If the password encryption is enabled, the password will be in encrypted form. If password encryption is disabled and the user specifies the password in encrypted form, or if the password has been converted to encrypted form by the last enabled password encryption command, the password will still be in encrypted form. It can not revert back to plain text.
Parameters	None.
Restrictions	Only Administrator level users can issue this command.

Example usage:

To enable password encryption on the Switch:

```
DGS-1100-10/ME:5> enable password encryption
Command: enable password encryption

Success !
DGS-1100-10/ME:5>
```

disable password encryption	
Purpose	Used to disable password encryption on a user account.
Syntax	disable password encryption
Description	The user account configuration information will be stored in the configuration file, and can be applied to the system at a time in the future. If the password encryption is enabled, the password will be in encrypted form. If password encryption is disabled and the user specifies the password in encrypted form, or if the password has been converted to encrypted form by the last enabled password encryption command, the password will still be in encrypted form. It can not revert back to plain text.
Parameters	None.
Restrictions	Only Administrat level users can issue this command.

Example usage:

To disable password encryption on the Switch:

```
DGS-1100-10/ME:5> disable password encryption
Command: disable password encryption

Success !
DGS-1100-10/ME:5>
```

create account

Purpose	To create user accounts.
Syntax	create account [admin operator user] <username 15>
Description	The create account command creates an administrator, operator, or user account that consists of a username and an optional password. Up to 31 accounts can be created. You can enter username and Enter. In this case, the system prompts for the account's password, which may be between 0 and 15 characters. Alternatively, you can enter the username and password on the same line.
Parameters	<p><i>admin</i> – Name of the administrator account.</p> <p><i>oper</i> – Specify an operator level account.</p> <p><i>user</i> – Specify a user account with read-only permissions.</p> <p><i><username 1-15></i> – The account username may be between 1 and 15 characters.</p> <p><i>password <password_string> {encrypted}</i> - the account password can be included, and (optionally) can be encrypted.</p>
Restrictions	<p>Only Administrator level users can issue this command.</p> <p>Usernames can be between 1 and 15 characters.</p> <p>Passwords can be between 0 and 15 characters.</p>



NOTE: You are not required to enter a User Name. However, if you do not enter a User Name, you cannot perform the following actions:

- Create a monitor or operator (level 1 or level 14) users until an administrator user (level 15) is defined.
- Delete the last administrator user if there are monitor and/or operator users defined.

Example usage:

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

```
DGS-1100-10/ME:5> create account admin dlink
Command: create account admin dlink

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

Success!
DGS-1100-10/ME:5>
```

config account

Purpose	To change the password for an existing user account.
Syntax	config account <username 15>
Description	The config account command changes the password for a user account that has been created using the create account command. The system prompts for the account's new password, which may be between 0 and 15 characters.
Parameters	<username 15> – the account username.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the user password of 'dlink' account:

```
DGS-1100-10/ME:5> 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-1100-10/ME:5>
```

show account

Purpose	To display information about all user accounts on the Switch.
Syntax	show account
Description	The show account command displays all account usernames and their access levels created on the Switch. Up to 31 user accounts can exist on the Switch at one time.
Parameters	None.
Restrictions	None.

Example usage:

To display an account which has been created:

```
DGS-1100-10/ME:5> show account
Command: show account

Username      Access Level
-----
dlink         Admin
```

Total Entries : 1

DGS-1100-10/ME:5>

delete account

Purpose	To delete an existing user account.
Syntax	delete account <username 15>
Description	The delete account command deletes a user account that has been created using the create account command.
Parameters	<username 15> – the account username.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete the user account 'System':

DGS-1100-10/ME:5> delete account System
Command: delete account System

Success!
DGS-1100-10/ME:5>

show session

Purpose	To display information about currently logged-in users.
Syntax	show session
Description	The show session command displays a list of all the users that are logged-in at the time the command is issued. The information includes the session ID (0 for the first logged-in user, 1 for the next logged-in user, etc.), the Protocol used to connect to the Switch, the user's IP address, the user's access Level (1=user, 15=admin), and the account name on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display the way users logged in:

DGS-1100-10/ME:5> show session
Command: show session

ID	Login Time	Live Time	From	Level	Name
0	1/1/2013 00:11:05	00:07:33	Telnet	3	anonymous

Total Entries: 1

DGS-1100-10/ME:5>

show switch

Purpose	To display information about the Switch.
Syntax	show switch
Description	The show switch command displays information about the Switch settings, including Device Type, MAC Address, IP configuration, Hardware/Software version, System information, and Switch Network configuration.
Parameters	None.
Restrictions	None.

Example usage:

To display the Switch information:

```
DGS-1100-10/ME:5> show switch
Command: show switch

Device Type           :DGS-1100-10/ME V1.00.002
MAC Address           :DE-AD-BE-EF-01-02
IP Address            :10.90.90.90
VLAN Name             :default
Subnet Mask           :255.0.0.0
Default Gateway       :0.0.0.0
System boot version   :0.09.03
System firmware version :V1.00.002
System hardware version :A1
System serial number  :1MB1733K0000A
System name           :
System Location       :
System up time        :0 days, 0 hrs, 13 min, 43 secs
System Contact        :
System Time           :00:13:47 01 01 2013
IGMP Snooping        :Disabled
802.1X Status         :Disabled
Telnet                :Enabled <TCP 23>
Web                   :Enabled <TCP 80>
RMON                  :Disabled
Syslog Global State   :Disabled

DGS-1100-10/ME:5>
```

enable web

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

Syntax	enable web {<tcp_port_number 1-65535>}
Description	The enable web command enables the Web-based management software on the Switch. The user can specify the TCP port number the Switch uses to listen for Telnet requests.
Parameters	<tcp_port_number 1-65535> – The TCP port number. TCP ports are numbered between 1 and 65535. The ‘well-known’ port for the Web-based management software is 80.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

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

```
DGS-1100-10/ME:5> enable web
Command: enable web

Success!
DGS-1100-10/ME:5>
```

disable web

Purpose	To disable the HTTP-based management software on the Switch.
Syntax	disable web
Description	The disable web command disables the Web-based management software on the Switch.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To disable HTTP-based management software on the Switch:

```
DGS-1100-10/ME:5> disable web
Command: disable web

Success!
DGS-1100-10/ME:5>
```

enable autoconfig

Purpose	Used to activate the auto configuration function for the Switch. This will load a previously saved configuration file for current use.
Syntax	enable autoconfig
Description	When autoconfig is enabled on the Switch, the DHCP reply will contain a configuration file and path name. It will then request the file from the TFTP server specified in the reply. When autoconfig is enabled, the ipif settings will automatically become DHCP client.
Parameters	None.

Restrictions	<p>When autoconfig is enabled, the Switch becomes a DHCP client automatically (same as: config ipif System dhcp). The DHCP server must have the TFTP server IP address and configuration file name, and be configured to deliver this information in the data field of the DHCP reply packet. The TFTP server must be running and have the requested configuration file in its base directory when the request is received from the Switch. Consult the DHCP server and TFTP server software instructions for information on loading a configuration file.</p> <p>If the Switch is unable to complete the auto configuration process the previously saved local configuration file present in Switch memory will be loaded.</p>
--------------	---

Example usage:

To enable auto configuration on the Switch:

```
DGS-1100-10/ME:5> enable autoconfig
Command: enable autoconfig

Success !
DGS-1100-10/ME:5>
```

disable autoconfig

Purpose	Use this to deactivate auto configuration from DHCP.
Syntax	disable autoconfig
Description	The disable autoconfig command is used to instruct the Switch not to accept auto configuration instruction from the DHCP server. This does not change the IP settings of the Switch. The ipif settings will continue as DHCP client until changed with the config ipif command.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command. .

Example usage:

To stop the auto configuration function:

```
DGS-1100-10/ME:5> disable autoconfig
Command: disable autoconfig

Success!
DGS-1100-10/ME:5>
```

show autoconfig

Purpose	Used to display the current autoconfig status of the Switch.
Syntax	show autoconfig
Description	The show autoconfig command is used to list the current status of the auto configuration function.

Parameters	None.
Restrictions	None.

Example usage:

To display the autoconfig status:

```
DGS-1100-10/ME:5> show autoconfig
Command: show autoconfig

Autoconfig State: Enabled
Timeout           : 50 sec

Success!
DGS-1100-10/ME:5>
```

show config

Purpose	To display the current or saved version of the configuration settings of the Switch.
Syntax	show config [[config_in_nvram config_id <value 1-2>] current_config] [begin exclude include] <string 80>
Description	The show config command is used to list the current status of the configuration settings of the Switch.
Parameters	<p>config_in_nvram config_id <value 1-2> - Display the system configuration from NV-RAM.</p> <p>current_config - Display system configuration from the DRAM database, i.e. the current system setting.</p> <p>[begin exclude include] - Display the configuration which is begun, excluded or included.</p> <p><string 80> - Display the configuration which begin or exclude the specified string. The maximum string is 80.</p>
Restrictions	None.

Example usage:

To display the autoconfig status:

```
#-----
#           DGS-1100-10/ME Gigabit Ethernet Switch Configuration
#
#           Firmware: Build 1.00.002
#           Copyright(C) 20113 D-Link Corporation. All rights reserved.
#-----
command-start

# SNMP
enable snmp
config snmp engineID 80:00:08:1c:04:46:53
```

```

disable snmp authenticate traps
disable snmp coldstart traps
disable snmp warmstart traps
disable snmp twistedpair_port_link traps
disable snmp fiber_port_link traps
disable snmp port_security_violation traps
disable snmp LBD traps
disable snmp upgrade_state traps
disable snmp duplicate_ip_detected traps
echo off
delete snmp community private
delete snmp community public
echo on
create snmp user ReadOnly ReadOnly v1
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a ALL

```

enable jumbo_frame

Purpose	To enable jumbo frames on the device.
Syntax	enable jumbo_frame
Description	The enable jumbo_frame command enables jumbo frames on the device.
Parameters	None.
Restrictions	Only Administrator or operate-level users can issue this command. Jumbo frames will be enabled after save and restart.

Example usage:

To enable jumbo frames:

```

DGS-1100-10/ME:5> enable jumbo_frame
Command: enable jumbo_frame.

Success!
DGS-1100-10/ME:5>

```

disable jumbo_frame

Purpose	To disable jumbo frames on the device.
Syntax	disable jumbo_frame
Description	The disable jumbo_frame command disables jumbo frames on the device.
Parameters	None.
Restrictions	Only Administrator or operate-level users can issue this command. Jumbo frames will be disabled after save and restart.

Example usage:

To disable jumbo_frames:

```
DGS-1100-10/ME:5> disable jumbo_frame
Command: disable jumbo_frame

Success!
DGS-1100-10/ME:5>
```

show jumbo_frame

Purpose	To display the jumbo frame configuration.
Syntax	show jumbo_frame
Description	The show jumbo_frame command displays the jumbo frame configuration.
Parameters	None.
Restrictions	None.

Example usage:

To show the jumbo_frames configuration status on the device:

```
DGS-1100-10/ME:5> show jumbo_frame
Command: show jumbo_frame

Jumbo Frame is Enabled.
DGS-1100-10/ME:5>
```

save

Purpose	To save changes in the Switch's configuration to non-volatile RAM.
Syntax	save [config> log]
Description	The save command used to enter the current switch configuration into non-volatile RAM. The saved switch configuration will be loaded into the Switch's memory each time the Switch is restarted.
Parameters	<i>config</i> – Used to save the current configuration to a file. <i>log</i> – Used to save the current log to a file. The log file cannot be deleted.
Restrictions	Only administrator-level users can issue this command.

Example usage:

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

```
DGS-1100-10/ME:5> save config
Command: save config

Success!
DGS-1100-10/ME:5>
```

reboot

Purpose	To reboot the Switch.
Syntax	reboot
Description	The reboot command restarts the Switch.
Parameters	None.
Restrictions	Only Administrator or operate-level users can issue this command.

Example usage:

To restart the Switch:

```
DGS-1100-10/ME:5> reboot
Command: reboot

Success!
DGS-1100-10/ME:5>
      DGS-1100-10/ME Switch

DGS-1100-10/ME login:
```

reset system

Purpose	To reset the Switch to the factory default settings.
Syntax	reset system {[include force_agree]}
Description	The reset system command restores the Switch's configuration to the default settings assigned from the factory. Rebooting will clear all entries in the Forwarding Data Base.
Parameters	<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><i>{[include force_agree]}</i> - When <i>force_agree</i> is specified, the reset command will be executed immediately without further confirmation.</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 their default values:

```
DGS-1100-10/ME:5> reset system
```

```
Command: reset system
```

```
Success!
```

```
DGS-1100-10/ME:5>
```

```
DGS-1100-10/ME Switch
```

```
DGS-1100-10/ME login:
```

logout

Purpose	To log out a user from the Switch.
Syntax	Logout
Description	The logout command terminates the current user's session on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To terminate the current user's Telnet session:

```
DGS-1100-10/ME:5> logout
```

ping

Purpose	To test the connectivity between network devices.
Syntax	ping <ipaddr> {times <value 0-255> timeout <sec 1-99> size <value 1-60000>}
Description	The ping command sends Internet Control Message Protocol (ICMP) echo messages to a remote IP address. The remote IP address then 'echos' or returns the message. This is used to confirm connectivity between the Switch and the remote device.
Parameters	<p><i><ipaddr></i> - The IP address of the host.</p> <p><i>times <value 0-255></i> - The number of individual ICMP echo messages to be sent. The maximum value is 255. The default is 4.</p> <p><i>timeout <sec 1-99></i> - 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>size <value 1-60000></i> - Specify the size of the test packet. A value of 0 to 2080 can be specified.</p>
Restrictions	None.

Example usage:

To ping the IP address 10.90.90.97 three times:

```
DGS-1100-10/ME:5> ping 10.90.90.97 times 3 size 100 timeout 3
Command: ping 10.90.90.97 times 10 size 100 timeout 3

Reply Not Received From : 10.90.90.97, Timeout : 3 secs
Reply Not Received From : 10.90.90.97, Timeout : 3 secs
Reply Not Received From : 10.90.90.97, Timeout : 3 secs

--- 10.90.90.97 Ping Statistics ---
3 Packets Transmitted, 0 Packets Received, 100% Packets Loss
DGS-1100-10/ME:5>
```

ping6

Purpose	To test the IPv6 connectivity between network devices.
Syntax	ping6 <ipv6addr> {size <value 1-6000> timeout <sec 1-99> times <value 1-255>}
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	<p><i><ipv6addr></i> - The IPv6 address of the host.</p> <p><i>size <value 1-6000></i> - Specify the size of the test packet. A value of 1 to 6000 can be specified.</p> <p><i>timeout <sec 1-99></i> - 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>times <value 1-255></i> - The number of individual ICMP echo messages to be sent. The maximum value is 255. The default is 4.</p>
Restrictions	None.

Example usage:

To ping the IPv6 address to “3000::1” four times:

```
DGS-1100-10/ME:5>ping6 3000::1 times 4
Command: ping6 3000::1 times 4

Reply From : 3000::1, bytes=200, time<10ms

--- 3000::1 Ping Statistics ---
4 Packets Transmitted, 4 Packets Received, 0% Packets Loss
```

```
DGS-1100-10/ME:5>
```

enable telnet

Purpose	To enable the telnet.
Syntax	enable telnet {<tcp_port_number 1-65535>}
Description	The enable telnet command enables telnet.
Parameters	<tcp_port_number 1-65535> - Specify the TCP port number for the telnet setting.
Restrictions	Only Administrator or operate-level users can issue this command

Example usage:

To enable telnet:

```
DGS-1100-10/ME:5>enable telnet
Command: enable telnet

Success!
DGS-1100-10/ME:5>
```

disable telnet

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

Example usage:

To disable telnet:

```
DGS-1100-10/ME:5>disable telnet
Command: disable telnet

Success !
DGS-1100-10/ME:5>
```

config time_range

Purpose	To configure the time range on the Switch.
Syntax	config time_range <range_name 20> [[hours start_time <start_time 32> end_time <end_time 32> weekdays <daylist 32> date from_day year <start_year 2011-2029> month <start_mth 1-12> date <start_date 1-31> to_day year <end_year 2011-2029>

	month <end_mth 1-12> date <end_date 1-31>] delete]
Description	The config time_range command defines time ranges for access lists. If the end time is earlier than the start time, the end time will move to the following day
Parameters	<p><i><range_name 20></i> – Specifies the time range name. The range of characters is 1 - 20.</p> <p><i>start_time <start_time 32></i> – defines the time on which the time range will start to be active.</p> <p><i>end_time <end_time 32 ></i>– defines the time on which the time range will stop being active.</p> <p><i>weekdays <daylist 32></i> – defines the days of the week on which the time range will be active.</p> <p><i><start_year 2011-2029 ></i> – Specifies the time range start year.</p> <p><i><start_mth 1-12></i> – Specifies the time range start month.</p> <p><i><start_date 1-31></i> – Specifies the time range start date.</p> <p><i><end_year 2011-2029 ></i> – Specifies the time range end year.</p> <p><i><end_mth 1-12></i> – Specifies the time range end month.</p> <p><i><end_date 1-31></i> – Specifies the time range end date.</p> <p><i>delete</i> – Delete the time range settings.</p>
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure the time range on the Switch:

```
DGS-1100-10/ME:5> config time_range dd hours start_time 00:22 end_time 12:34 weekdays tue-fri date from_day year 2012 month 1 date 1 to_day year 2012 month 1 date 3
Command: config time_range dd hours start_time 00:22 end_time 12:34 weekdays tue-fri date from_day year 2012 month 1 date 1 to_day year 2012 month 1 date 3

Success!
DGS-1100-10/ME:5>
```

show time_range

Purpose	To display the currently configured access profiles on the Switch.
Syntax	show time_range
Description	The show time_range command displays the time range configuration.
Parameters	None.
Restrictions	None.

Example usage:

To display time range settings on the Switch:

```
DGS-1100-10/ME:5> show time_range

Range name   : xxx
Start time   : 10:00
End time     : 11:00
Days        : wed sun

Total Entries : 1

DGS-1100-10/ME:5>
```

MODIFY BANNER AND PROMPT COMMANDS

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

Command	Parameter
config command_prompt	[<string 32> default username]
config greeting_message	{default}
show greeting_message	

Each command is listed in detail, as follows:

config command_prompt	
Purpose	To configure the command prompt.
Syntax	config command_prompt [<string 32> default username]
Description	The config command_prompt command configures the command prompt.
Parameters	<p><i><string 32></i> – The command prompt can be changed by entering a new name of no more that 32 characters.</p> <p><i>default</i> – The command prompt will reset to factory default command prompt. Default = the name of the Switch model, for example “DGS-1100-10/ME”.</p> <p><i>username</i> – The command prompt will be changed to the login username.</p>
Restrictions	<p>Only Administrator-level users can issue this command. Other restrictions include:</p> <p>If the “reset” command is executed, the modified command prompt will remain modified. However, the “reset config/reset system” command will reset the command prompt to the original factory banner.</p>

Example usage:

To modify the command prompt to “AtYourService”:

```
DGS-1100-10/ME:5>config command_prompt AtYourService
Command: config command_prompt AtYourService

Success!
AtYourService:5#
```

config greeting_message

Purpose	Used to configure the login banner (greeting message).
Syntax	config greeting_message {default}
Description	The config greeting_message command to modify the login banner (greeting message).
Parameters	<p><i>default</i> – If the user enters default to the modify banner command, then the banner will be reset to the original factory banner. To open the Banner Editor, click Enter after typing the config greeting_message command. Type the information to be displayed on the banner by using the commands described on the Banner Editor:</p> <p>Quit without save: Ctrl+C Save and quit: Ctrl+W Move cursor: Left/Right/Up/Down Delete line: Ctrl+D Erase all setting: Ctrl+X Reload original setting: Ctrl+L</p>
Restrictions	<p>Only Administrator-level users can issue this command. Other restrictions include:</p> <p>If the “reset” command is executed, the modified banner will remain modified. However, the “reset config/reset system” command will reset the modified banner to the original factory banner. The capacity of the banner is 6*80. 6 Lines and 80 characters per line.</p> <p>Ctrl+W will only save the modified banner in the DRAM. Users need to type the “save config/save all” command to save it into Flash.</p> <p>Only valid in threshold level.</p>

Example usage:

```

To the banner:DGS-1100-10/ME:5>
Command: config greeting_message

Greeting Messages Editor
=====

                DGS-1100-10/ME Gigabit Ethernet Switch
                Command Line Interface

                Copyright(C) 2012 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	The show greeting_message command is used to view the currently configured greeting message on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To view the currently configured greeting message:

```
DGS-1100-10/ME:5>show greeting_message
Command: show greeting_message

DGS-1100-10/ME Gigabit Ethernet Switch
Command Line Interface

Copyright(C) 2012 D-Link Corporation. All rights reserved.

DGS-1100-10/ME:5>
```

SWITCH PORT COMMANDS

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

Command	Parameter
config ports	[all <portlist 1-10>] medium_type [copper fiber] MDI/MDIX [MDI MDIX auto] {description <desc 32> clear_description} flow_control [enable disable] learning [enable disable] state [enable disable] speed [auto 1000_full 100_full 100_half 10_full 10_half]}
show ports	{<portlist 1-10> all} {description err_disabled}
show duld ports	{all <portlist 1-10>}

Each command is listed in detail, as follows:

config ports	
Purpose	To configure the Switch's Ethernet port settings.
Syntax	config ports [all <portlist 1-10>] medium_type [copper fiber] MDI/MDIX [MDI MDIX auto] {description <desc 32> clear_description} flow_control [enable disable] learning [enable disable] state [enable disable] speed [auto 1000_full 100_full 100_half 10_full 10_half]}
Description	The config ports command configures the Switch's Ethernet port settings. Only the ports listed in the <portlist> are affected.
Parameters	<p><portlist 1-10> – A port or range of ports to be configured.</p> <p><i>all</i> – Configures all ports on the Switch.</p> <p><i>medium_type</i> [copper fiber] – If configuring the Combo ports, this defines the type of medium being configured.</p> <p><i>MDI/MDIX</i> [MDI MDIX j auto] – Specifies the MDI or MDIX setting of the port. The MDIX setting can be auto, normal or cross.</p> <p>If set to normal state, the port in MDIX mode, can be connected to PC NIC using a straight cable. If set to cross state, the port in mdi mode, can be connected to a port (in mdix mode) on another switch through a straight cable.</p> <p><i>description</i> <desc 32> – Enter and alphanumeric string of no more than 32 characters to describe a selected port interface.</p> <p><i>clear_description</i> – Clear the description for the specified ports.</p> <p><i>flow_control</i> [enable] – Enables flow control for the specified ports.</p> <p><i>flow_control</i> [disable] – Disables flow control for the specified ports.</p> <p><i>learning</i> [enable disable] c 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.</p> <p><i>speed</i> – Sets the speed of a port or range of ports, with the addition of one of the following:</p>

	<ul style="list-style-type: none"> • <i>auto</i> – Enables auto-negotiation for the specified range of ports. • <i>[10 100 1000]</i> – Configures the speed in Mbps for the specified range of ports. • <i>[half full]</i> – Configures the specified range of ports as either full or half-duplex.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To configure the speed of ports 1-3 to be 100 Mbps, full duplex, learning and state enabled:

```
DGS-1100-10/ME:5>config ports 1-3 medium_type copper speed 100_full learning
enable state enable
Command: config ports 1-3 medium_type copper speed 100_full learning enable
state enable

Success

DGS-1100-10/ME:5>
```

show ports	
Purpose	To display the current configuration of a range of ports.
Syntax	show ports {<portlist 1-10> all} {description err_disabled}
Description	The show ports command displays the current configuration of a port or range of ports.
Parameters	<p><portlist 1-10> – A port or range of ports whose settings are to be displayed.</p> <p>all – Specifies all ports to be displayed.</p>
Restrictions	None.

Example usage:

To display the configuration of port 3 on the Switch:

```
DGS-1100-10/ME:5> show ports 3
Command: show ports 3

Port State/ Settings Connection Address
Type MDI Speed/Duplex/FlowCtrl Speed/Duplex/FlowCtrl Learning
-----
3 Enabled 100M/Full/Enabled Link Down Enabled
MDI

DGS-1100-10/ME:5>
```

show duld ports

Purpose	To display the Switch's Ethernet duld port settings.
Syntax	show duld ports {all <portlist>}
Description	The show duld ports command displays the Switch's Ethernet duld port settings.
Parameters	<i>{all <portlist>}</i> - Specifies all ports or range of ports to be displayed.
Restrictions	None.

Example usage:

To display the Switch's Ethernet duld ports 1-5 settings:

```
DGS-1100-10/ME:5> show duld ports 1-5
Command: show duld ports 1-5
```

port	Admin State	Oper Status	Mode	Link Status	Discovery Time(Sec)
1	Disabled	Disabled	Normal	Unknown	5
2	Disabled	Disabled	Normal	Unknown	5
3	Disabled	Disabled	Normal	Unknown	5
4	Disabled	Disabled	Normal	Unknown	5
5	Disabled	Disabled	Normal	Unknown	5
6	Disabled	Disabled	Normal	Unknown	5

```
DGS-1100-10/ME:5>
```

LOOPBACK DETECTION COMMANDS

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

Command	Parameter
enable loopdetect	
disable loopdetect	
config loopdetect mode	[portbase vlanbase]
config loopdetect ports	[<portlist 1-10> all] [enable disable]
config loopdetect	interval_time <value 1-32767> lbd_recover_time [0 <value 60-1000000>]
show loopdetect	{ports [<portlist 1-10> all]}

Each command is listed in detail, as follows:

enable loopdetect

Purpose	To enable the loop back detection on the Switch.
Syntax	enable loopdetect
Description	The enable loopdetect command enables the loop back detection on the Switch.
Parameters	None.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To enable the loopback detection feature on the Switch:

```
DGS-1100-10/ME:5>enable loopdetect
Command: enable loopdetect

Success!
DGS-1100-10/ME:5>
```

disable loopdetect

Purpose	To disable the loop back detection on the Switch.
Syntax	disable loopdetect
Description	The disable loopdetect command disables the loop back detection on the Switch.
Parameters	None.

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

Example usage:

To disable the loopback detection feature on the Switch:

```
DGS-1100-10/ME:5>disable loopdetect
Command: disable loopdetect

Success!
DGS-1100-10/ME:5>
```

config loopdetect mode

Purpose	To configure the loop back detection mode to be either portbase or vlanbase on the Switch.
Syntax	config loopdetect mode [portbase vlanbase]
Description	The config loopdetect mode command configures loop back detection mode to be portbase or vlanbase on the Switch.
Parameters	<i>[portbase vlanbase]</i> - Specifies the loopdetect mode to be portbase or vlanbase.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To configure the loopback detection mode to be portbase on the Switch:

```
DGS-1100-10/ME:5>config loopdetect mode portbase
Command: config loopdetect mode portbase

Success!
DGS-1100-10/ME:5>
```

config loopdetect ports

Purpose	To configure loop back detection to be enabled or disabled for the specific ports on the Switch.
Syntax	config loopdetect ports [<portlist 1-10> all] [enable disable]
Description	The config loopdetect ports command configures the loop back detection to be enabled or disabled for the specific ports on the Switch.
Parameters	<i><portlist 1-10></i> - A port or range of ports to be configured. <i>all</i> - All ports settings are to be configured. <i>[enabled disabled]</i> - Specifies whether loop back detection is enabled or disabled for the specified ports on the Switch.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To enable the loop back detection on the Switch:

```
DGS-1100-10/ME:5>config loopdetect ports all enable
Command: config loopdetect ports all enable

Success!
DGS-1100-10/ME:5>
```

config loopdetect

Purpose	To configure the loop back detection interval time and recover time on the Switch.
Syntax	config loopdetect interval_time <value 1-32767> lbd_recover_time [0 <value 60-100000>]
Description	The config loopdetect command configures the loop back detection interval time and recover time on the Switch.
Parameters	<i>interval_time</i> <value 1-32767> – Specifies the interval time of loop back detection. The range is between 1 and 32767 seconds. <i>lbd_recover_time</i> [0 <value 60-10000>] – Specifies the recovery time of loop back detection on the switch. The range is between 60 and 10000 seconds.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To configure the loop back detection with interval time 500 on the Switch:

```
DGS-1100-10/ME:5>config loopdetect interval_time 500
Command: config loopdetect interval_time 500

Success!
DGS-1100-10/ME:5>
```

show loopdetect

Purpose	To display loop back detection information on the Switch.
Syntax	show loopdetect {ports [<portlist 1-10> all]}
Description	The show loopdetect command displays the loop back detection information on the Switch.
Parameters	<portlist 1-10> – A port or range of ports to be displayed. <i>all</i> – All ports settings are to be displayed.
Restrictions	None.

Example usage:

To display the loop back detection information on the Switch:

```
DGS-1100-10/ME:5>show loopdetect
Command: show loopdetect
```

Loopdetect Global Settings

Loopdetect Status : Enabled
Loopdetect Mode : Port-Base
Loopdetect Interval : 100
Recover Time : 60
DGS-1100-10/ME:5>

PPPOE CIRCUIT ID INSERTION COMMANDS

PPPoE Circuit ID Insertion is used to produce the unique subscriber mapping capability that is possible on ATM networks between ATM-DSL local loop and the PPPoE server. The PPPoE server will use the inserted Circuit Identifier sub-tag of the received packet to provide AAA services (Authentication, Authorization and Accounting). Through this method, Ethernet networks can be the alternative to ATM networks.

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

Command	Parameter
config pppoe circuit_id_insertion state	[enable disable]
config pppoe circuit_id_insertion ports	[all <portlist 1-10>] [circuit_id [mac ip udf <string 32>] state [enable disable]]
show pppoe circuit_id_insertion	
show pppoe circuit_id_insertion ports	{<portlist>}

Each command is listed in detail, as follows:

config pppoe circuit_id_insertion state	
Purpose	Used to enable or disable the PPPoE circuit identifier insertion.
Syntax	config pppoe circuit_id_insertion state [enable disable]
Description	<p>When PPPoE circuit identifier insertion is enabled, and the tag is absent, the system will insert the circuit ID tag to the received PPPoE discover and request packet. It will then remove the circuit ID tag from the received PPPoE offer and session confirmation packet.</p> <p>The inserted circuit ID contains the following information:</p> <ul style="list-style-type: none"> Client MAC address Device ID Port number <p>By default, the Switch IP address is used as the device ID to encode the circuit ID option.</p>
Parameters	<i>[enable disable]</i> – Enables or disables PPPoE circuit ID insertion globally. The function is disabled by default.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To globally enable PPPoE circuit identifier insertion:

```
DGS-1100-10/ME:5>config pppoe circuit_id_insertion state enable
Command: config pppoe circuit_id_insertion state enable

Success!

DGS-1100-10/ME:5>
```

config pppoe circuit_id_insertion ports

Purpose	Used to enable and disable PPPoE circuit identifier insertion on a per port basis and specify how to encode the circuit ID option.
Syntax	config pppoe circuit_id_insertion ports [all <portlist 1-10>] [circuit_id [mac ip udf <string 32>] state [enable disable]]
Description	When the port's state and the global state are enabled and if the TAG is absent, the system will then insert the Circuit ID TAG to the received PPPoE discovery initiation and request packet. It will then remove the Circuit ID tag, inserted by the system, from the received PPPoE offer and session confirmation packet.
Parameters	<p><i>[all <portlist 1-10>]</i> – Specifies a list of ports or all ports to be configured.</p> <p>The default settings are enabled for ID insertion per port, but disabled globally.</p> <p><i>circuit_id</i> – Configures the device ID used for encoding of the circuit ID option.</p> <p><i>mac</i> – Specifies that the Switch MAC address will be used to encode the circuit ID option.</p> <p><i>ip</i> – Specifies that the Switch IP address will be used to encode the circuit ID option.</p> <p><i>udf</i> – A user defined string to be used to encode the circuit ID option. The maximum length is 32.</p> <p>The default encoding for the device ID option is the Switch IP address.</p> <p><i>state</i> – Specify to either enable or disable PPPoE circuit ID insertion for the ports listed.</p>
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To enable port 1~5 PPPoE circuit ID insertion function and use Host MAC:

```
DGS-1100-10/ME:5>config pppoe circuit_id_insertion ports 1-5 circuit_id
mac state enable
Command: config pppoe circuit_id_insertion ports 1-5 circuit_id mac
state enable

Success!

DGS-1100-10/ME:5>
```

show pppoe circuit_id_insertion

Purpose	Used to display the PPPoE circuit identifier insertion status for the Switch.
Syntax	show pppoe circuit_id_insertion
Description	The show pppoe circuit_id_insertion command is used to display the global state configuration of the PPPoE circuit ID insertion function.
Parameters	None.
Restrictions	None.

Example usage:

To view the global PPPoE ID insertion state:

```
DGS-1100-10/ME:5>show pppoe circuit_id_insertion
Command: show pppoe circuit_id_insertion

Status: Enabled
DGS-1100-10/ME:5>
```

show pppoe circuit_id_insertion ports

Purpose	Used to display the PPPoE ID insertion configuration on a per port basis.
Syntax	show pppoe circuit_id_insertion ports {all <portlist 1-10>}
Description	The show pppoe circuit_id_insertion ports command allows the user to view the configuration of PPPoE ID insertion for each port.
Parameters	<i>{all <portlist 1-10>}</i> - Specifies which ports to display. If no ports are specified, every port's configuration will be listed.
Restrictions	None.

Example usage:

To view the PPPoE circuit ID configuration for ports 2 to 5:

```
DGS-1100-10/ME:5>show pppoe circuit_id_insertion ports 2-5
Command: show pppoe circuit_id_insertion ports 2-5

Port State  Cirucit ID
-----
2  Enabled  Switch MAC
3  Enabled  Switch MAC
4  Enabled  Switch MAC
5  Enabled  Switch MAC
DGS-1100-10/ME:5>
```

NETWORK MANAGEMENT (SNMP) COMMANDS

The Switch supports the Simple Network Management Protocol (SNMP) versions 1, 2c, and 3. Users can specify which version of the SNMP users want to use to monitor and control the Switch. The three versions of SNMP, vary in the level of security provided between the management station and the network device. The following table lists the security features of the three SNMP versions.

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

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

Command	Parameter
create snmp user	<username 32> <groupname 32> [v1 v2c v3 [MD5 <auth_password 32> SHA <auth_password 32> none] [DES <priv_password 32> none]]
delete snmp user	<username 32> [v1 v2c v3]
show snmp user	
create snmp view	<view_name 32> <oid 32> <oid_mask 32 view_type [included excluded]
delete snmp view	<view_name 32> [all <oid 32>]
show snmp view	{<view_name 32>}
create snmp community	<community_string 32> <username 32>
delete snmp community	<community_string 32>
show snmp community	{<community_string 32>}
config snmp engineID	<snmp_engineID 64>
create snmp group	<groupname 32> [v1 v2c v3 [noauth_nopriv auth_nopriv auth_priv]{notify_view <view_name 32>}] {read_view <view_name 32> write_view <view_name 32>}
delete snmp group	<groupname 32> [v1 v2c v3] [auth_nopriv auth_priv noauth_priv]
show snmp groups	
show snmp global state	
create snmp host	<ipaddr> [v1 <username 32> v2c <username 32> v3 [noauth_nopriv

Command	Parameter
	auth_nopriv auth_priv] <username 32>]
delete snmp host	<ipaddr>
show snmp host	{<ipaddr>}
create snmp v6host	<ip6_addr> [v1 <username 32> v2c <username 32> v3 [noauth_nopriv auth_nopriv auth_priv] <username 32>]
delete snmp v6host	<ip6_addr>
show snmp v6host	<ip6_addr>
enable snmp traps	
disable snmp traps	
show snmp traps	
enable snmp authenticate traps	
disable snmp authenticate traps	
config syslocation	<string 32>
config sysname	<string 32>
enable snmp	
disable snmp	
enable snmp fiber_port_link traps	
disable snmp fiber_port_link traps	
enable snmp LBD traps	
disable snmp LBD traps	
enable snmp port_security_violation traps	
disable snmp port_security_violation traps	
enable snmp twistedpair_port_link traps	
disable snmp twistedpair_port_link traps	

Each command is listed in detail, as follows:

create snmp user	
Purpose	To create a new SNMP user and add that user to an SNMP group.
Syntax	create snmp user <username 32> <groupname 32> [v1 v2c v3 [MD5 <auth_password 32> SHA <auth_password 32> none] [DES <priv_password 32> none]]
Description	The create snmp user command creates a new SNMP user and adds that user to an existing SNMP group.
Parameters	<p><i><username 32></i> - The new SNMP username, up to 32 alphanumeric characters.</p> <p><i><groupname 32></i> - The SNMP group name the new SNMP user is associated with, has up to 32 alphanumeric characters.</p> <p><i>auth</i> - The user may also choose the type of authentication algorithms that are used to authenticate the snmp user. The choices are:</p> <ul style="list-style-type: none"> • <i>MD5</i> - Specifies that the HMAC-MD5-96 authentication level to be used. md5 may be utilized by entering one of the following: • <i><auth_password 32></i> - A string of between 1 and 32 alphanumeric characters used to authorize the agent to receive packets for the host. • <i>SHA</i> - Specifies that the HMAC-SHA-96 authentication level will be used. • <i><priv_password 32></i> - A string of between 1 and 32 alphanumeric characters used to authorize the agent to receive packets for the host. • <i>DES</i> - Specifies that the DES authentication level will be used.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To create an SNMP user on the Switch:

```
DGS-1100-10/ME:5>create snmp user dlink SW22 v3 MD5 1234 DES jklj22
Command: create snmp user dlink SW22 v3 MD5 1234 DES jklj22

Success!
DGS-1100-10/ME:5>
```

delete snmp user	
Purpose	To remove an SNMP user from an SNMP group and also to delete the associated SNMP group.
Syntax	delete snmp user <username 32> [v1 v2c v3]
Description	The delete snmp user command removes an SNMP user from its SNMP group and then deletes the associated SNMP group.
Parameters	<i><username 32></i> - A string of up to 32 alphanumeric characters that

	identifies the SNMP user to be deleted.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To delete a previously created SNMP user on the Switch:

```
DGS-1100-10/ME:5>delete snmp user dlink v3
Command: delete snmp user dlink v3

Success!
DGS-1100-10/ME:5>
```

show snmp user

Purpose	To display information about each SNMP username in the SNMP group username table.
Syntax	show snmp user
Description	The show snmp user command displays information about each SNMP username in the SNMP group username table.
Parameters	None.
Restrictions	None.

Example usage:

To display the SNMP users currently configured on the Switch:

```
DGS-1100-10/ME:5>show snmp user
Command: show snmp user

Username  Group Name  SNMP Version  Auth-Protocol  PrivProtocol
-----  -
ReadOnly  ReadOnly    V1             None           None
ReadOnly  ReadOnly    V2             None           None
ReadWrite ReadWrite   V1             None           None
ReadWrite ReadWrite   V2             None           None

Total Entries: 4

DGS-1100-10/ME:5>
```

create snmp view

Purpose	To assign views to community strings to limit which MIB objects an SNMP manager can access.
Syntax	create snmp view <view_name 32> <oid 32> <oid_mask 32 view_type [included excluded]

Description	The create snmp view command assigns views to community strings to limit which MIB objects an SNMP manager can access.
Parameters	<p><i><view_name 32></i> – A string of up to 30 alphanumeric characters that identifies the SNMP view to be created.</p> <p><i><oid 32></i> – The object ID that identifies an object tree (MIB tree) to be included or excluded from access by an SNMP manager.</p> <p><i><oid_mask 32></i> – The object ID mask that identifies an object tree (MIB tree) to be included or excluded from access by an SNMP manager.</p> <p><i>included</i> – Includes this object in the list of objects that an SNMP manager can access.</p> <p><i>excluded</i> – Excludes this object from the list of objects that an SNMP manager can access.</p>
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To create an SNMP view:

```
DGS-1100-10/ME:5>create snmp view dlink 1.3.6 1.1.1 view_type excluded
Command: create snmp view dlink 1.3.6 1.1.1 view_type excluded

Success!
DGS-1100-10/ME:5>
```

delete snmp view

Purpose	To remove an SNMP view entry previously created on the Switch.
Syntax	delete snmp view <view_name 32> [all <oid 32>]
Description	The delete snmp view command removes an SNMP view previously created on the Switch.
Parameters	<p><i><view_name 32></i> – A string of up to 32 alphanumeric characters that identifies the SNMP view to be deleted.</p> <p><i>[all <oid 32>]</i> – The object ID that identifies an object tree (MIB tree) that is deleted from the Switch.</p>
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To delete all configured SNMP view from the Switch:

```
DGS-1100-10/ME:5> delete snmp view dlink all
Command: delete snmp view dlink all

Success!
DGS-1100-10/ME:5>
```

show snmp view

Purpose	To display an SNMP view previously created on the Switch.
Syntax	show snmp view {<view_name 32>}
Description	The show snmp view command displays an SNMP view previously created on the Switch.
Parameters	<view_name 32> – A string of up to 30 alphanumeric characters that identifies the SNMP view to be displayed.
Restrictions	None.

Example usage:

To display SNMP view configuration:

```
DGS-1100-10/ME:5>show snmp view
Command: show snmp view

SNMP View Table Configuration
View Name      Subtree OID      OID Mask      View Type
-----
dlink          1.2.3.4          1.1.1.1       Excluded
ReadWrite     1                1              Included

Total Entries: 2

DGS-1100-10/ME:5>
```

create snmp community

Purpose	To create an SNMP community string to define the relationship between the SNMP manager and an SNMP agent.
Syntax	create snmp community <community_string 32> <username 32>
Description	<p>The create snmp community command creates an SNMP community string and assigns access-limiting characteristics to this community string. The community string acts like a password to permit access to the agent on the Switch. One or more of the following characteristics can be associated with the community string:</p> <ul style="list-style-type: none"> An Access List of IP addresses of SNMP managers that are permitted to use the community string to gain access to the Switch's SNMP agent. A MIB view that defines the subset of all MIB objects to be accessible to the SNMP community. Read/write or read-only level permission for the MIB objects accessible to the SNMP community.
Parameters	<p><community_string 32> – A string of up to 32 alphanumeric characters that is used to identify members of an SNMP community. This string is used like a password to give remote SNMP managers access to MIB objects in the Switch's SNMP agent.</p> <p><username 32> – A string of up to 32 alphanumeric characters that</p>

	is used to identify the group of MIB objects that a remote SNMP manager is allowed to access on the Switch.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To create the SNMP community string 'dlink:'

```
DGS-1100-10/ME:5>create snmp community dlinkgroup dlink
Command: create snmp community dlinkgroup dlink

Success!

DGS-1100-10/ME:5>
```

delete snmp community

Purpose	To remove a specific SNMP community string from the Switch.
Syntax	delete snmp community <community_string 32>
Description	The delete snmp community command removes a previously defined SNMP community string from the Switch.
Parameters	<i><community_string 32></i> - A string of up to 32 alphanumeric characters that is used to identify which members of an SNMP community to delete. This string is used like a password to give remote SNMP managers access to MIB objects in the Switch's SNMP agent.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To delete the SNMP community string 'dlinkgroup':

```
DGS-1100-10/ME:5>delete snmp community dlinkgroup
Command: delete snmp community dlinkgroup

Success!

DGS-1100-10/ME:5>
```

show snmp community

Purpose	To display SNMP community strings configured on the Switch.
Syntax	show snmp community {<community_string 32>}
Description	The show snmp community command displays SNMP community strings that are configured on the Switch.
Parameters	<i><community_string 32></i> - A string of up to 20 alphanumeric characters that is used to identify members of an SNMP community. This string is used like a password to give remote SNMP managers access to MIB objects in the Switch's SNMP agent.

Restrictions	None.
--------------	-------

Example usage:

To display the currently entered SNMP community strings:

```
DGS-1100-10/ME:5> show snmp community
Command: show snmp community

SNMP Community Table
(Maximum Entries : 10)
Community Name      User Name
-----
private             ReadWrite
public              ReadOnly

Total Entries: 2

DGS-1100-10/ME:5>
```

config snmp engineID

Purpose	To configure a name for the SNMP engine on the Switch.
Syntax	config snmp engineID <snmp_engineID 64>
Description	The config snmp engineID command configures a name for the SNMP engine on the Switch.
Parameters	<i><snmp_engineID 64></i> - A string, of between 10 and 64 alphanumeric characters, to be used to identify the SNMP engine on the Switch.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To give the SNMP agent on the Switch:

```
DGS-1100-10/ME:5>config snmp engineID 12345678900
Command: config snmp engineID 12345678900

Success!
DGS-1100-10/ME:5>
```

create snmp group

Purpose	To create a new SNMP group, or a table that maps SNMP users to SNMP views.
Syntax	create snmp group <groupname 32> [v1 v2c v3 [noauth_nopriv auth_nopriv auth_priv]{notify_view <view_name 32>}] {read_view <view_name 32> write_view

	<view_name 32>}
Description	The create snmp group command creates a new SNMP group, or a table that maps SNMP users to SNMP views.
Parameters	<p><i><groupname 32></i> – A name of up to 30 alphanumeric characters that identifies the SNMP group the new SNMP user is to be associated with.</p> <p><i>v1</i> – Specifies that SNMP version 1 is to be used. The Simple Network Management Protocol (SNMP), version 1, is a network management protocol that provides a means to monitor and control network devices.</p> <p><i>v2c</i> – Specifies that SNMP version 2c is to be used. The SNMP v2c supports both centralized and distributed network management strategies. It includes improvements in the Structure of Management Information (SMI) and adds some security features.</p> <p><i>v3</i> – Specifies that the SNMP version 3 is to be used. SNMP v3 provides secure access to devices through a combination of authentication and encrypting packets over the network. SNMP v3 adds:</p> <ul style="list-style-type: none"> • Message integrity – Ensures that packets have not been tampered with during transit. • Authentication – Determines if an SNMP message is from a valid source. • Encryption – Scrambles the contents of messages to prevent it from being viewed by an unauthorized source. <p><i>noauth_nopriv</i> – Specifies that there is no authorization and no encryption of packets sent between the Switch and a remote SNMP manager.</p> <p><i>auth_nopriv</i> – Specifies that authorization is required, but there is no encryption of packets sent between the Switch and a remote SNMP manager.</p> <p><i>auth_priv</i> – Specifies that authorization is required, and that packets sent between the Switch and a remote SNMP manager are encrypted.</p> <p><i>read_view</i> – Specifies that the SNMP group being created can request SNMP messages.</p> <ul style="list-style-type: none"> • <i><view_name 32></i> – A string of up to 32 objects that a remote SNMP manager is allowed to access on the Switch. <p><i>write_view</i> – Specifies that the SNMP group being created has write privileges.</p> <ul style="list-style-type: none"> • <i><view_name 32</i> identifies the group of MIB objects that a remote SNMP manager is allowed to access on the Switch. <p><i>notify_view</i> – Specifies that the SNMP group being created can receive SNMP trap messages generated by the Switch's SNMP agent.</p> <ul style="list-style-type: none"> • <i><view_name 32></i> – A string of up to 32 alphanumeric characters that identifies the group of MIB objects that a remote SNMP manager is allowed to access on the Switch.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To create an SNMP group named 'sg1':

```
DGS-1100-10/ME:5>create snmp group sg1 v2c read_view sg1
write_view sg1 notify_view sg1
Command: create snmp group sg1 v2c read_view sg1 write_view
sg1 notify_view sg1

Success!
DGS-1100-10/ME:5>
```

delete snmp group

Purpose	To remove an SNMP group from the Switch.
Syntax	delete snmp group <groupname 32> [v1 v2c v3 [auth_priv noauth_nopriv]]
Description	The delete snmp group command removes an SNMP group from the Switch.
Parameters	<i><groupname 32></i> – A string of that identifies the SNMP group the new SNMP user will be associated with up to 32 alphanumeric characters.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To delete the SNMP group named 'sg1':

```
DGS-1100-10/ME:5> delete snmp group sg1 v2c
Command: delete snmp group sg1 v2c

Success!
DGS-1100-10/ME:5>
```

show snmp groups

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

Example usage:

To display the currently configured SNMP groups on the Switch:

```
DGS-1100-10/ME:5>show snmp groups
Command: show snmp groups

SNMP Group Table
(Maximum Entries : 10)

Group Name  Read View  Write View  Notify View  Security Model  Security Level
-----
sg1         df         df          d            v3              AuthPriv
ReadOnly    ReadWrite  ---         ReadWrite    v1              NoAuthNoPriv
ReadOnly    ReadWrite  ---         ReadWrite    v2c             NoAuthNoPriv
ReadWrite   ReadWrite  ReadWrite   ReadWrite    v1              NoAuthNoPriv
ReadWrite   ReadWrite  ReadWrite   ReadWrite    v2c             NoAuthNoPriv

Total Entries: 5

DGS-1100-10/ME:5>
```

show snmp global state

Purpose	To display the global state of SNMP currently configured on the Switch.
Syntax	show snmp global state
Description	The show snmp global state command displays the global state of SNMP groups currently configured on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display the currently configured SNMP global state on the Switch:

```
DGS-1100-10/ME:5>show snmp global state
Command: show snmp global state

SNMP Global State : Enable

DGS-1100-10/ME:5>
```

create snmp host

Purpose	To create a recipient of SNMP traps generated by the Switch's SNMP agent.
Syntax	create snmp host <ipaddr> [v1 <username 32> v2c <username

	32> v3 [noauth_nopriv auth_nopriv auth_priv] <username 32>]
Description	The create snmp host command creates a recipient of SNMP traps generated by the Switch's SNMP agent.
Parameters	<p><i><ipaddr></i> – The IP address of the remote management station to serve as the SNMP host for the Switch.</p> <p><i>v1</i> – Specifies that SNMP version 1 is to be used. The Simple Network Management Protocol (SNMP), version 1, is a network management protocol that provides a means to monitor and control network devices.</p> <p><i>v2c</i> – Specifies that SNMP version 2c is to be used. The SNMP v2c supports both centralized and distributed network management strategies. It includes improvements in the Structure of Management Information (SMI) and adds some security features.</p> <p><i>v3</i> – Specifies that the SNMP version 3 is to be used. SNMP v3 provides secure access to devices through a combination of authentication and encrypting packets over the network. SNMP v3 adds:</p> <ul style="list-style-type: none"> • Message integrity – ensures that packets have not been tampered with during transit. • Authentication – determines if an SNMP message is from a valid source. • Encryption – scrambles the contents of messages to prevent it being viewed by an unauthorized source. <p><i><username 32></i> – A string of up to 32 alphanumeric characters that identifies user names of an SNMP community. This string is used like a password to give remote SNMP managers access to MIB objects in the Switch's SNMP agent.</p> <p><i>noauth_nopriv</i> – Specifies that there is no authorization and no encryption of packets sent between the Switch and a remote SNMP manager.</p> <p><i>auth_nopriv</i> – Specifies that authorization is required, but there is no encryption of packets sent between the Switch and a remote SNMP manager.</p> <p><i>auth_priv</i> – Specifies that authorization is required, and that packets sent between the Switch and a remote SNMP manager are encrypted.</p>
Restrictions	Only Administrator and operator-level users can issue this command

Example usage:

To create an SNMP host to receive SNMP messages:

```
DGS-1100-10/ME:5>create snmp host 10.90.90.22 v3 noauth_nopriv dlink
Command: create snmp host 10.90.90.22 v3 noauth_nopriv dlink

Success!
DGS-1100-10/ME:5>
```

delete snmp host

Purpose To remove a recipient of SNMP traps generated by the Switch's

	SNMP agent.
Syntax	delete snmp host <ipaddr>
Description	The delete snmp host command deletes a recipient of SNMP traps generated by the Switch's SNMP agent.
Parameters	<ipaddr> – The IP address of a remote SNMP manager that receives SNMP traps generated by the Switch's SNMP agent.
Restrictions	Only Administrator or operator-level users can issue this command

Example usage:

To delete an SNMP host entry:

```
DGS-1100-10/ME:5>delete snmp host 10.90.90.22
Command: delete snmp host 10.90.90.22

Success!
DGS-1100-10/ME:5>
```

show snmp host

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

Example usage:

To display the currently configured SNMP hosts on the Switch:

```
DGS-1100-10/ME:5>show snmp host
Command: show snmp host

SNMP Host Table
(Maximum Entries : 10)

Host IP Address   SNMP Version   Community Name/SNMPv3 User Name
-----
10.90.90.22      V3-NoAuthNoPriv  dlink

Total Entries : 1

DGS-1100-10/ME:5>
```

create snmp v6host

Purpose	To create a recipient of SNMP traps generated by the Switch's SNMP agent.
Syntax	create snmp v6host <ip6_addr> [v1 <username 32> v2c <username 32> v3 [noauth_nopriv auth_nopriv auth_priv] <username 32>]
Description	The create snmp v6host command creates a recipient of SNMP traps generated by the Switch's SNMP agent.
Parameters	<p><i><ip6_addr></i> – The IPv6 address of the remote management station to serve as the SNMP host for the Switch.</p> <p><i>v1</i> – Specifies that SNMP version 1 is to be used. The Simple Network Management Protocol (SNMP), version 1, is a network management protocol that provides a means to monitor and control network devices.</p> <p><i>v2c</i> – Specifies that SNMP version 2c is to be used. The SNMP v2c supports both centralized and distributed network management strategies. It includes improvements in the Structure of Management Information (SMI) and adds some security features.</p> <p><i>v3</i> – Specifies that the SNMP version 3 is to be used. SNMP v3 provides secure access to devices through a combination of authentication and encrypting packets over the network. SNMP v3 adds:</p> <ul style="list-style-type: none"> • Message integrity – ensures that packets have not been tampered with during transit. • Authentication – determines if an SNMP message is from a valid source. • Encryption – scrambles the contents of messages to prevent it being viewed by an unauthorized source. <p><i><username 32></i> – A string of up to 32 alphanumeric characters that identifies user name of an SNMP community. This string is used like a password to give remote SNMP managers access to MIB objects in the Switch's SNMP agent.</p> <p><i>noauth_nopriv</i> – Specifies that there is no authorization and no encryption of packets sent between the Switch and a remote SNMP manager.</p> <p><i>auth_nopriv</i> – Specifies that authorization is required, but there is no encryption of packets sent between the Switch and a remote SNMP manager.</p> <p><i>auth_priv</i> – Specifies that authorization is required, and that packets sent between the Switch and a remote SNMP manager are encrypted.</p>
Restrictions	Only Administrator and operator-level users can issue this command

Example usage:

To create an SNMP host to receive SNMP messages:

```
DGS-1100-10/ME:5>create snmp v6host 3000::1 v3 noauth_nopriv dlink
Command: create snmp v6host 3000::1 v3 noauth_nopriv dlink
```

```
Success!
```

DGS-1100-10/ME:5>

delete snmp v6host	
Purpose	To remove a recipient of SNMP traps generated by the Switch's SNMP agent.
Syntax	delete snmp v6host <ip6_addr>
Description	The delete snmp host command deletes a recipient of SNMP traps generated by the Switch's SNMP agent.
Parameters	<i><ip6_addr></i> – The IPv6 address of a remote SNMP manager that receives SNMP traps generated by the Switch's SNMP agent.
Restrictions	Only Administrator or operator-level users can issue this command

Example usage:

To delete an SNMP host entry:

```

DGS-1100-10/ME:5>delete snmp v6host 90.90.22
Command: delete snmp host 10.90.90.22

Success!
DGS-1100-10/ME:5>
    
```

show snmp v6host	
Purpose	To display the recipient of SNMP traps generated by the Switch's SNMP agent.
Syntax	show snmp v6host {<ip6_addr>}
Description	The show snmp host command is used to display the IPv6 addresses and configuration information of remote SNMP managers that are designated as recipients of SNMP traps generated by the Switch's SNMP agent.
Parameters	<i><ip6_addr></i> – The IPv6 address of a remote SNMP manager that receives SNMP traps generated by the Switch's SNMP agent.
Restrictions	None.

Example usage:

To display the currently configured SNMP hosts on the Switch:

```

DGS-1100-10/ME:5>show snmp v6host
Command: show snmp v6host

SNMP Host Table
(Maximum Entries : 10)

Host IP Address           SNMP Version      Community or User Name
    
```

```

-----
3000::1                V3-NoAuthNoPriv  dlink

Success!
DGS-1100-10/ME:5>

```

enable snmp traps

Purpose	To enable SNMP trap support.
Syntax	enable snmp traps
Description	The enable snmp traps command enables SNMP trap support on the Switch.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command

Example usage:

To enable SNMP trap support on the Switch:

```

DGS-1100-10/ME:5>enable snmp traps
Command: enable snmp traps

Success!
DGS-1100-10/ME:5>

```

disable snmp traps

Purpose	To disable SNMP trap support on the Switch.
Syntax	disable snmp traps
Description	The disable snmp traps command disables SNMP trap support on the Switch.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To prevent SNMP traps from being sent from the Switch:

```

DGS-1100-10/ME:5>disable snmp traps
Command: disable snmp traps

Success!
DGS-1100-10/ME:5>

```

show snmp traps

Purpose	To display SNMP trap support status on the Switch.
---------	--

Syntax	show snmp traps
Description	The show snmp traps command displays the SNMP trap support status currently configured on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To view the current SNMP trap support:

```
DGS-1100-10/ME:5> show snmp traps
Command: show snmp traps

SNMP Traps : Disabled
SNMP Authentication Traps : Disabled
Coldstart Traps : Disabled
Warmstart Traps : Disabled
Firmware Upgrade Traps : Disabled
Port Security violation Traps : Disabled
Loopback detection Traps : Disabled
Duplicate IP Detected Traps : Disabled
Fiber Port Link Up/Down Traps : Disabled
Twisted Pair Port Link Up/Down Traps : Disabled

DGS-1100-10/ME:5>
```

enable snmp authenticate traps

Purpose	To enable SNMP authentication trap support.
Syntax	enable snmp authenticate traps
Description	The enable snmp authenticate traps command enables SNMP authentication trap support on the Switch.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command

Example usage:

To turn on SNMP authentication trap support:

```
DGS-1100-10/ME:5>enable snmp authenticate traps
Command: enable snmp authenticate traps

Success!
DGS-1100-10/ME:5>
```

disable snmp authenticate traps

Purpose	To disable SNMP authentication trap support.
Syntax	disable snmp authenticate traps
Description	The disable snmp authenticate traps command disables SNMP authentication trap support on the Switch.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command

Example usage:

To disable the SNMP authentication trap support:

```
DGS-1100-10/ME:5>disable snmp authenticate traps
Command: disable snmp authenticate traps

Success!
DGS-1100-10/ME:5>
```

config syslocation

Purpose	To enter a description of the location of the Switch.
Syntax	config syslocation <string 32>
Description	The config syslocation command enters a description of the location of the Switch. A maximum of 32 characters can be used.
Parameters	<string 32> - A maximum of 32 characters is allowed.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure the Switch location for 'HQ5F':

```
DGS-1100-10/ME:5>config syslocation HQ5F
Command: config syslocation HQ5F

Success!
DGS-1100-10/ME:5>
```

config sysname

Purpose	To define the name for the Switch.
Syntax	config sysname <string 32>
Description	The config sysname command defines the name of the Switch.
Parameters	<string 32> - A maximum of 32 characters is allowed.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure the Switch name as '10ME':

```
DGS-1100-10/ME:5>config sysname 10ME
Command: config sysname 10ME

Success!
DGS-1100-10/ME:5>
```

enable snmp

Purpose	To enable SNMP support.
Syntax	enable snmp
Description	The enable snmp command enables SNMP support on the Switch.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To enable SNMP support on the Switch:

```
DGS-1100-10/ME:5>enable snmp
Command: enable snmp

Success!
DGS-1100-10/ME:5>
```

disable snmp

Purpose	To disable SNMP support.
Syntax	disable snmp
Description	The disable snmp command disables SNMP support on the Switch.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To disable SNMP support on the Switch:

```
DGS-1100-10/ME:5>disable snmp
Command: disable snmp

Success!
DGS-1100-10/ME:5>
```

enable snmp fiber_port_link traps

Purpose	To enable SNMP fiber port link traps support on the Switch.
Syntax	enable snmp fiber_port_link traps
Description	The enable snmp fiber_port_link traps command enables SNMP fiber port link traps support on the Switch. After enabling the SNMP fiber port link traps support, the Switch will send out a trap to the SNMP manage host when the fiber port is link up or link down.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command

Example usage:

To enable SNMP fiber port link traps support on the Switch:

```
DGS-1100-10/ME:5>enable snmp fiber_port_link traps
Command: enable snmp fiber_port_link traps

Success!
DGS-1100-10/ME:5>
```

disable snmp fiber_port_link traps

Purpose	To disable SNMP fiber port link traps.
Syntax	disable snmp fiber_port_link traps
Description	The disable snmp fiber_port_link traps command disables SNMP fiber port link traps support on the Switch.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command

Example usage:

To disable SNMP fiber port link traps support on the Switch:

```
DGS-1100-10/ME:5>disable snmp fiber_port_link traps
Command: disable snmp fiber_port_link traps

Success!
DGS-1100-10/ME:5>
```

enable snmp LBD traps

Purpose	To enable SNMP LBD traps.
Syntax	enable snmp LBD traps
Description	The enable snmp LBD traps command enables SNMP LBD traps support on the Switch.
Parameters	None.

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

Example usage:

To enable SNMP LBD traps support on the Switch:

```
DGS-1100-10/ME:5>enable snmp LBD traps
Command: enable snmp LBD traps

Success!
DGS-1100-10/ME:5>
```

disable snmp LBD traps

Purpose	To disable SNMP LBD traps.
Syntax	disable snmp LBD traps
Description	The disable snmp LBD traps command disables SNMP LBD traps support on the Switch.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To disable SNMP LBD traps support on the Switch:

```
DGS-1100-10/ME:5>disable snmp LBD traps
Command: disable snmp LBD traps

Success!
DGS-1100-10/ME:5>
```

enable snmp port_security_violation traps

Purpose	To enable SNMP port security violation traps.
Syntax	enable snmp port_security_violation traps
Description	The enable snmp port_security_violation traps command enables SNMP port security violation traps on the Switch.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To enable SNMP port security violation traps support on the Switch:

```
DGS-1100-10/ME:5>enable snmp port_security_violation traps
Command: enable snmp port_security_violation traps
```

```
Success!
DGS-1100-10/ME:5>
```

disable snmp port_security_violation traps

Purpose	To disable SNMP port security violation traps.
Syntax	disable snmp port_security_violation traps
Description	The disable snmp port_security_violation traps command disables SNMP port security violation traps on the Switch.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To disable SNMP port security violation traps support on the Switch:

```
DGS-1100-10/ME:5>disable snmp port_security_violation traps
Command: disable snmp port_security_violation traps

Success!
DGS-1100-10/ME:5>
```

enable snmp twistedpair_port_link traps

Purpose	To enable SNMP twisted pair ports link traps support on the Switch.
Syntax	enable snmp twistedpair_port_link traps
Description	The enable snmp twistedpair_port_link traps command enables SNMP twisted pair ports link traps support on the Switch.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To enable the SNMP twisted pair ports link traps on the Switch:

```
DGS-1100-10/ME:5>enable snmp twistedpair_port_link traps
Command: enable snmp twistedpair_port_link traps

Success!
DGS-1100-10/ME:5>
```

disable snmp twistedpair_port_link traps

Purpose	To disable SNMP twisted pair ports link traps support on the Switch.
Syntax	disable snmp twistedpair_port_link traps
Description	The disable snmp twistedpair_port_link traps command disables SNMP twisted pair ports link traps support on the Switch.
Parameters	None.

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

Example usage:

To disable the SNMP twisted pair ports link traps on the Switch:

```
DGS-1100-10/ME:5>disable snmp twistedpair_port_link traps  
Command: disable snmp twistedpair_port_link traps  
  
Success!  
DGS-1100-10/ME:5>
```

DOWNLOAD/UPLOAD COMMANDS

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

Command	Parameter
download	[<i>cfg_fromTFTP</i> [<ipaddr> <ipv6_addr>] <path_filename 64>] [<i>firmware_fromTFTP</i> [<ipaddr> <ipv6_addr>] < path_filename 64>] [<i>log_fromTFTP</i> [<ipaddr> <ipv6_addr>] <path_filename 64>] [<i>log_toTFTP</i> [<ipaddr> <ipv6_addr>] <path_filename 64>]
upload	[[<i>firmware_toTFTP</i> [<ipaddr> <ipv6_addr>] <path_filename 64>] [<i>cfg_toTFTP</i> [<ipaddr> <ipv6_addr>] <path_filename 64>]

Each command is listed in detail, as follows:

download	
Purpose	To download and install a firmware, boot, or switch configuration file from a TFTP server.
Syntax	download [<i>cfg_fromTFTP</i> [<ipaddr> <ipv6_addr>] <path_filename 64>] [<i>firmware_fromTFTP</i> [<ipaddr> <ipv6_addr>] < path_filename 64>] [<i>log_fromTFTP</i> [<ipaddr> <ipv6_addr>] <path_filename 64>] [<i>log_toTFTP</i> [<ipaddr> <ipv6_addr>] <path_filename 64>]
Description	The download command downloads a firmware, boot, log or switch configuration file from a TFTP server.
Parameters	<p><i>cfg_fromTFTP</i> – Downloads a switch configuration file from a TFTP server.</p> <p><ipaddr> – The IPv4 address of the TFTP server.</p> <p><ipv6_addr> – The IPv6 address of the TFTP server.</p> <p><path_filename 64> – The DOS path and filename of the switch configuration file, up to 64 characters, on the TFTP server. For example, C:\31xx.had.</p> <p><i>startup</i> – Indicates the Configuration file is to be downloaded to the startup config.</p> <p><i>firmware_fromTFTP</i> – Downloads and installs firmware on the Switch from a TFTP server.</p> <p>< path_filename 64> – The DOS path and filename of the firmware file or log file, up to 64 characters, on the TFTP server. For example, C:\31xx.had.</p> <p><i>log_fromTFTP</i> – Downloads a log file from a TFTP server.</p> <p><i>cfg_toTFTP</i> – Downloads a log file to a TFTP server.</p>
Restrictions	Only Administrator or operator-level users can issue this command.

Parameters	<p><i>firmware_toTFTP</i> – Specifies that the Switch’s current firmware are to be uploaded to the TFTP server.</p> <p><i><ipaddr></i> – The IPv4 address of the TFTP server. The TFTP server must be on the same IP subnet as the Switch.</p> <p><i><ipv6_addr></i> – The IPv6 address of the TFTP server. The TFTP server must be on the same IP subnet as the Switch.</p> <p><i><path_filename 64></i> – The location of the Switch configuration file on the TFTP server.</p> <p><i>cfg_fromTFTP</i> – Uploads a switch configuration file from a TFTP server.</p>
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

```

DGS-1100-10/ME:5>upload cfg_toTFTP 1.1.1.23 dgs_1100-10me.ros
Command: upload log_toTFTP 1.1.1.23 dgs_1100-10me.ros
01-Jan-2000 01:26:11 %COPY-I-FILECPY: Files Copy - source
URL running-config destination URL tftp://1.1.1.23/1/running-
config
...01-Jan-2000 01:26:16 %COPY-W-TRAP: The copy operation
was completed success fully!
158 bytes copied in 00:00:05 [hh:mm:ss]

DGS-1100-10/ME:5>

```

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	Parameter
enable dhcp_relay	
disable dhcp_relay	
config dhcp_relay add ipif system	<ipaddr>
config dhcp_relay delete ipif system	<ipaddr>
config dhcp_relay hops	<value 1-16>
config dhcp_relay option_82	[check [enable disable] policy [drop keep replace] remote_id [default user_define <string 32>] state [enable disable]]
show dhcp_relay	{ipif}
enable dhcp_local_relay	
disable dhcp_local_relay	
config dhcp_local_relay	vlan [<vlan_name 20> vlanid <vidlist>] state[enable disable]
show dhcp_local_relay	
enable dhcpv6_relay	
disable dhcpv6_relay	
show dhcpv6_relay	{ipif system}
config dhcpv6_relay	[add delete] ipif System <ipv6_addr>
config dhcpv6_relay hop_count	<value 1-32>
Config dhcpv6_relay option_37	[state [enable disable] check] [enable disable] remote_id [default cid_with_user_define <string 128> user_define <string 128>]]

Each command is listed in detail, as follows:

enable dhcp_relay	
Purpose	To enable DHCP Relay server on the Switch
Syntax	enable dhcp_relay
Description	The enable dhcp_relay command sets the DHCP Relay to be globally enabled on the Switch and on all existing VLANs.

Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To enable DHCP Relay on the Switch:

```
DGS-1100-10/ME:5>enable dhcp_relay
Command: enable dhcp_relay

Success!
DGS-1100-10/ME:5>
```

disable dhcp_relay

Purpose	To disable DHCP Relay server on the Switch
Syntax	disable dhcp_relay
Description	The disable dhcp_relay command sets the DHCP Relay to be globally disabled on the Switch and on all existing VLANs.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To disable DHCP Relay on the Switch:

```
DGS-1100-10/ME:5>disable dhcp_relay
Command: disable dhcp_relay

Success!
DGS-1100-10/ME:5>
```

config dhcp_relay add ipif System

Purpose	To define a DHCP server as a DHCP Relay server
Syntax	config dhcp_relay add ipif System <ipaddr>
Description	The config dhcp_relay add ipif System command adds DHCP servers as DHCP Relay servers.
Parameters	<ipaddr> – The IP address of the DHCP server. Up to 4 servers can be defined.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To add a DHCP server as a DHCP Relay server:

```
DGS-1100-10/ME:5>config dhcp_relay add ipif System 10.6.150.49
Command: config dhcp_relay add ipif System 10.6.150.49
```

Success!

DGS-1100-10/ME:5>

config dhcp_relay delete ipif System

Purpose	To delete a DHCP server from the DHCP Relay server list.
Syntax	config dhcp_relay delete ipif System <ipaddr>
Description	The config dhcp_relay delete ipif System command deletes a DHCP server defined as a DHCP Relay server.
Parameters	<ipaddr> – The IP address of the DHCP server.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

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

```
DGS-1100-10/ME:5>config dhcp_relay delete ipif System 10.6.150.49
```

```
Command: config dhcp_relay delete ipif System 10.6.150.49
```

Success!

DGS-1100-10/ME:5>

config dhcp_relay hops

Purpose	To delete a DHCP server from the DHCP Relay server list.
Syntax	config dhcp_relay hops <value 1-16>
Description	The config dhcp_relay hops command configures the DHCP/BOOTP relay feature.
Parameters	<value 1-16> – Specifies the maximum number of relay agent hops that the DHCP packets can cross.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure the DHCP relay on the Switch:

```
DGS-1100-10/ME:5>config dhcp_relay hops 12
```

```
Command: config dhcp_relay hops 12
```

Success!

DGS-1100-10/ME:5>

config dhcp_relay option_82

Purpose	To configure the check, policy, and state of the DHCP relay agent information option 82 field of the Switch.
Syntax	config dhcp_relay option_82 [check [enable disable] policy [drop keep replace] remote_id [default user_define <string 32>] state [enable disable]]
Description	The config dhcp_relay option_82 is used to configure the check, policy and state of DHCP relay agent information option 82 of the Switch
Parameters	<p><i>check</i>: used to configure the check of DHCP relay agent information option 82 of the Switch.</p> <p><i>enable</i> – When the field is toggled to enable, the relay agent will check the validity of the packet's option 82 field. If the switch receives a packet that contains the option 82 field from a DHCP client, the switch drops the packet because it is invalid. In packets received from DHCP servers, the relay agent will drop invalid messages.</p> <p><i>disable</i> – When the field is toggled to disable, the relay agent will not check the validity of the packet's option 82 field.</p> <p><i>policy</i>: used to configure the re-forwarding policy of DHCP relay agent information option 82 of the Switch.</p> <p><i>replace</i> – The option 82 field will be replaced if the option 82 field already exists in the packet received from the DHCP client.</p> <p><i>drop</i> – The packet will be dropped if the option 82 field already exists in the packet received from the DHCP client.</p> <p><i>keep</i> – The option 82 field will be retained if the option 82 field already exists in the packet received from the DHCP client.</p> <p><i>state</i>: used to configure the state of DHCP relay agent information option 82 of the Switch.</p> <p><i>enable</i> – When this field is toggled to Enabled the relay agent will insert and remove DHCP relay information (option 82 field) in messages between DHCP server and client. When the relay agent receives the DHCP request, it adds the option 82 information, and the IP address of the relay agent (if the relay agent is configured), to the packet. Once the option 82 field information has been added to the packet it is sent on to the DHCP server. When the DHCP server receives the packet, if the server is capable of option 82, it can implement policies like restricting the number of IP addresses that can be assigned to a single remote ID or circuit ID. Then the DHCP server echoes the option 82 field in the DHCP reply. The DHCP server unicasts the reply to the back to the relay agent if the request was relayed to the server by the relay agent. The switch verifies that it originally inserted the option 82 data. Finally, the relay agent removes the option 82 field and forwards the packet to the switch port that connects to the DHCP client that sent the DHCP request.</p> <p><i>disable</i> – If the field is toggled to disable the relay agent will not insert and remove DHCP relay information (option 82 field) in messages between DHCP servers and clients, and the check and policy settings will have no effect.</p>
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To disable the DHCP relay option 82 on the Switch:

```
DGS-1100-10/ME:5>config dhcp_relay option_82 state disable
Command: config dhcp_relay option_82 state disable

Success!
DGS-1100-10/ME:5>
```

show dhcp_relay

Purpose	To display the DHCP Relay settings on the Switch.
Syntax	show dhcp_relay {ipif}
Description	The show dhcp_relay command displays the DHCP Relay status and list of servers defined as DHCP Relay servers on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display DHCP Relay settings:

```
DGS-1100-10/ME:5> show dhcp_relay
Command: show dhcp_relay

DHCP Relay Status                : Enabled
DHCP Relay Hops Count Limit      : 4
DHCP Relay Time Threshold        : 0
DHCP Relay Agent Information Option82 State : Enabled
DHCP Relay Agent Information Option82 Check : Enabled
DHCP Relay Agent Information Option82 Policy : replace
DHCP Relay Agent Information Option82 Remote ID : string
DGS-1100-10/ME:5>
```

enable dhcp_local_relay

Purpose	To enable the DHCP local relay feature globally
Syntax	enable dhcp_local_relay
Description	The enable dhcp_local_relay command enables the DHCP local relay feature on the Switch.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To enable the DHCP Local Relay:

```
DGS-1100-10/ME:5>enable dhcp_local_relay
Command: enable dhcp_local_relay
```

```

Success
DGS-1100-10/ME:5>

```

disable dhcp_local_relay

Purpose	To disable the DHCP local relay feature globally
Syntax	disable dhcp_local_relay
Description	The disable dhcp_local_relay command disables the DHCP local relay feature on the Switch.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To disable the DHCP Local Relay:

```

DGS-1100-10/ME:5>disable dhcp_local_relay
Command: disable dhcp_local_relay

Success!
DGS-1100-10/ME:5>

```

config dhcp_local_relay

Purpose	To specify which VLAN's the feature works on.
Syntax	config dhcp_local_relay vlan [<vlan_name 20> vlanid <vidlist>] state[enable disable]
Description	Each VLAN which was added to the DHCP Local Relay list participates in the DHCP Local Relay process – Option 82 is added to DHCP requests on this VLAN, and Removed from DHCP Replies on this VLAN.
Parameters	<i><vlan_name 20></i> – the VLAN name identifier <i>vlanid <vidlist></i> – The VLAN tag identifier <i>state [enable disable]</i> – enable or disable the DHCP Local Relay status by VLAN name or VLAN ID.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To disable the VLAN ID10 from VLAN of DHCP Local Relay:

```

DGS-1100-10/ME:5>config dhcp_local_relay vlan vlanid 10 state disable
Command: config dhcp_local_relay vlan vlanid 10 state disable

Success!
DGS-1100-10/ME:5>

```

show dhcp_local_relay

Purpose	To display which VLAN's the feature works on.
Syntax	show dhcp_local_relay
Description	Each VLAN which was added to the DHCP Local Relay list participates in the DHCP Local Relay process – Option 82 is added to DHCP requests on this VLAN, and Removed from DHCP Replies on this VLAN.
Parameters	None.
Restrictions	None.

Example usage:

To display the DHCP local relay information on the Switch:

```
DGS-1100-10/ME:5> show dhcp_local_relay
Command: show dhcp_local_relay

DHCP Local Relay Status      : Disabled
DHCP Local Relay VID List    : 1
DGS-1100-10/ME:5>
```

enable dhcpv6_relay

Purpose	To enable DHCPv6 Relay function on the Switch
Syntax	enable dhcpv6_relay
Description	The enable dhcpv6_relay command is used to enable the DHCPv6 relay global state on the Switch.
Parameters	None.
Restrictions	Only Administrator or operate-level users can issue this command.

Example usage:

To enable DCHPv6 Relay on the Switch:

```
DGS-1100-10/ME:5>enable dhcpc6_relay
Command: enable dhcpc6_relay

Success!
DGS-1100-10/ME:5>
```

disable dhcpv6_relay

Purpose	To disable DHCPv6 Relay function on the Switch
Syntax	disable dhcpv6_relay
Description	The disable dhcpv6_relay command is used to disable the DHCPv6 relay global state on the Switch.

Parameters	None.
Restrictions	Only Administrator or operate-level users can issue this command.

Example usage:

To disable DHCPv6 Relay on the Switch:

```
DGS-1100-10/ME:5>disable dhcpv6_relay
Command: disable dhcpv6_relay

Success!
DGS-1100-10/ME:5>
```

show dhcpv6_relay

Purpose	To display the current DHCPv6 relay configuration.
Syntax	show dhcpv6_relay {ipif system}
Description	The show dhcpv6_relay command displays the current DHCPv6 relay configuration for all interfaces, if a IP interface name is specified, it will display the DHCPv6 relay configuration for that IP interface.
Parameters	None.
Restrictions	None.

Example usage:

To display DHCPv6 Relay settings:

```
DGS-1100-10/ME:5> show dhcpv6_relay
Command: show dhcpv6_relay

DHCPv6 Relay Status           : Enabled
DHCPv6 Relay Hops Count Limit : 4
DHCPv6 Relay Option37 State   : Disabled
DHCPv6 Relay Option37 Check   : Disabled
DHCPv6 Relay Option37 Remote ID : DE-AD-BE-EF-01-02
DGS-1100-10/ME:5>
```

config dhcpv6_relay

Purpose	Used to add or delete a destination IP address in the switch's DHCPv6 relay table.
Syntax	config dhcpv6_relay [add delete] ipif System <ipv6_addr>
Description	The config dhcpv6_relay command can add or delete an IPv6 destination address used to forward (relay) DHCPv6 packets.
Parameters	<i>add</i> – Add an IPv6 destination to the DHCPv6 relay table. <i>delete</i> – Remove an IPv6 destination to the DHCPv6 relay table. <i>ipif system</i> – The name of the IP interface in which DHCPv6 relay is

	to be enabled. <ip6v6_addr> – The DHCPv6 server IP address.
Restrictions	Only Administrator or operate-level users can issue this command.

Example usage:

To add the DHCPv6 relay on the Switch:

```
DGS-1100-10/ME:5>config dhcpv6_relay add ipif System 3000::1
Command: config dhcpv6_relay add ipif System 3000::1

Success!
DGS-1100-10/ME:5>
```

config dhcpv6_relay hop_count

Purpose	Used to configure the DHCPv6 relay hop count of the switch.
Syntax	config dhcpv6_relay hop_count <value 1-32>
Description	The config dhcpv6_relay hops_count command is used to configure the DHCPv6 relay hop count of the switch.
Parameters	<value 1-32> – 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 or operate-level users can issue this command.

Example usage:

To configure the DHCPv6 relay hop count on the Switch:

```
DGS-1100-10/ME:5>config dhcpv6_relay hop_count 3
Command: config dhcpv6_relay hop_count 3

Success!
DGS-1100-10/ME:5>
```

config dhcpv6_relay option_37

Purpose	Used to configure the DHCPv6 relay option 37 of the switch.
Syntax	config dhcpv6_relay option_37 [state [enable disable]] check [enable disable] remote_id [default cid_with_user_define <string 128> user_define <string 128>]]
Description	The config dhcpv6_relay hops_count command is used to configure the DHCPv6 Relay option 37 function. When DHCPv6 relay option 37 is enabled, the DHCP packet is inserted with the option 37 field before being relayed to the server. The DHCP packet will be processed based on the behavior defined in the check and remote ID type setting. When the state is disabled, the DHCP packet is relayed directly to the server. □
Parameters	<i>state [enable disable]</i> - Specify DHCPv6 relay option37 state.

When the state is enabled, the DHCP packet is inserted with the option 37 field before being relayed to the server. When the state is disabled, the DHCP packet is relayed directly to the server.

check [enable | disable] - Specify to check the packets or not. When the check state is enabled, packets from client side should not have the option 37 field. If client originating packets have the option 37 field, they will be dropped. Specify for not checking the packets.

remote_id [default | cid_with_user_define <string 128> | user_define <string 128>] - Specify the content in the remote ID.

default – Specify to have the remote ID as VLAN ID + Module + Port + System MAC address of the device.

cid_with_user_define – Specify to have the remote ID as VLAN ID + Module + Port + user defined string.

user_define – Use the user-defined string as the remote ID. □

Restrictions

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

Example usage:

To configure the DHCPv6 relay hop count on the Switch:

```
DGS-1100-10/ME:5>config dhcpv6_relay hop_count 3
```

```
Command: config dhcpv6_relay hop_count 3
```

```
Success!
```

```
DGS-1100-10/ME:5>
```

NETWORK MONITORING COMMANDS

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

Command	Parameter
show packet ports	<portlist 1-10>
show error ports	<portlist 1-10>
show utilization	[ports {<portlist>} cpu mem]
clear counters ports	<porlist 1-10>
clear log	
show log	{[index <value 1-500> - <value 1-500>] severity [debug informational warning]}
save log	
enable syslog	
disable syslog	
create syslog host	<index 1-4> ipaddress [<ipaddr> <ipv6addr>] {severity [informational warning debug] facility [local0 local1 local2 local3 local4 local5 local6 local7] state [enable disable] udp_port [514 <udp_port_number 6000-65535>]}
config syslog host	[all <index 1-4>] {severity [informational warning debug] facility [local0 local1 local2 local3 local4 local5 local6 local7] state [enable disable] udp_port [514 <udp_port_number 6000-65535>] ipaddress [<ipaddr> <ipv6addr>]}
delete syslog host	[<index 1-4> all]
show syslog host	{<index 1-4>}
cable diagnostic port	[<portlist 1-10> all]

Each command is listed in detail, as follows:

show packet ports	
Purpose	To display statistics for the packets sent and received in frames per second by the Switch.
Syntax	show packet ports <portlist 1-10>
Description	The show packet ports command displays statistics about packets sent and received by ports specified in the port list. The results are separated into three tables, labeled A, B, and C in the window below. Table A is relevant to the size of the packets, Table B is relevant to the type of packets and Table C is relevant to the type of frame associated with these packets.
Parameters	<portlist 1-10> – A port or range of ports whose statistics are to be

	displayed.
Restrictions	None.

Example usage:

To display the packets analysis for port 7:

```
DGS-1100-10/ME:5>show packet ports
Command: show packet ports

Port Number : 1
Frame Size  Frame Counts  Frames/sec  Frame Type  Total  Total/sec
-----
64          2161          2           RX Bytes   168377  128
65-127      249           0           RX Frames  2435    2
128-255     18            0
256-511     7             0           TX Bytes   331492  1071
512-1023    0             0           TX Frames  3550    3
1024-1518   0             0

Unicast RX  2158          2
Multicast RX 5            0
Broadcast RX 272          0

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

show error ports

Purpose	To display the error statistics for a port or a range of ports.
Syntax	show error ports <portlist 1-10>
Description	The show error ports command displays all of the packet error statistics collected and logged by the Switch for a given port list.
Parameters	<i><portlist 1-10></i> – A port or range of ports whose error statistics are to be displayed.
Restrictions	None.

Example usage:

To display the errors of port 1:

```
DGS-1100-10/ME:5>show errors port 1
Command: show error ports 1

Port Number : 1
RX Frames          TX Frames
-----
CRC Error          0          Excessive Deferral  0
Undersize          0          CRC Error            0
```

Oversize	0	Late Collision	0
Fragment	8	Excessive Collision	0
Jabber	0	Single Collision	0
Drop Pkts	0	Collision	0

DGS-1100-10/ME:5>

show utilization

Purpose	To display real-time port utilization statistics.
Syntax	show utilization [ports {<portlist 1-10>} cpu dram]
Description	The show utilization command displays the real-time utilization statistics for ports in bits per second (bps) for the Switch, and for the CPU in a percentage.
Parameters	<p><i>ports{</i> – Entering this parameter will display the current port utilization of the Switch.</p> <p><i><portlist 1-10></i> – Specifies a range of ports to be displayed.</p> <p><i>cpu</i> – Entering this parameter will display the current CPU utilization of the Switch.</p> <p><i>dram</i> – Entering this parameter will display the current memory utilization of the Switch.</p>
Restrictions	None.

To display the port 2 utilization statistics:

```
DGS-1100-10/ME:5>show utilization ports 2
Command: show utilization ports 2

Port TX/sec RX/sec Util
-----
2    0    0    0

CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
DGS-1100-10/ME:5>
```

To display the cpu utilization statistics:

```
DGS-1100-10/ME:5>show utilization cpu
Command: show utilization cpu
CPU Utilization:
-----
Five Seconds: 2%
One Minute : 2%
Five Minute : 2%
```

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

DGS-1100-10/ME:5>

clear counters

Purpose	To clear the Switch's statistics counters.
Syntax	clear counters ports <porlist 1-10>
Description	The clear counters command clears the counters used by the Switch to compile statistics.
Parameters	<portlist 1-10> – Specifies a range of ports to be cleared.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To clear the counters:

```
DGS-1100-10/ME:5> clear counters ports 2-5
Command: clear counters ports 2-5

Success!
DGS-1100-10/ME:5>
```

clear log

Purpose	To clear the Switch's history log.
Syntax	clear log
Description	The clear log command clears the Switch's history log.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To clear the log information:

```
DGS-1100-10/ME:5>clear log
Command: clear log

Success!
DGS-1100-10/ME:5>
```

show log

Purpose	To display the Switch history log.
Syntax	show log {[index <value 1-500> - <value 1-500>] severity [debug informational warning]}
Description	The show log command displays the contents of the Switch's

	history log.
Parameters	<i>index</i> <value 1-500> – The number of entries in the history log to display. <i>severity</i> [<i>debug</i> <i>informational</i> <i>warning</i>] – Specifies the severity type to be displayed.
Restrictions	None.

Example usage:

To display the Switch history log:

DGS-1100-10/ME:5> show log index 1 - 2			
Command: show log index 1 - 2			
Index	Time	Log Text	Log Severity
----	-----	-----	-----
DGS-1100-10/ME:5>			

save log

Purpose	To save the Switch history log.
Syntax	save log
Description	The save log command saves the contents of the Switch's history log.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To save the Switch history log:

DGS-1100-10/ME:5> save log
Command: save log
Success!
DGS-1100-10/ME:5>

enable syslog

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

Example usage:

To enable the syslog function on the Switch:

```
DGS-1100-10/ME:5>enable syslog
Command: enable syslog

Success!
DGS-1100-10/ME:5>
```

disable syslog	
Purpose	To disable the system log from being sent to a remote host.
Syntax	disable syslog
Description	The disable syslog command disables the system log from being sent to a remote host.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To disable the syslog function on the Switch:

```
DGS-1100-10/ME:5>disable syslog
Command: disable syslog

Success!
DGS-1100-10/ME:5>
```

create syslog host					
Purpose	To create a new syslog host.				
Syntax	create syslog host <index 1-4> ipaddress [<ipaddr> <ipv6addr>] {severity [informational warning debug] facility [local0 local1 local2 local3 local4 local5 local6 local7] state [enable disable] udp_port [514 <udp_port_number 6000-65535>]}				
Description	The create syslog host command creates a new syslog host.				
Parameters	<p><i>all</i> – Specifies that the command is to be applied to all hosts.</p> <p><i><index 1-4></i> – The syslog host index id. There are four available indices, numbered 1 to 4.</p> <p><i>ipaddress [<ipaddr> <ipv6addr>]</i> – The IPv4 or IPv6 address of the remote host to which syslog messages are to be sent.</p> <p><i>severity</i> – The message severity level indicator. These are described in the table below (Bold font indicates that the corresponding severity level is currently supported on the Switch):</p> <table border="1" style="margin-left: 40px;"> <thead> <tr> <th>Numerical Code</th> <th>Severity</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> </tr> </tbody> </table>	Numerical Code	Severity		
Numerical Code	Severity				

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

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

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

debug – Specifies that debug message are to be sent to the remote host.

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

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

22	local use 6 (local6)
23	local use 7 (local7)
	<p><i>local0</i> – Specifies that local use 0 messages are to be sent to the remote host. This corresponds to number 16 from the list above.</p> <p><i>local1</i> – Specifies that local use 1 messages are to be sent to the remote host. This corresponds to number 17 from the list above.</p> <p><i>local2</i> – Specifies that local use 2 messages are to be sent to the remote host. This corresponds to number 18 from the list above.</p> <p><i>local3</i> – Specifies that local use 3 messages are to be sent to the remote host. This corresponds to number 19 from the list above.</p> <p><i>local4</i> – Specifies that local use 4 messages are to be sent to the remote host. This corresponds to number 20 from the list above.</p> <p><i>local5</i> – Specifies that local use 5 messages are to be sent to the remote host. This corresponds to number 21 from the list above.</p> <p><i>local6</i> – Specifies that local use 6 messages are to be sent to the remote host. This corresponds to number 22 from the list above.</p> <p><i>local7</i> – Specifies that local use 7 messages is sent to the remote host. This corresponds to number 23 from the list above.</p> <p><i>udp_port [514 <udp_port_number 6000-65535>]</i> – Specifies the UDP port number that the syslog protocol is to use to send messages to the remote host.</p> <p><i>state [enable disable]</i> – Allows the sending of syslog messages to the remote host, specified above, to be enabled and disabled.</p>
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To create syslog host:

```
DGS-1100-10/ME:5> create syslog host 1 ipaddress 1.1.2.1 severity informational
facility local0 state enable
Command: create syslog host 1 ipaddress 1.1.2.1 severity informational facility
local0 state enable

Success!
DGS-1100-10/ME:5>
```

config syslog host

Purpose	To configure the syslog protocol to send system log data to a remote host.
Syntax	config syslog host [<i>all</i> <index 1-4>] {severity [<i>informational</i> <i>warning</i> <i>debug</i>] facility [<i>local0</i> <i>local1</i> <i>local2</i> <i>local3</i> <i>local4</i> <i>local5</i> <i>local6</i> <i>local7</i>] state [<i>enable</i> <i>disable</i>] udp_port [514 <udp_port_number 6000-65535>] ipaddress [<ipaddr> <ipv6addr>]}
Description	The config syslog host command configures the syslog protocol to send system log information to a remote host.
Parameters	<i>all</i> – Specifies that the command applies to all hosts. <index 1-4> – Specifies that the command applies to an index of

hosts. There are four available indices, numbered 1 to 4.

severity – The message severity level indicator. These are described in the following table (Bold font indicates that the corresponding severity level is currently supported on the Switch):

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

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

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

debug – Specifies that debug message are to be sent to the remote host.

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

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

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

15	clock daemon
16	local use 0 (local0)
17	local use 1 (local1)
18	local use 2 (local2)
19	local use 3 (local3)
20	local use 4 (local4)
21	local use 5 (local5)
22	local use 6 (local6)
23	local use 7 (local7)

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

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

local2 – Specifies that local use 2 messages are to be sent to the remote host. This corresponds to number 18 from the list above.

local3 – Specifies that local use 3 messages are to be sent to the remote host. This corresponds to number 19 from the list above.

local4 – Specifies that local use 4 messages are to be sent to the remote host. This corresponds to number 20 from the list above.

local5 – Specifies that local use 5 messages are to be sent to the remote host. This corresponds to number 21 from the list above.

local6 – Specifies that local use 6 messages are to be sent to the remote host. This corresponds to number 22 from the list above.

local7 – Specifies that local use 7 messages are to be sent to the remote host. This corresponds to number 23 from the list above.

udp_port [514 | <udp_port_number 6000-65535>] – Specifies the UDP port number that the syslog protocol is to use to send messages to the remote host.

ipaddress [<ipaddr> | <ipv6addr>] – Specifies the IPv4 or IPv6 address of the remote host to which syslog messages are to be sent.

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

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

Example usage:

To configure a syslog host:

```
DGS-1100-10/ME:5> config syslog host 1 severity debug
Command: config syslog host 1 severity debug
```

Success!

```
DGS-1100-10/ME:5>
```

delete syslog host

Purpose To remove a previously configured syslog host from the Switch.

Syntax **delete syslog host [<index 1-4> | all]**

Description	The delete syslog host command removes a previously configured syslog host from the Switch.
Parameters	<i><index 1-4></i> – The syslog host index id. There are four available indices, numbered 1 to 4. <i>all</i> – Specifies that the command applies to all hosts.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To delete a previously configured syslog host:

```
DGS-1100-10/ME:5>delete syslog host all
Command: delete syslog host all

Success!
DGS-1100-10/ME:5>
```

show syslog host	
Purpose	To display the syslog hosts currently configured on the Switch.
Syntax	show syslog host {<index 1-4>}
Description	The show syslog host command displays the syslog hosts that are currently configured on the Switch.
Parameters	<i><index 1-4></i> – The syslog host index id. There are four available indices, numbered 1 to 4.
Restrictions	None.

Example usage:

To show Syslog host information:

```
DGS-1100-10/ME:5> show syslog host
Command: show syslog host

Host 1
  IP Address: 1.1.2.1
  Severity   : Debug
  Facility   : local0
  UDP Port   : 514
  Status     : Enabled

Total Entries: 1
DGS-1100-10/ME:5>
```

cable diagnostic port	
Purpose	To determine if there are any errors on the copper cables and the position where the errors may have occurred.

Syntax	cable diagnostic port [<portlist 1-10> all]
Description	The cable diagnostic port command is used to determine if there are any errors on the copper cables and the position where the errors may have occurred. Cable length is detected as following range: <50m, 50~80, 80~100, >100m. Deviation is +/-5 meters, therefore "No Cable" may be displayed under "Test Result," when the cable used is less than 5 m in length. The Fault Distance will show "No Cable", whether the fiber is connected to the port or not.
Parameters	<i><portlist 1-10></i> – A port or range of ports to be configured. <i>all</i> – Specifies all ports on the Switch are to be configured.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To determine the copper cables and position of port 3 on the Switch:

```
DGS-1100-10/ME:5>cable diagnostic port 3
Command: cable diagnostic port 3

Perform Cable Diagnostics ...

Port Type  Link Status  Test Result  Fault Distance (meters)  Length(M)
----  ----  -----  -----  -----
3      GE      Link Down  Pair1:N/A   Pair1:No Cable           N/A
                               Pair2:OPEN  Pair2:1
                               Pair3:N/A   Pair3:N/A
                               Pair4:N/A   Pair4:N/A

DGS-1100-10/ME:5>
```

FORWARDING DATABASE COMMANDS

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

Command	Parameter
create fdb vlan	<vlanid 1-4094> <macaddr> port <port 1-10>
create multicast_fdb	<vlanid 1-4094><macaddr>
config multicast_fdb	< vlanid 1-4094> <macaddr> [add delete] <portlist 1-10>
config fdb aging_time	<sec 10-600>
delete fdb	<vlan_name 20> <macaddr>
show multicast_fdb	{vlan <vlan_name 20> mac_address <macaddr>}
show fdb	{port <port 1-10> vlan <vlan_name 32> mac_address <macaddr> static aging_time}
config multicast port_filtering_mode	[all <portlist 1-10>] [forward_unregistered_groups filter_unregistered_groups]
show multicast port_filtering_mode	

Each command is listed in detail, as follows:

create fdb vlan	
Purpose	To create a static entry in the unicast MAC address forwarding table (database)
Syntax	create fdb vlan <vlanid 1-4094> <macaddr> port <port 1-10>
Description	The create fdb command creates a static entry in the Switch's unicast MAC address forwarding database.
Parameters	<p><i><vlanid 1-4094></i> – The VLAN ID on which the MAC address resides.</p> <p><i><macaddr></i> – The MAC address to be added to the forwarding table.</p> <p><i>port <port 1-10></i> – The port number corresponding to the MAC destination address. The Switch will always forward traffic to the specified device through this port.</p>
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To create a unicast MAC FDB entry:

```
DGS-1100-10/ME:5> create fdb vlan 1 00-00-00-00-01-02 port 2
Command: create fdb vlan 1 00-00-00-00-01-02 port 2

Success!
```

```
DGS-1100-10/ME:5>
```

create multicast_fdb

Purpose	To create a static entry in the multicast MAC address forwarding table (database).
Syntax	create multicast_fdb <vlanid 1-4094><macaddr>
Description	The create multicast_fdb command creates a static entry in the multicast MAC address forwarding table (database).
Parameters	<vlanid 1-4094> – The item of the VLAN on which the MAC address resides. The range is between 1 and 4094. <macaddr> – The MAC address to be added to the forwarding table.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To create multicast MAC forwarding:

```
DGS-1100-10/ME:5>create multicast_fdb 1 00-00-00-01-02-03
Command: create multicast_fdb 1 00-00-00-01-02-03

Success!
DGS-1100-10/ME:5>
```

config multicast_fdb

Purpose	To configure the Switch's multicast MAC address forwarding database.
Syntax	config multicast_fdb <vlanid 1-4094> <macaddr> [add delete] <portlist 1-10>
Description	The config multicast_fdb command configures the multicast MAC address forwarding table.
Parameters	<vlanid 1-4094> – The item of the VLAN on which the MAC address resides. The range is between 1 and 4094. <macaddr> – The MAC address to be configured to the forwarding table. <i>add</i> – Specifies that the MAC address is to be added to the forwarding table. <i>delete</i> – Specifies that the MAC address is to be removed from the forwarding table. <portlist 1-10> – A port or range of ports to be configured.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure multicast MAC forwarding:

```
DGS-1100-10/ME:5>config multicast_fdb 1 00-00-00-01-02-03
Command: config multicast_fdb 1 00-00-00-01-02-03
```

```

Success!
DGS-1100-10/ME:5>

```

config fdb aging_time

Purpose	To set the aging time of the forwarding database.
Syntax	config fdb aging_time <sec 10-600>
Description	The config fdb aging_time command sets the aging time of the forwarding database. The aging time affects the learning process of the switch. Dynamic forwarding table entries, which are made up of the source MAC addresses and their associated port numbers, are deleted from the table if they are not accessed within the aging time. The aging time can be from 0 to 630 minutes with a default value of 5 minutes. A very long aging time can result in dynamic forwarding table entries that are out-of-date or no longer exist. This may cause incorrect packet forwarding decisions by the switch. If the aging time is too short however, many entries may be aged out too soon. This will result in a high percentage of received packets whose source addresses cannot be found in the forwarding table, in which case the switch will broadcast the packet to all ports, negating many of the benefits of having a switch.
Parameters	<sec 10-600> – The aging time for the MAC address forwarding database value, in seconds.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To set the fdb aging time:

```

DGS-1100-10/ME:5>config fdb aging_time 300
Command: config fdb aging_time 300

Success!
DGS-1100-10/ME:5>

```

delete fdb

Purpose	To delete an entry in the Switch's forwarding database.
Syntax	delete fdb <vlan_name 20> <macaddr>
Description	The delete fdb command deletes an entry in the Switch's MAC address forwarding database.
Parameters	<vlan_name 20> – The name of the VLAN on which the MAC address resides. <macaddr> – The MAC address to be removed from the forwarding table.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To delete a permanent FDB entry:

```
DGS-1100-10/ME:5>delete fdb default 00-00-00-00-01-02
Command: delete fdb default 00-00-00-00-01-02

Success!
DGS-1100-10/ME:5>
```

show multicast_fdb

Purpose	To display the contents of the Switch's multicast forwarding database.
Syntax	show multicast_fdb {vlan <vlan_name 20> mac_address <macaddr>}
Description	The show multicast_fdb command displays the current contents of the Switch's multicast MAC address forwarding database.
Parameters	<i>vlan <vlan_name 20></i> – The name of the VLAN on which the MAC address resides. <i>mac_address <macaddr></i> – The MAC address that will be added to the forwarding table.
Restrictions	None.

Example usage:

To display multicast MAC address table:

```
DGS-1100-10/ME:5> show multicast_fdb
Command: show multicast_fdb

Total Entries: 0

DGS-1100-10/ME:5>
```

show fdb

Purpose	To display the current unicast MAC address forwarding database.
Syntax	show fdb {port <port 1-10> vlan <vlan_name 32> mac_address <macaddr> static aging_time}
Description	The show fdb command displays the current contents of the switch's forwarding database.
Parameters	<i><port 1-10></i> – The port number corresponding to the MAC destination address. The Switch always forwards traffic to the specified device through this port. <i><vlan_name 32></i> – The name of the VLAN on which the MAC address resides. <i><macaddr></i> – The MAC address entry in the forwarding table. <i>static</i> – Specifies that static MAC address entries are to be

	displayed.
	<i>aging_time</i> - Displays the aging time for the MAC address forwarding database.
Restrictions	None.

Example usage:

To display unicast MAC address table:

```
DGS-1100-10/ME:5>show fdb port 3
Command: show fdb port 3

VID VLAN Name          MAC Address      Port Type
-----
1  default              00-00-01-01-02-03 3  Permanent

Total Entries : 1
DGS-1100-10/ME:5>
```

To display the aging time:

```
DGS-1100-10/ME:5>show fdb aging_time
Command: show fdb aging_time

Unicast MAC Address Aging Time = 300 sec

DGS-1100-10/ME:5>
```

config multicast port_filtering_mode

Purpose	To configure multicast filtering.
Syntax	config multicast port_filtering_mode [all <portlist 1-10>] [forward_unregistered_groups filter_unregistered_groups]
Description	The config multicast port_filtering_mode command enables filtering of multicast addresses.
Parameters	<i>[all <portlist 1-10>]</i> - A port or range of ports to be configured. <i>forward_unregistered_groups</i> - Forwards unregistered multicast packets. <i>filter_unregistered_groups</i> - Filter unregistered multicast packets.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure multicast filtering

```
DGS-1100-10/ME:5> config multicast port_filtering_mode 2
filter_unregistered_groups
```

```

Command: config multicast port_filtering_mode 2
filter_unregistered_groups

```

```

Success!
DGS-1100-10/ME:5>

```

show multicast port_filtering_mode

Purpose	To display multicast filtering settings on the Switch.
Syntax	show multicast port_filtering_mode
Description	The show multicast port_filtering_mode command displays the multicast filtering settings.
Parameters	None.
Restrictions	None.

Example usage:

To show multicast filtering settings:

```

DGS-1100-10/ME:5> show multicast port_filtering_mode
Command: show multicast port_filtering_mode

```

```

Multicast Filter Mode For Unregistered Group:

```

```

Forwarding List: 1,3-10

```

```

Filtering List: 2

```

```

DGS-1100-10/ME:5>

```

BROADCAST STORM CONTROL COMMANDS

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

Command	Parameter
config traffic control	[<portlist 1-10> all] {[action [drop shutdown] broadcast multicast unknow_unicast threshold <value 64-1024000> [enable disable]}
show traffic control	{<portlist 1-10>}
config traffic_control trap	[storm_cleared storm_occured both none]

Each command is listed in detail, as follows:

config traffic control	
Purpose	To configure broadcast / multicast / unknown unicast traffic control.
Syntax	config traffic control [<portlist 1-10> all] {[action [drop shutdown] broadcast multicast unknow_unicast threshold <value 64-1024000> [enable disable]}
Description	The config traffic control command configures broadcast, multicast and unknown unicast storm control.
Parameters	<p><i><portlist 1-10></i> - A port or range of ports to be configured.</p> <p><i>all</i> - Specifies all ports on the Switch are to be configured.</p> <p><i>action [drop shutdown]</i> - Specifies the traffic control action to be drop or shutdown. A traffic control trap is active only when the control action is configured as "shutdown". If the control action is "drop", there will no traps issue while storm event is detected.</p> <p><i>storm_type</i> - The type of broadcast storm for which to configure the traffic control. The options are:</p> <ul style="list-style-type: none"> • <i>broadcast</i> - Enables broadcast storm control only. • <i>multicast</i> - Enables broadcast and multicast storm control. • <i>unknow_unicast</i> - Enables broadcast and unicast storm control. <p><i>threshold <value 64-1024000></i> - The upper threshold at which the specified traffic control is switched on. The value is the number of broadcast/multicast/dlf packets, in Kbps, received by the Switch that will trigger the storm traffic control measures. The value ranges in size from 64 to 1024000 Kbps. The default setting is 64 Kbit/sec.</p> <p><i>[enable disable]</i> - Enables or disables the specified storm type.</p>
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

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

```
DGS-1100-10/ME:5> config traffic control all multicast enable unknow_unicast
```

```

disable
Command: config traffic control all multicast enable unknow_unicast disable

Success!
DGS-1100-10/ME:5>
    
```

show traffic control

Purpose	To display current traffic control settings.
Syntax	show traffic control {<portlist 1-10>}
Description	The show traffic control command displays the current storm traffic control configuration on the Switch.
Parameters	<portlist 1-10> - A port or range of ports whose settings are to be displayed.
Restrictions	None.

Example usage:

To display traffic control setting:

```

DGS-1100-10/ME:5> show traffic control 1-3
Command: show traffic control 1-3

Traffic Storm Control Trap :[None]

Port Thres Broadcast Multicast Unicast Action Count Time Port
hold Storm Storm Storm Down Interval Status
-----
1 0 Disabled Enabled Disabled drop 0 0 Normal
2 0 Disabled Enabled Disabled drop 0 0 Normal
3 0 Disabled Enabled Disabled drop 0 0 Normal
DGS-1100-10/ME:5>
    
```

config traffic_control trap

Purpose	To configure the traffic control trap on the Switch.
Syntax	config traffic_control trap [storm_cleared storm_occured both none]
Description	The config traffic_control trap command configures the current storm traffic trap configuration on the Switch.
Parameters	<p><i>storm_cleared</i> – A notification will be generated when a storm event is cleared.</p> <p><i>storm_occured</i> – A notification will be generated when a storm event is detected.</p> <p><i>both</i> – A notification will be generated both when a storm event is detected and cleared.</p> <p><i>none</i> – No notification will be generated when storm event is detected or cleared.</p>

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

Example usage:

To configure traffic trap setting:

```
DGS-1100-10/ME:5> config traffic_control trap storm_cleared
Command: config traffic_control trap storm_cleared

Success!
DGS-1100-10/ME:5>
```

QOS COMMANDS

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

Command	Parameter
config bandwidth_control	[<portlist 1-10> all] {rx_rate [no_limit <value 16-1000000>] tx_rate [no_limit <value 16-1000000>]}
show bandwidth_control	{[<portlist 1-10> all]}
config qos mode	[802.1p dscp portbased]
show qos mode	
config scheduling_mechanism	[strict wrr]
show scheduling_mechanism	
config dscp_mapping	dscp_value <value_list 0-63> queue <value 0-7>
show dscp_mapping	{dscp_value <value_list 0-63>}

Each command is listed in detail, as follows:

config bandwidth_control	
Purpose	To configure bandwidth control on the Switch.
Syntax	config bandwidth_control [<portlist 1-10> all] {rx_rate [no_limit <value 16-1000000>] tx_rate [no_limit <value 16-1000000>]}
Description	The config bandwidth_control command defines bandwidth control.
Parameters	<p><portlist 1-10> - A port or range of ports to be configured.</p> <p>all - Specifies that the config bandwidth_control command applies to all ports on the Switch.</p> <p>rx_rate - Enables ingress rate limiting</p> <ul style="list-style-type: none"> no_limit – Indicates no limit is defined. <value 16–1000000> – Indicates a range between 16-1000000 kbps. <p>tx_rate – Enables egress rate limiting.</p> <ul style="list-style-type: none"> no_limit – Indicates no limit is defined. <value 16–1000000> – Indicates a range between 16-1000000 kbps.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure bandwidth control configuration:

```
DGS-1100-10/ME:5>config bandwidth_control all rx_rate no_limit tx_rate
no_limit
Command: config bandwidth_control all rx_rate no_limit tx_rate no_limit

Success!
DGS-1100-10/ME:5>
```

show bandwidth_control

Purpose	To display bandwidth control settings on the Switch.
Syntax	show bandwidth control [{<portlist 1-10> all}]
Description	The show bandwidth_control command displays bandwidth control.
Parameters	<portlist 1-10> – A port or range of ports to be configured. all – Specifies that the show bandwidth_control command applies to all ports on the Switch.
Restrictions	None.

Example usage:

To display the bandwidth control configuration:

```
DGS-1100-10/ME:5> show bandwidth_control
Command: show bandwidth_control
```

Port	Tx Rate	Rx Rate	Tx Effective Rate	Rx Effective Rate
1	no limit	no limit	no limit	no limit
2	no limit	no limit	no limit	no limit
3	no limit	no limit	no limit	no limit
4	no limit	no limit	no limit	no limit
5	no limit	no limit	no limit	no limit
6	no limit	no limit	no limit	no limit
7	no limit	no limit	no limit	no limit
8	no limit	no limit	no limit	no limit
9	no limit	no limit	no limit	no limit
10	no limit	no limit	no limit	no limit

```
DGS-1100-10/ME:5>
```

config qos mode

Purpose	To configure the QoS mode.
Syntax	config qos mode [802.1p dscp portbased]

Description	The config qos mode command is used to configure the QoS mode on the Switch.
Parameters	<i>[802.1p dscp portbased]</i> – Specifies the QoS mode to be 802.1p, dscp or portbased.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure the QoS mode to be portbased on the Switch:

```
DGS-1100-10/ME:5> config qos mode portbased
Command: config qos mode portbased

Success!
DGS-1100-10/ME:5>
```

show qos mode

Purpose	To display the QoS mode.
Syntax	show qos mode
Description	The show qos mode command is used to display the QoS mode on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display the QoS mode on the Switch:

```
DGS-1100-10/ME:5> show qos mode
Command: show qos mode

Qos mode : portbased
DGS-1100-10/ME:5>
```

config scheduling_mechanism

Purpose	To configure the scheduling mechanism for the QoS function.
Syntax	config scheduling_mechanism [strict wrr]
Description	<p>The config scheduling_mechanism command configures the scheduling mechanism for the QoS function. It allows the user to select between a round robin (WRR) and a strict mechanism for emptying the priority classes of service of the QoS function. The Switch contains four hardware priority classes of service. Incoming packets must be mapped to one of these four hardware priority classes of service, or queues. This command is used to specify the rotation by which these four hardware priority queues are emptied.</p> <p>The Switch's default is to empty the four hardware priority queues in order – from the highest priority hardware queue (class 3) to the lowest priority hardware queue (class 0). Each queue will transmit all</p>

	of the packets in its buffer before allowing the next lower priority queue to transmit its packets. A lower priority hardware queue will be pre-empted from emptying its queue if a packet is received on a higher priority hardware queue. The packet received on the higher priority hardware queue transmits its packet before allowing the lower priority hardware queue to resume clearing its queue.
Parameters	<p><i>strict</i> – Specifies that the highest class of service is the first to be processed. That is, the highest class of service should finish emptying before the others begin.</p> <p><i>wrr</i> – Specifies that the priority classes of service are to empty packets in a weighted roundrobin (WRR) order.</p>
Restrictions	Only administrator or operator level users can issue this command.

Example usage:

To configure the traffic scheduling mechanism for each COS queue:

```
DGS-1100-10/ME:5>config scheduling_mechanism strict
Command: config scheduling_mechanism strict

Success!
DGS-1100-10/ME:5>
```

show scheduling_mechanism

Purpose	To display the current traffic scheduling mechanisms in use on the Switch.
Syntax	show scheduling_mechanism
Description	The show scheduling_mechanism command displays the current traffic scheduling mechanisms in use on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To show the scheduling mechanism:

```
DGS-1100-10/ME:5> show scheduling_mechanism
Command: show scheduling_mechanism

Queue Mechanism      : strict
DGS-1100-10/ME:5>
```

config dscp_mapping

Purpose	To enable setting the DSCP User Priority
Syntax	config dscp_mapping dscp_value <value_list 0-63> queue <value 0-7>
Description	The config dscp_mapping command enables mapping the DSCP value (the priority) to a specific queue (the class_id).

Parameters	<i><value_list 0-63></i> –The selected value of priority. The value may be between 0 and 63. <i>queue <value 0-7></i> – Specifies the priority to be mapped.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure the DSCP mapping with value 10 and priority high:

```
DGS-1100-10/ME:5> config dscp_mapping dscp_value 10 queue 0
Command: config dscp_mapping dscp_value 10 queue 0

Success!
DGS-1100-10/ME:5>
```

show dscp_mapping	
Purpose	To display the setting of DSCP mapping.
Syntax	show dscp_mapping {dscp_value <value_list 0-63>}
Description	The show dscp_mapping command displays the mapping of DSCP value.
Parameters	<i>dscp_value <value_list 0-63></i> - The selected value of priority will be displayed. The value may be between 0 and 63.
Restrictions	None.

Example usage:

To display the DSCP mapping with value 10:

```
DGS-1100-10/ME:5> show dscp_mapping dscp_value 10
Command: show dscp_mapping dscp_value 10

DSCP Priority
-----
10      0
DGS-1100-10/ME:5>
```

RMON COMMANDS

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

Command	Parameter
enable rmon	
disable rmon	
create rmon alarm	<alarm_index 1-65535> <OID_variable 255> <interval 1-2147482647> [absolute delta] rising-threshold <value 0-2147483647> <rising_event_index 1-65535> falling-threshold <value 0-2147483647> <falling_event_index 1-65535> {[owner <owner_string 32>]}
delete rmon alarm	<alarm_index 1-65535>
create rmon collection stats	<stats_index 1-65535> port <ifindex> owner <owner_string 32>
delete rmon collection stats	<stats_index 1-65535>
create rmon collection history	<hist_index 1-65535> port <ifindex> {buckets <buckets_req 1-50> interval <interval 1-3600> owner <owner_string 32>}
delete rmon collection history	<hist_index 1-65535>
create rmon event	<event_index 1-65535> description <desc_string 128> {[log owner <owner_string 32> trap <community_string 32>]}
delete rmon event	<event_index 1-65535>
show rmon	{statistics <stats_index 1-65535> alarms events history <hist_index 1-65535> overview}

Each command is listed in detail, as follows:

enable rmon	
Purpose	To enable remote monitoring (RMON) status for the SNMP function.
Syntax	enable rmon
Description	The enable rmon command enables remote monitoring (RMON) status for the SNMP function on the Switch.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To enable the RMON feature on the Switch:

```
DGS-1100-10/ME:5>enable rmon
```

```
Command: enable rmon
```

```
Success!
DGS-1100-10/ME:5>
```

disable rmon

Purpose	To disable remote monitoring (RMON) status for the SNMP function.
Syntax	disable rmon
Description	The disable rmon command disables remote monitoring (RMON) status for the SNMP function on the Switch.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To disable the RMON feature on the Switch:

```
DGS-1100-10/ME:5>disable rmon
Command: disable rmon

Success!
DGS-1100-10/ME:5>
```

create rmon alarm

Purpose	To allow the user to configure the network alarms. Network alarms occur when a network problem, or event, is detected.
Syntax	create rmon alarm <alarm_index 1-65535> <OID_variable 255> <interval 1-2147482647> [absolute delta] rising-threshold <value 0-2147483647> <rising_event_index 1-65535> falling-threshold <value 0-2147483647> <falling_event_index 1-65535> {[owner <owner_string 32>]}
Description	The create rmon alarm command allows the user to configure the network alarms. Network alarms occur when a network problem, or event, is detected.
Parameters	<p><alarm_index> – Specifies the alarm number.</p> <p><OID_variable 255> – Specifies the MIB variable value.</p> <p><interval 1-2147482647> – Specifies the alarm interval time in seconds.</p> <p>[absolute delta] – Specifies the sampling method for the selected variable and comparing the value against the thresholds. The possible values are absolute and delta:</p> <ul style="list-style-type: none"> <i>absolute</i> –Compares the values directly with the thresholds at the end of the sampling interval. <i>delta</i> –Subtracts the last sampled value from the current value. The difference in the values is compared to the threshold. <p>rising-threshold <value 0-2147483647> – Specifies the rising counter value that triggers the rising threshold alarm.</p>

<rising_event_index 1-65535> – Specifies the event that triggers the specific alarm.

falling-threshold <value 0-2147483647> – Specifies the falling counter value that triggers the falling threshold alarm.

<falling_event_index 1-65535> – Specifies the event that triggers the specific alarm. The possible field values are user defined RMON events.

owner <owner_string 32> – Specifies the device or user that defined the alarm.

Restrictions

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

Example usage:

To create a RMON alarm on the Switch:

```
DGS-1100-10/ME:5>create rmon alarm 20 1 absolute rising-threshold
200 2falling-threshold 100 1 owner dlink
```

```
Command: create rmon alarm 20 1 absolute rising-threshold 200
2falling-threshold 100 1 owner dlink
```

Success!

```
DGS-1100-10/ME:5>
```

delete rmon alarm

Purpose	To remove the network alarms.
Syntax	delete rmon alarm <alarm_index 1-65535>
Description	The delete rmon alarm command removes the network alarms.
Parameters	<i><alarm_index 1-65535></i> – Specifies the alarm number to be removed.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To delete a RMON alarm on the Switch:

```
DGS-1100-10/ME:5>delete rmon alarm 100
```

```
Command: delete rmon alarm 100
```

Success!

```
DGS-1100-10/ME:5>
```

create rmon collection stats

Purpose	To allow users to configure the rmon stats settings on the Switch.
Syntax	create rmon collection stats <stats_index 1-65535> port <ifindex> owner <owner_string 32>
Description	The create rmon collection stats command allows users to configure the rmon stats settings on the Switch.

Parameters	<p><i><stats_index 1-65535></i> – Specifies the stats number.</p> <p><i>port <ifindex></i> – Specifies the port from which the RMON information was taken.</p> <p><i>owner <owner_string 32></i> – Specifies the device or user that defined the stats.</p>
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To create a RMON collection stats on the Switch:

```
DGS-1100-10/ME:5> create rmon collection stats 100 port 1 owner dlink
Command: create rmon collection stats 100 port 1 owner dlink

Success!
DGS-1100-10/ME:5>
```

delete rmon collection stats

Purpose	To remove the network collection stats.
Syntax	delete rmon collection stats <stats_index 1-65535>
Description	The delete rmon collection stats command removes the network collection stats on the Switch.
Parameters	<i><stats_index 1-65535></i> – Specifies the stats number to be removed.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To delete a RMON collection stats on the Switch:

```
DGS-1100-10/ME:5>delete rmon collection stats 2
Command: delete rmon collection stats 2

Success!
DGS-1100-10/ME:5>
```

create rmon collection history

Purpose	To allow the user to configure the rmon history settings on the Switch.
Syntax	create rmon collection history <hist_index 1-65535> port <ifindex> {buckets <buckets_req 1-50> interval <interval 1-3600> owner <owner_string 32>}
Description	The create rmon collection history command allows user to configure the rmon history settings on the Switch.
Parameters	<p><i><hist_index 1-65535></i> – Indicates the history control entry number.</p> <p><i>port <ifindex></i> – Specifies the port from which the RMON information was taken.</p> <p><i>buckets <buckets_req 1-50></i> – Specifies the number of buckets that</p>

	the device saves. <i>interval</i> < <i>interval 1-3600</i> > – Specifies in seconds the time period that samplings are taken from the ports. The field range is <i>1-3600</i> . The default is <i>1800</i> seconds (equal to 30 minutes). <i>owner</i> < <i>owner_string 127</i> > – Specifies the RMON station or user that requested the RMON information.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To create a RMON collection history on the Switch:

```
DGS-1100-10/ME:5> create rmon collection history 120 port 1 buckets 10
Command: create rmon collection history 120 port 1 buckets 10

Success!
DGS-1100-10/ME:5>
```

delete rmon collection history

Purpose	To remove the network collection history.
Syntax	delete rmon collection history <hist_index 1-65535>
Description	The delete rmon collection history command removes the network collection history on the Switch.
Parameters	< <i>hist_index 1-65535</i> > – Specifies the alarm history number to be removed.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To delete a RMON collection history on the Switch:

```
DGS-1100-10/ME:5>delete rmon collection history 2
Command: delete rmon collection history 2

Success!
DGS-1100-10/ME:5>
```

create rmon event

Purpose	To enable the user to configure the settings of a rmon event on the Switch.
Syntax	create rmon event <event_index 1-65535> description <desc_string 128> [[log owner <owner_string 32> trap <community_string 32>]]
Description	The create rmon event command enables users to configure the settings of a rmon event on the Switch.
Parameters	< <i>event_index 1-65535</i> > – Specifies the event number. <i>description</i> < <i>desc_string 128</i> > – Specifies the user-defined event description.

	<p><i>log</i> – Indicates that the event is a log entry.</p> <p><i>owner</i> <<i>owner_string</i> 32> – Specifies the time that the event occurred.</p> <p><i>trap</i> <<i>community_string</i> 32> – Specifies the community to which the event belongs.</p>
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To create a RMON collection history on the Switch:

```
DGS-1100-10/ME:5>create rmon event 125 description linkrmon owner
dlink
Command: create rmon event 125 description linkrmon owner dlink

Success!
DGS-1100-10/ME:5>
```

delete rmon event

Purpose	To remove the network event.
Syntax	delete rmon event <event_index 1-65535>
Description	The delete rmon event command removes the network event on the Switch.
Parameters	< <i>event_index</i> 1-65535> – Specifies the event number to be removed.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To delete a RMON event on the Switch:

```
DGS-1100-10/ME:5>delete rmon event 2
Command: delete rmon event 2

Success!
DGS-1100-10/ME:5>
```

show rmon

Purpose	To display remote monitoring (RMON) status for the SNMP function.
Syntax	show rmon {statistics <stats_index 1-65535> alarms events history <hist_index 1-65535> overview}
Description	The show rmon command displays remote monitoring (RMON) status for the SNMP function on the Switch.
Parameters	<p><i>statistics</i> <<i>stats_index</i> 1-65535> – Specify the index of RMON statistics to be displayed.</p> <p><i>alarms</i> – Specify the RMON alarm to be displayed.</p> <p><i>events</i> – Specify the RMON events to be displayed.</p> <p><i>history</i> <<i>hist_index</i> 1-65535> – Specify the RMON history to be displayed.</p>

	<i>overview</i> – Display the RMON overview.
Restrictions	None.

Example usage:

To display the RMON feature on the Switch:

```
DGS-1100-10/ME:5> show rmon statistics 100 alarms
events
Command: show rmon statistics 100 alarms events

RMON is Enabled
Collection 100 on 1 is active, and owned by dlink,
Monitors ifEntry.1.1 which has
Received 0 octets, 0 packets,
0 broadcast and 0 multicast packets,
0 undersized and 0 oversized packets,
0 fragments and 0 jabbers,
0 CRC alignment errors and 0 collisions.
# of packets received of length (in octets):
64: 0, 65-127: 0, 128-255: 0,
256-511: 0, 512-1023: 0, 1024-1518: 0
Alarm table is empty
Event table is empty

DGS-1100-10/ME:5>
```

PORT MIRRORING COMMANDS

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

Command	Parameter
enable mirror	
disable mirror	
create mirror id	<int 1-4> target <int 1-10> add source ports [rx tx both] <portlist 1-10>
config mirror	id <int 1-4> target <short 1-10> [add delete] source ports <portlist 1-10> [both rx tx]
show mirror	{id <int 1-4>}

Each command is listed in detail, as follows:

enable mirror

Purpose	Used to enable a previously entered port mirroring configuration.
Syntax	enable mirror
Description	The enable mirror command, combined with the disable mirror command below, allows the user to enter a port mirroring configuration into the Switch, as well as turn port mirroring on and off without having to modify the port mirroring configuration.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To enable the mirroring feature:

```
DGS-1100-10/ME:5>enable mirror
Command: enable mirror

Success!
DGS-1100-10/ME:5>
```

disable mirror

Purpose	Used to disable a previously entered port mirroring configuration.
Syntax	disable mirror
Description	The disable mirror command, combined with the enable mirror command above, allows the user to enter a port mirroring configuration into the switch, and then turn the port mirroring on and off without having to modify the port mirroring configuration.

Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To disable mirroring configurations:

```
DGS-1100-10/ME:5>disable mirror
Command: disable mirror

Success!
DGS-1100-10/ME:5>
```

create mirror id

Purpose	Used to create a port mirroring ID.
Syntax	create mirror id <int 1-4> target <int 1-10> add source ports [rx tx both] <portlist 1-10>
Description	The create mirror id command allows a port to have all of its traffic also sent to a designated port, where a network sniffer or other device can monitor the network traffic. In addition, one can specify that only traffic received by or sent by one or both is mirrored to the target port.
Parameters	<i>id <int 1-4></i> – Specifies the mirror ID to be created. <i>target <int 1-10></i> – Specifies the target of mirror ID. <i>[rx tx both]</i> – Allows mirroring of packets received, sent or both by the source port. <i><portlist 1-10></i> – Specifies the port or ports being mirrored. This cannot include the target port.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To create the mirroring ID:

```
DGS-1100-10/ME:5> create mirror id 1 target 1 add source ports both 2-4
Command: create mirror id 1 target 1 add source ports both 2-4

Success!
DGS-1100-10/ME:5>
```

config mirror

Purpose	To configure a mirror port – source port pair on the Switch.
Syntax	config mirror id <int 1-4> target <short 1-10> [add delete] source ports <portlist 1-10> [both rx tx]
Description	The config mirror target command allows a port to have all of its traffic also sent to another designated port, where a network sniffer or other device can monitor the network traffic. In addition, one can specify that only traffic received by or sent by one or both is mirrored

	to the target port.
Parameters	<p><i>id</i> <int 1-4> – Specifies the mirror ID.</p> <p><i>target</i> <short 1-10> – Specifies the port that mirrors traffic forwarding.</p> <p><i>[add delete]</i> – Specifies to add or delete the target port.</p> <p><i>source ports</i> <portlist 1-10> – Specifies the port or ports being mirrored. This cannot include the target port.</p> <p><i>rx</i> – Allows mirroring of packets received by (flowing into) the source port.</p> <p><i>tx</i> – Allows mirroring of packets sent to (or flowing out of) the source port.</p> <p><i>both</i> – Allows mirroring of all the packets received or sent by the source port.</p> <p><i>Comment:</i> The user can define up to 8 source ports and one destination port. One source port can be configured each time using one CLI command, so in order to configure multiple source ports, multiple CLI commands should be used.</p>
Restrictions	A target port cannot be listed as a source port. Only Administrator or operator-level users can issue this command.

Example usage:

To add the mirroring ports:

```
DGS-1100-10/ME:5>config mirror target 4 add source ports 1-3 both
Command: config mirror target 4 add source ports 1-3 both

Success!
DGS-1100-10/ME:5>
```

show mirror	
Purpose	To show the current port mirroring configuration on the Switch.
Syntax	show mirror {id <int 1-4>}
Description	The show mirror command displays the current port mirroring configuration on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display mirroring ID 1 configuration:

```
DGS-1100-10/ME:5> show mirror id 1
Command: show mirror id 1

Port Mirror is Enabled

ID  Target Port  Ingress port  Egress port  Both
---  -----  -----  -----  -----
```

1	1	2-4	2-5	2-4
DGS-1100-10/ME:5>				

VLAN COMMANDS

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

Command	Parameter
create vlan	<vlan_name 20> tag <vlanid 2-4094>
delete vlan	[<vlan_name 20> vlanid <vidlist 2-4094>]
config vlan	[<vlan_name 20> vlanid <int 1-4094>] [[add [tagged untagged] delete] <portlist 1-10>]
show vlan	{<vlan_name 20> vlanid <vidlist 1-4094> ports <portlist 1-10>}
enable asymmetric_vlan	
disable asymmetric_vlan	
show asymmetric_vlan	
enable management_vlan	
disable management_vlan	
config management_vlan	vlanid <vlanid 1-4094>
show management_vlan	
show port_vlan pvid	

Each command is listed in detail, as follows:

create vlan	
Purpose	To create a VLAN on the Switch.
Syntax	create vlan <vlan_name 20> tag <vlanid 2-4094>
Description	The create vlan command creates a VLAN on the Switch.
Parameters	<i><vlan_name 20></i> – The name of the VLAN to be created. <i>tag <vlanid 2-4094></i> – The VLAN ID of the VLAN to be created. The allowed values range from 2 to 4094.
Restrictions	Each VLAN name can be up to 32 characters. If the VLAN is not given a tag, it will be a port-based VLAN. Only administrator or operator-level users can issue this command.

Example usage:

To create a VLAN v1 tag 3:

```
DGS-1100-10/ME:5>create vlan v1 tag 3
Command: create vlan v1 tag 3

Success!
DGS-1100-10/ME:5>
```

delete vlan

Purpose	To delete a previously configured VLAN on the Switch.
Syntax	delete vlan [<vlan_name 20> vlanid <vidlist 2-4094>]
Description	The delete vlan command deletes a previously configured VLAN on the Switch.
Parameters	<i><vlan_name 20></i> – The name of the VLAN to be deleted. <i>vlanid <vidlist 2-4092></i> – The VLAN of the VLAN to be deleted.
Restrictions	Only administrator or operator-level users can issue this command. A user is required to disable Guest VLAN before deleting a VLAN.

Example usage:

To remove a vlan where VLAN ID is 2:

```
DGS-1100-10/ME:5>delete vlan vlanid 2
Command: delete vlan vlanid 2

Success!
DGS-1100-10/ME:5>
```

config vlan

Purpose	To add additional ports to a previously configured VLAN and to modify a VLAN name.
Syntax	config vlan [<vlan_name 20> vlanid <int 1-4094>] [[add [tagged untagged] delete] <portlist 1-10>
Description	The config vlan command allows the user to add or delete ports to the port list of a previously configured VLAN. You can specify the additional ports as tagging, untagging, or forbidden. The default is to assign the ports as untagged.
Parameters	<i><vlan_name 20></i> – The name of the VLAN to be configured. <i>vlanid <int 1-4094 ></i> – The ID of the VLAN to which to add ports. <i>add</i> – Specifies that ports are to be added to a previously created vlan. <i>delete</i> - Specifies that ports are to be deleted from a previously created vlan. <i>tagged</i> – Specifies the additional ports as tagged. <i>untagged</i> – Specifies the additional ports as untagged. <i><portlist 1-10></i> – A port or range of ports to be added to or deleted

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

Example usage:

To add ports 1-3 as tagged ports to the VLAN ID 1:

```
DGS-1100-10/ME:5> config vlan vlanid 1 add tagged 1-3
Command: config vlan vlanid 1 add tagged 1-3
```

```
Success!
DGS-1100-10/ME:5>
```

show vlan

Purpose	To display the current VLAN configuration on the Switch
Syntax	show vlan {<vlan_name 20> vlanid <vidlist 1-4094> ports <portlist 1-10>}
Description	The show vlan 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	<i><vlan_name 20></i> – Specify the VLAN id to be displayed. <i>vlanid <vidlist 1-4094></i> – Specify the VLAN id to be displayed. <i>ports <portlist 1-10></i> – Specify the ports to be displayed.
Restrictions	None.

Example usage:

To display the Switch's current VLAN settings:

```
DGS-1100-10/ME:5> show vlan
Command: show vlan

VID          : 1          VLAN NAME    : default
VLAN Type    : Static
Member Ports : 1-10
Untagged Ports : 4-10

VID          : 100       VLAN NAME    : rd1
VLAN Type    : Static
Member Ports :
Untagged Ports :
```

```
DGS-1100-10/ME:5>
```

enable asymmetric_vlan

Purpose	To enable Asymmetric VLAN on the switch.
Syntax	enable asymmetric_vlan
Description	The enable asymmetric_vlan command, along with the disable asymmetric_vlan command below, is used to enable and disable Asymmetric VLAN on the Switch
Parameters	None.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To enable Asymmetric VLAN on the switch:

```
DGS-1100-10/ME:5>enable asymmetric_vlan
Command: enable asymmetric_vlan

Success!
DGS-1100-10/ME:5>
```

disable asymmetric_vlan

Purpose	To disable Asymmetric VLAN on the switch.
Syntax	disable asymmetric_vlan
Description	The disable asymmetric_vlan command, along with the enable asymmetric_vlan command below, is used to disable and enable Asymmetric VLAN on the Switch.
Parameters	None.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To disable asymmetric_vlan on the switch:

```
DGS-1100-10/ME:5>disable asymmetric_vlan
Command: disable asymmetric_vlan

Success!
DGS-1100-10/ME:5>
```

show asymmetric_vlan

Purpose	To display the Asymmetric VLAN status on the Switch.
Syntax	show asymmetric_vlan
Description	The show asymmetric_vlan command displays the Asymmetric VLAN status on the Switch.
Parameters	None.

Restrictions	None.
--------------	-------

Example usage:

To display Asymmetric VLAN status:

```
DGS-1100-10/ME:5>show asymmetric_vlan
Command: show asymmetric_vlan

Asymmetric VLAN : Enable
DGS-1100-10/ME:5>
```

enable management vlan

Purpose	To enable the management VLAN on the Switch.
Syntax	enable management vlan
Description	The enable management vlan command enables the management VLAN on the Switch.
Parameters	None.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To enable management VLAN on the switch:

```
DGS-1100-10/ME:5>enable management vlan
Command: enable management vlan

Success!
DGS-1100-10/ME:5>
```

disable management vlan

Purpose	To disable the management VLAN on the Switch.
Syntax	disable management vlan
Description	The disable management vlan command disables the management VLAN on the Switch.
Parameters	None.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To disable management VLAN on the switch:

```
DGS-1100-10/ME:5>disable management vlan
Command: disable management vlan
```

```

Success!
DGS-1100-10/ME:5>

```

config management vlan

Purpose	To configure management VLAN on the Switch.
Syntax	config management vlanid <vlanid 1-4094>
Description	The config management vlan command configures management VLAN on the Switch.
Parameters	<i>vlanid <vlanid 1-4094></i> - Specifies management VLAN ID on the Switch.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure the management VLAN on the switch:

```

DGS-1100-10/ME:5> config management vlanid 1
Command: config management vlanid 1

Success!
DGS-1100-10/ME:5>

```

show management vlan

Purpose	To display the management VLAN on the Switch.
Syntax	show management vlan
Description	The show management vlan command displays the management VLAN information on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display the management VLAN on the switch:

```

DGS-1100-10/ME:5>show management vlan
Command: show management vlan

management vlan is enable

management vlan id : 1
management vlan name: default
DGS-1100-10/ME:5>

```

show port_vlan pvid

Purpose	To display the port PVID of VLAN on the Switch.
Syntax	show port_vlan pvid
Description	The show port_vlan pvid command displays the port PVID of VLAN on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display the port PVID of VLAN on the switch:

```
DGS-1100-10/ME:5> show port_vlan pvid  
Command: show port_vlan pvid
```

Port	PVID
1	1
2	1
3	1
4	1
5	1
6	1
7	1
8	1
9	1
10	1

```
DGS-1100-10/ME:5>
```

Q-IN-Q COMMANDS

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

Command	Parameter
enable qinq	
disable qinq	
show qinq	{ports [<portlist 1-10> all]}
config qinq ports	[<portlist 1-10> all] [role [nni uni] outer_tpid <hex 0x1-0xffff>]

Each command is listed in detail, as follows:

enable qinq	
Purpose	To enable the Q-in-Q mode.
Syntax	enable qinq
Description	The enable qinq command is used to enable the Q-in-Q mode. When Q-in-Q is enabled, all network port roles will be NNI port and their outer TPID will be set to 88a8. All existing static VLANs will run as SP-VLAN. All dynamically learned L2 address will be cleared. The default setting of Q-in-Q is disabled.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To enable Q-in-Q:

```
DGS-1100-10/ME:5>enable qinq
Command: enable qinq

Success!
DGS-1100-10/ME:5>
```

disable qinq	
Purpose	To disable the Q-in-Q mode.
Syntax	disable qinq
Description	The disable qinq command is used to disable the Q-in-Q mode. All dynamically learned L2 address will be cleared. All dynamically registered VLAN entries will be cleared. All existing SP-VLANs will run as static 1Q VLANs. The default setting of Q-in-Q is disabled.

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

Example usage:

To disable Q-in-Q:

```
DGS-1100-10/ME:5>disable qinq
Command: disable qinq

Success!
DGS-1100-10/ME:5>
```

show qinq

Purpose	To show global Q-in-Q and port Q-in-Q mode status.
Syntax	show qinq {ports [<portlist 1-10> all]}
Description	The show qinq command is used to show the global Q-in-Q status, including: port role in Q-in-Q mode and port outer TPID.
Parameters	<portlist> - Specifies a range of ports to be displayed. If no parameter is specified, the system will display all Q-in-Q port information. <i>all</i> - Specifies all ports to be displayed.
Restrictions	None.

Example usage:

To show the Q-in-Q status for ports 1 to 4:

```
DGS-1100-10/ME:5> show qinq ports 1-4
Command: show qinq ports 1-4

Port Role  Outer TPID
-----
1  NNI  88a8
2  NNI  88a8
3  NNI  88a8
4  NNI  88a8

Total Entries : 4
DGS-1100-10/ME:5>
```

config qinq ports

Purpose	Used to configure Q-in-Q ports.
Syntax	config qinq ports [<portlist 1-10> all] [role [nni uni] outer_tpid <hex 0x1-0xffff>]

Description	The config qinq ports command is used to configure the port level setting for the Q-in-Q VLAN function. This setting is not effective when the Q-in-Q mode is disabled.
Parameters	<i><portlist 1-10></i> - A range of ports to configure. <i>all</i> – Specifies all ports to be configure. <i>role</i> - Port role in Q-in-Q mode, it can be UNI port or NNI port. <i>outer_tpid</i> - TPID in the SP-VLAN tag.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure all ports as UNI port, set outer TPID to 0xffff:

```
DGS-1100-10/ME:5> config qinq ports all outer_tpid 0xffff role uni
Command: config qinq ports all outer_tpid 0xffff role uni
```

Warning: The outer TPID will be globally applied to all ports!

```
Success!
DGS-1100-10/ME:5>
```

BASIC IP COMMANDS

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

Command	Parameter
config ipif system	[dhcp dhcp_option12 {clear_hostname hostname <hostname 63> state [enable disable] } ipaddress [<network_address> gateway <ipaddr>] [ipv6 ipv6address <ipv6networkaddr>] [dhcpv6_client [enable disable]]]
show ipif	

Each command is listed in detail, as follows:

config ipif System	
Purpose	To configure the DHCPv6 client state for the interface.
Syntax	config ipif System [dhcp dhcp_option12 {clear_hostname hostname <hostname 63> state [enable disable] } ipaddress [<network_address> gateway <ipaddr>] [ipv6 ipv6address <ipv6networkaddr>] [dhcpv6_client [enable disable]]]
Description	The config ipif system command is used to configure the DHCPv6 client state for one interface.
Parameters	<p><i>system</i> – The IP interface name to be configured. The default IP Interface name on the Switch is ‘System’. All IP interface configurations done are executed through this interface name.</p> <p><i>dhcp</i> – Specifies the DHCP protocol for the assignment of an IP address to the Switch to use for the DHCP Protocol.</p> <p><i>hostname <hostname 63></i> – Specifies the host name of DHCP.</p> <p><i>ipaddress <network_address></i> – IP address and netmask of the IP interface to be created. The address and mask information may be specified by using the traditional format (for example, 10.1.2.3/255.0.0.0 or in CIDR format, 10.1.2.3/16).</p> <p><i>gateway <ipaddr></i> – IP address of gateway to be created.</p> <p><i>state [enable disable]</i> – Enables or disables the IP interface.</p> <p><i>ipv6 ipv6address <ipv6networkaddr></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 [enable disable]</i> – Enable or disable the DHCPv6 client state of the interface.</p>
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure the DHCPv6 client state of the System interface to enabled:

```
DGS-1100-10/ME:5>config ipif System dhcpv6_client enable
Command: config ipif System dhcpv6_client enable
```

```
Success!
DGS-1100-10/ME:5>
```

show ipif

Purpose	To display the configuration of an IP interface on the Switch.
Syntax	show ipif
Description	The show ipif command displays the configuration of an IP interface on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display IP interface settings:

```
DGS-1100-10/ME:5> show ipif
Command: show ipif

IP Setting Mode           : Static
IP Address                : 10.90.90.90
IP Subnet Mask            : 255.0.0.0
IP Default Gateway       : 0.0.0.0
Interface Admin State    : Enabled
DHCPv6 Client State      : Disabled
IPv6 Link-Local Address  :
IPv6 Global Unicast Address :
DHCP Option12 State      : Disabled
DHCP Option12 Host Name  : DGS-1100-10/ME
IPv4 State                : Enabled
IPv6 State                : Enabled
DGS-1100-10/ME:5>
```

MAC NOTIFICATION COMMANDS

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

Command	Parameter
enable mac_notification	
disable mac_notification	
config mac_notification	[interval <int 1-2147483647> historysize <int 1-500>]
config mac_notification ports	[<portlist 1-10> all] [enable disable]
show mac_notification	
show mac_notification ports	<portlist 1-10>

Each command is listed in detail, as follows:

enable mac_notification

Purpose	Used to enable global MAC address table notification on the Switch.
Syntax	enable mac_notification
Description	The enable mac_notification command is used to enable MAC address notification without changing configuration.
Parameters	None.
Restrictions	Only administrator or operator-level users can issue this command

Example usage:

To enable MAC notification without changing basic configuration:

```
DGS-1100-10/ME:5>enable mac_notification
Command: enable mac_notification

Success!
DGS-1100-10/ME:5>
```

disable mac_notification

Purpose	Used to disable global MAC address table notification on the Switch.
Syntax	disable mac_notification

Description	The disable mac_notification command is used to disable MAC address notification without changing configuration.
Parameters	None.
Restrictions	Only administrator or operator-level users can issue this command

Example usage:

To disable MAC notification without changing basic configuration:

```
DGS-1100-10/ME:5>disable mac_notification
Command: disable mac_notification

Success!
DGS-1100-10/ME:5>
```

config mac_notification

Purpose	Used to configure MAC address notification.
Syntax	config mac_notification [interval <int 1-2147483647> historysize <int 1-500>]
Description	The config mac_notification command is used to monitor MAC addresses learned and entered into the FDB.
Parameters	<i>interval <int 1-2147483647></i> – The time in seconds between notifications. The user may choose an interval between 1 and 2147483647 seconds. <i>historysize <1-500></i> – The maximum number of entries listed in the history log used for notification.
Restrictions	Only administrator or operator-level users can issue this command

Example usage:

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

```
DGS-1100-10/ME:5>config mac_notification interval 1
Command: config mac_notification interval 1

Success!
DGS-1100-10/ME:5>
```

config mac_notification ports

Purpose	Used to configure MAC address notification status settings.
Syntax	config mac_notification ports [<portlist 1-10> all] [enable disable]
Description	The config mac_notification ports command is used to monitor MAC addresses learned and entered into the FDB.
Parameters	<i><portlist 1-10></i> – Specifies a port or range of ports to be configured. <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 or operator-level users can issue this command

Example usage:

To enable port 7 for MAC address table notification:

```
DGS-1100-10/ME:5>config mac_notification ports 7 enable
Command: config mac_notification ports 7 enable

Success!
DGS-1100-10/ME:5>
```

show mac_notification

Purpose	Used to display the Switch's MAC address table notification global settings.
Syntax	show mac_notification
Description	The show mac_notification 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-1100-10/ME:5>show mac_notification
Command: show mac_notification

Global Mac Notification Settings

State          : Enabled
Interval       : 1
History Size   : 1
DGS-1100-10/ME:5>
```

show mac_notification ports

Purpose	Used to display the Switch's MAC address table notification status settings.
Syntax	show mac_notification ports <portlist 1-10>
Description	The show mac_notification ports command is used to display the Switch's MAC address table notification status settings.
Parameters	<i><portlist></i> – Specify a port or group of ports to be viewed. Entering this command without the parameter will display the MAC notification table for all ports.

Restrictions	None.
--------------	-------

Example usage:

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

```
DGS-1100-10/ME:5> show mac_notification ports 1-3
```

```
Command: show mac_notification ports 1-3
```

```
Port #  MAC Address Table Notification State
```

```
-----
```

```
1      Disabled
```

```
2      Disabled
```

```
3      Disabled
```

```
DGS-1100-10/ME:5>
```

IGMP SNOOPING COMMANDS

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

Command	Parameter
enable igmp_snooping	{forward_mcrouter_only}
disable igmp_snooping	{forward_mcrouter_only}
show igmp_snooping	{vlan <vlan_name 20>}
config igmp_snooping	[vlan_name <vlan_name 20> vlanid <vidlist 1-4094> all] [fast_leave [enable disable] state [enable disable]]
config igmp_snooping querier	[vlan_name <vlan_name 20> vlanid <vidlist 1-4094> all] state [enable disable] {host_timeout <sec 130-153025> router_timeout <sec 60-600> version <value 1-3> last_member_query_interval <sec 1-25> max_response_time <sec 10-25> query_interval <sec 60-600> robustness_variable <value 2-255>}
create igmp_snooping multicast_vlan	<vlan_name 20> <vlanid 2-4094>
config igmp_snooping multicast_vlan	<vlan_name 20> [add delete] [member_port <portlist 1-10> source_port <portlist 1-10> tag_member_port <portlist 1-10>] state [enable disable] {replace_source_ip [none <ipaddr> <ipv6addr>]}
delete igmp_snooping multicast_vlan	<vlan_name 20> [ip ipv6]
config igmp_snooping multicast_vlan_group	<vlan_name 20> [ip ipv6] [add delete] [<mcast_address_range> all]
config router_ports	[vlan_name <string 20> vlanid <vidlist 1-4094> all] [add delete] <portlist 1-10>
config igmp access_authentication ports	[<portlist> all] state [enable disable]
show igmp access_authentication ports	[<portlist> all]
enable igmp_snooping multicast_vlan	
disable igmp_snooping multicast_vlan	
show igmp_snooping multicast_vlan	<vlan_name 20> [ip ipv6]
show igmp_snooping multicast_vlan_group	<vlan_name 20> [ip ipv6]
show igmp_snooping group	{vlan <vlan_name 20> vlanid <vidlist 1-4094>}

Command	Parameter
show igmp_snooping host	{group <ipaddr> ports <portlist 1-10> vlan <vlan_name 20> vlanid <vidlist 1-4094>}
show router_port	{vlan <vlan_name 20> vlanid <vidlist 1-4094> static dynamic}

Each command is listed in detail, as follows:

enable igmp_snooping

Purpose	To enable IGMP snooping on the Switch.
Syntax	enable igmp_snooping {forward_mcrouter_only}
Description	The enable igmp_snooping command enables IGMP snooping on the Switch.
Parameters	<i>{forward_mcrouter_only}</i> – Only enables the forward mcrouter for IGMP Snooping on the Switch.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To enable IGMP snooping on the Switch:

```
DGS-1100-10/ME:5> enable igmp_snooping
Command: enable igmp_snooping

Success!
DGS-1100-10/ME:5>
```

disable igmp_snooping

Purpose	To disable IGMP snooping on the Switch.
Syntax	disable igmp_snooping {forward_mcrouter_only}
Description	The disable igmp_snooping command disables IGMP snooping on the switch.
Parameters	<i>{forward_mcrouter_only}</i> – Only disables the forward mcrouter for IGMP Snooping on the switch.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To disable IGMP snooping on the Switch:

```
DGS-1100-10/ME:5> disable igmp_snooping
Command: disable igmp_snooping

Success!
DGS-1100-10/ME:5>
```

show igmp_snooping

Purpose	To display IGMP snooping on the switch.
Syntax	show igmp_snooping {vlan <vlan_name 20>}
Description	The show igmp_snooping command displays IGMP snooping on the switch.
Parameters	<i>vlan <vlan_name 20></i> – Displays the vlan for IGMP Snooping on the switch.
Restrictions	None.

Example usage:

To display IGMP snooping on the switch:

```
DGS-1100-10/ME:5> show igmp_snooping vlan default
Command: show igmp_snooping vlan default
```

```
IGMP Snooping Global State      : Enabled
Forward Router Only             : Enabled
```

```
VLAN Name                       : default
Host Timeout                    : 260
Router Timeout                  : 250
Query Interval                  : 125
Max Response Time               : 10
Robustness Value                : 2
Last Member Query Interval      : 2
Querier State                   : Disabled
State                           : Enabled
Fast Leave                      : Disabled
Version                         : 3
```

```
Total Entries: 1
```

```
DGS-1100-10/ME:5>
```

config igmp_snooping

Purpose	To configure IGMP snooping on the switch.
Syntax	config igmp_snooping [vlan_name <vlan_name 20> vlanid <vidlist 1-4094> all] [fast_leave [enable disable] state [enable disable]]
Description	The config igmp_snooping command configures IGMP snooping on the switch.
Parameters	<i>vlan_name <vlan_name 20></i> – The name of the VLAN for which IGMP snooping is to be configured.

	<p><i>vlanid</i> <vidlis 1-4094> – The VLAN ID for which IGMP snooping is to be configured.</p> <p>all – Specifies all VLAN for which IGMP snooping is to be configured.</p> <p><i>fast_leave</i> [<i>enable</i> <i>disable</i>] – Enables or disables the fast leave function.</p> <p><i>state</i> [<i>enable</i> <i>disable</i>] – Enables or disables IGMP snooping for the specified VLAN.</p>
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure the igmp snooping:

```
DGS-1100-10/ME:5> config igmp_snooping vlan_name default state
enable
Command: config igmp_snooping vlan_name default state enable

Success !
DGS-1100-10/ME:5>
```

config igmp_snooping querier

Purpose	To configure IGMP snooping querier on the Switch.
Syntax	config igmp_snooping querier [<i>vlan_name</i> < <i>vlan_name</i> 20> <i>vlanid</i> < <i>vidlist</i> 1-4094> all] <i>state</i> [<i>enable</i> <i>disable</i>] { <i>host_timeout</i> < <i>sec</i> 130-153025> <i>router_timeout</i> < <i>sec</i> 60-600> <i>version</i> < <i>value</i> 1-3> <i>last_member_query_interval</i> < <i>sec</i> 1-25> <i>max_response_time</i> < <i>sec</i> 10-25> <i>query_interval</i> < <i>sec</i> 60-600> <i>robustness_variable</i> < <i>value</i> 2-255>}
Description	The config igmp_snooping querier command enables IGMP snooping querier on a specific VLAN.
Parameters	<p><i>vlan_name</i> <<i>vlan_name</i> 20> – The name of the VLAN for which IGMP snooping is to be configured. Up to 20 characters can be used.</p> <p><i>vlanid</i> <<i>vidlist</i> 1-4094> – The VLAN id for which IGMP snooping is to be configured.</p> <p>all – Specifies all VLAN for which IGMP snooping is to be configured.</p> <p><i>state</i> [<i>enable</i> <i>disable</i>] – Enables/Disables IGMP Snooping Querier.</p> <p><i>version</i> <<i>value</i> 1-3> – Specifies the IGMP Querier version on the VLAN.</p> <p><i>host_timeout</i> <<i>sec</i> 130-153025> – Specifies the maximum amount of time a host can be a member of a multicast group without the switch receiving a host membership report. The default is 260 seconds.</p> <p><i>router_timeout</i> <<i>sec</i> 60-600> – Specifies the maximum amount of time a route can be a member of a multicast group without the switch receiving a host membership report.</p> <p><i>last_member_query_interval</i> <<i>sec</i> 1-25> – Specifies the last member query interval of IGMP. The range is from 1 to 25 seconds.</p> <p><i>max_response_time</i> <<i>sec</i> 10-25> – Specifies the max response time of IGMP. The range is from 10 to 25 seconds.</p>

	<i>query_interval</i> <sec 60-600> – Specifies the query interval of IGMP. The range is from 60 to 600 seconds.
	<i>robustness_variable</i> <value 2-255> – The IGMP snooping robustness variable of IGMP snooping is to be configured.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure the igmp snooping:

```
DGS-1100-10/ME:5> config igmp_snooping querier vlanid 2 state enable
last_member_query_interval 2
Command: config igmp_snooping querier vlanid 2 state enable
last_member_query_interval 2

Success !
DGS-1100-10/ME:5>
```

create igmp_snooping multicast_vlan

Purpose	To create an IGMP snooping multicast VLAN on the Switch.
Syntax	create igmp_snooping multicast_vlan <vlan_name 20> <vlanid 2-4094>
Description	The create igmp_snooping multicast_vlan command creates an IGMP snooping multicast VLAN on the Switch.
Parameters	<i>vlan</i> <vlan_name 20> – The name of the VLAN for which IGMP snooping is to be created. Up to 32 characters can be used. <vlanid 2-4092> – The ID of the VLAN for which IGMP snooping is to be created. The range is from 2 to 4094.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To create an igmp snooping multicast VLAN:

```
DGS-1100-10/ME:5>create igmp_snooping multicast_vlan mvln2 5
Command: create igmp_snooping multicast_vlan mvln2 5

Success!
DGS-1100-10/ME:5>
```

config igmp_snooping multicast_vlan

Purpose	To configure IGMP snooping multicast VLAN on the Switch.
Syntax	config igmp_snooping multicast_vlan <vlan_name 20> [add delete] [member_port <portlist 1-10> source_port <portlist 1-10> tag_member_port <portlist 1-10>] state [enable disable] {replace_source_ip [none <ipaddr> <ipv6addr>]}

Description	The config igmp_snooping multicast_vlan command enables IGMP snooping multicast VLAN on the Switch.
Parameters	<p><i>vlan <vlan_name 20></i> – The name of the VLAN for which IGMP snooping is to be configured. Up to 32 characters can be used.</p> <p><i>[add delete]</i> – Add or delete the specified multicast VLAN of IGMP snooping.</p> <p><i>member_port <portlist 1-10></i> – Specifies a port or a range of ports to be the member port for the multicast VLAN of IGMP snooping.</p> <p><i>source_port <portlist 1-10></i> – Specifies a port or a range of ports to be the source port for the multicast VLAN of IGMP snooping.</p> <p><i>tag_member_port <portlist 1-10></i> – Specifies a port or a range of ports to be the tagged port for the multicast VLAN of IGMP snooping.</p> <p><i>state [enable disable]</i> – Enables/Disables IGMP Snooping multicast VLAN.</p> <p><i>replace_source_ip [none <ipaddr> <ipv6addr>]</i> – Specifies the replace source IP address.</p>
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure the igmp snooping multicast VLAN:

```
DGS-1100-10/ME:5>config igmp_snooping multicast_vlan default state
enable
Command: config igmp_snooping multicast_vlan default state enable

Success!
DGS-1100-10/ME:5>
```

delete igmp_snooping multicast_vlan

Purpose	To remove an IGMP snooping multicast VLAN on the Switch.
Syntax	delete igmp_snooping multicast_vlan <vlan_name 20> [ip ipv6]
Description	The delete igmp_snooping multicast_vlan command removes IGMP snooping multicast VLAN on the Switch.
Parameters	<p><i><vlan_name 20></i> – Specify the multicast vlan name to be removed on the Switch.</p> <p><i>[ip ipv6]</i> – Specify the ip or ipv6 of multicast vlan to be removed on the Switch.</p>
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To remove the igmp snooping multicast VLAN 'rd1':

```
DGS-1100-10/ME:5>delete igmp_snooping multicast_vlan rd1
Command: delete igmp_snooping multicast_vlan rd1
```

```
Success!
DGS-1100-10/ME:5>
```

config igmp_snooping multicast_vlan_group

Purpose	To specify that IGMP snooping is to be configured for multicast vlan groups on the Switch.
Syntax	config igmp_snooping multicast_vlan_group <vlan_name 20> [ip ipv6] [add delete] [<mcast_address_range> all]
Description	The config igmp_snooping multicast_vlan_group command specifies an IGMP snooping multicast VLAN group on the Switch.
Parameters	<p><i>vlan <vlan_name 20></i> – The name of the VLAN for which IGMP snooping is to be configured. Up to 32 characters can be used.</p> <p><i>[ip ipv6]</i> – Specify the ip or ipv6 of multicast vlan group to be configured on the Switch.</p> <p><i>[add delete]</i> – Specify whether to add or delete ports defined in the following parameter <ipaddr>.</p> <p><i>[<mcast_address_range> all]</i> – Specify the address to be configured with the IGMP snooping multicast VLAN group.</p>
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure the igmp snooping multicast VLAN:

```
DGS-1100-10/ME:5> config igmp_snooping multicast_vlan_group default ip
delete all
Command: config igmp_snooping multicast_vlan_group default ip delete
all

Success!
DGS-1100-10/ME:5>
```

config router_ports

Purpose	To configure ports as router ports.
Syntax	config router_ports [vlan_name <string 20> vlanid <vidlist 1-4094> all] [add delete] <portlist 1-10>
Description	The config router_ports command designates a range of ports as being connected to multicast-enabled routers. This ensures all packets with such a router as its destination will reach the multicast-enabled router – regardless of protocol, etc.
Parameters	<p><i>vlan_name <string 20></i> – The name of the VLAN on which the router port resides. Up to 20 characters can be used.</p> <p><i>vlanid <vidlist 1-4094></i> – The VLAN id of the VLAN on which the router port resides.</p> <p><i>all</i> – Specifies all ports on the Switch to be configured.</p> <p><i>[add delete]</i> – Specifies whether to add or delete ports defined in the following parameter <portlist>, to the router port function.</p> <p><i><portlist 1-10></i> – A port or range of ports that will be configured as</p>

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

Example usage:

To add a static router port:

```
DGS-1100-10/ME:5> config router_ports vlanid 12 add 2
Command: config router_ports vlanid 12 add 2

Success!
DGS-1100-10/ME:5>
```

config igmp access_authentication ports

Purpose	To configure the IGMP access authentication on the Switch.
Syntax	config igmp access_authentication ports [<portlist 1-10> all] state [enable disable]
Description	The config igmp access_authentication ports command configures the IGMP access authentication on the Switch.
Parameters	<i><portlist 1-10></i> – A port or range of ports that will be configured as IGMP access authentication ports. <i>all</i> – Specify all ports to be configured as IGMP access authentication ports. <i>state[enable disable]</i> – Specifies the state for the port to be disabled or enabled.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure authentication port of IGMP:

```
DGS-1100-10/ME:5>config igmp access_authentication ports all state
enable
Command: config igmp access_authentication ports all state enable

Success !
DGS-1100-10/ME:5>
```

show igmp access_authentication ports

Purpose	To display the IGMP access authentication configuration on the Switch.
Syntax	show igmp access_authentication ports [<portlist 1-10> all]
Description	The show igmp access_authentication command displays the IGMP access authentication configuration on the Switch.
Parameters	<i>all</i> – Specifies all ports to be displayed. <i><portlist 1-10></i> – A port or range of ports to be displayed on the

	Switch.
Restrictions	None.

Example usage:

To display the IGMP access authentication:

```
DGS-1100-10/ME:5> show igmp access_authentication ports 1-3
Command: show igmp access_authentication ports 1-3

Port  Authentication State
-----
1      : Enabled
2      : Enabled
3      : Enabled
DGS-1100-10/ME:5>
```

enable igmp_snooping multicast_vlan

Purpose	To enable IGMP snooping multicast VLAN on the Switch.
Syntax	enable igmp_snooping multicast_vlan
Description	The enable igmp_snooping multicast_vlan command enables IGMP snooping on the Switch.
Parameters	<i>multicast_vlan</i> – Enables the multicast VLAN for IGMP Snooping on the Switch.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To enable IGMP snooping multicast VLAN on the Switch:

```
DGS-1100-10/ME:5>enable igmp_snooping multicast_vlan
Command: enable igmp_snooping multicast_vlan

Success !
DGS-1100-10/ME:5>
```

disable igmp_snooping multicast_vlan

Purpose	To disable IGMP snooping multicast VLAN on the Switch.
Syntax	disable igmp_snooping multicast_vlan
Description	The disable igmp_snooping multicast_vlan command disables IGMP snooping multicast VLAN on the Switch. IGMP snooping can be disabled only if IP multicast routing is not being used. Disabling IGMP snooping allows all IGMP and IP multicast traffic to flood within a given IP interface.
Parameters	<i>multicast_vlan</i> – Disables the multicast VLAN for IGMP Snooping on the Switch.

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

Example usage:

To disable IGMP snooping multicast VLAN on the Switch:

```
DGS-1100-10/ME:5>disable igmp_snooping multicast_vlan
Command: disable igmp_snooping multicast_vlan

Success !
DGS-1100-10/ME:5>
```

show igmp_snooping multicast_vlan

Purpose	To show the current status of IGMP snooping multicast VLAN on the Switch.
Syntax	show igmp_snooping multicast_vlan <vlan_name 20> [ip ipv6]
Description	The show igmp_snooping command displays the current IGMP snooping configuration on the Switch.
Parameters	<i><vlan_name 20></i> – The name of the VLAN for which IGMP snooping configuration is to be displayed. Up to 20 characters can be used. <i>[ip ipv6]</i> – Specify the ip or ipv6 of multicast vlan to be displayed on the Switch.
Restrictions	None.

Example usage:

To show igmp snooping multicast VLAN:

```
DGS-1100-10/ME:5>show igmp_snooping multicast_vlan default
Command: show igmp_snooping multicast_vlan default

IGMP Snooping Global State      : Disable
Multicast Router Only           : Disable
Data Driven Learning Max Entries : 64

VLAN Name                       : default
Query Interval                  : 1
Max Response Time               : 10
Robustness Value                : 2
Last Member Query Interval      : 1
Querier State                   : Disable
Querier Role                    : Non-Querier
Querier Select                  : Disable
Querier IP                      : 10.90.90.90
Querier Expiry Time             : 0
State                           : Enable
```

Fast Leave	: Disable
Version	: 3
Data Driven Learning Aged Out	: Disable

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

show igmp_snooping multicast_vlan_group

Purpose	To show the current status of IGMP snooping multicast VLAN group on the Switch.
Syntax	show igmp_snooping multicast_vlan_group <vlan_name 20> [ip ipv6]
Description	The show igmp_snooping multicast_vlan_group command displays the current IGMP snooping configuration on the Switch.
Parameters	<i><vlan_name 20></i> – The name of the VLAN for which IGMP snooping configuration is to be displayed. Up to 20 characters can be used. <i>[ip ipv6]</i> – Specify the ip or ipv6 of multicast vlan group to be displayed on the Switch.
Restrictions	None.

Example usage:

To show igmp snooping multicast VLAN group:

```
DGS-1100-10/ME:5> show igmp_snooping multicast_vlan_group rd1
Command: show igmp_snooping multicast_vlan_group rd1

VID Vlan Name          IP Range
----
-----

DGS-1100-10/ME:5>
```

show igmp_snooping group

Purpose	To display the current IGMP snooping group configuration on the Switch.
Syntax	show igmp_snooping group {vlan <vlan_name 20> vlanid <vidlist 1-4094>}
Description	The show igmp_snooping group command displays the current IGMP snooping group configuration on the Switch.
Parameters	<i>vlan <vlan_name 20></i> – The name of the VLAN of the IGMP snooping group configuration information that will be displayed. Up to 20 characters can be used. <i>vlanid <vidlist 1-4094></i> – The ID of the VLAN for which IGMP snooping group configuration information is to be displayed.
Restrictions	None.

Example usage:

To show igmp snooping group:

```
DGS-1100-10/ME:5> show igmp_snooping group vlan default
Command: show igmp_snooping group vlan default

Total Entries: 0

DGS-1100-10/ME:5>
```

show igmp_snooping host

Purpose	To display the IGMP snooping host table entries on the Switch.
Syntax	show igmp_snooping host {group <ipaddr> ports <portlist 1-10> vlan <vlan_name 20> vlanid <vidlist 1-4094>}
Description	The show igmp_snooping host command displays the current IGMP snooping forwarding table entries currently configured on the Switch.
Parameters	<p><i>group <ipaddr></i> – Specifies the IGMP Snooping group IP address to be displayed.</p> <p><i>ports <portlist 1-10></i> – Specifies the IGMP Snooping ports to be displayed.</p> <p><i>vlan <vlan_name 20></i> – Specifies the VLAN name of IGMP Snooping to be displayed.</p> <p><i>vlanid <vidlist 1-4094></i> – Specifies the VLAN ID of IGMP Snooping to be displayed.</p>
Restrictions	None.

Example usage:

To view the IGMP snooping host table on the Switch:

```
DGS-1100-10/ME:5>show igmp_snooping host
Command: show igmp_snooping host

VLAN ID   Group                Port No   IGMP Host
-----   -
Total Entries : 0

DGS-1100-10/ME:5>
```

show router_port

Purpose	To display the currently configured router ports on the Switch.
Syntax	show router_port {vlan <vlan_name 20> vlanid <vidlist 1-4094> static dynamic}

Description	The show router_port command displays the router ports currently configured on the Switch.
Parameters	<p><i>vlan</i> <<i>vlan_name</i> 20> – The name of the VLAN on which the router port resides. Up to 32 characters can be used.</p> <p><i>vlanid</i> <<i>vidlist</i> 1-4094> – The ID 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 learned.</p>
Restrictions	None.

Example usage:

To display the router ports:

```
DGS-1100-10/ME:5>show router_ports
Command: show router_ports

VLAN Name       : default
Static router port :
Dynamic router port :
Forbidden router port :

Total Entries : 1
DGS-1100-10/ME:5>
```

MLD SNOOPING COMMANDS

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

Command	Parameter
enable mld_snooping	
disable mld_snooping	
config mld_snooping	[vlan_name <vlan_name 20> vlanid <vidlist 1-4094> all] [state [enable disable]] fast_leave [enable disable]]
config mld_snooping router_ports	[vlan_name <string 20> vlanid <vidlist 1-4094> all] [add delete] <portlist 1-10>
config mld_snooping querier	[vlan_name <vlan_name 20> vlanid <vidlist 1-4094> all] [host_timeout <sec 130-153025> router_timeout <sec 60-600> last_member_query_interval <sec 1-25> max_response_time <sec 10-25> query_interval <sec 60-600> robustness_variable <value 2-255> state [enable disable] version <value 1-2>]
show mld snooping	[vlan <vlan_name 20> vlanid <vidlist 1-4094> all]
show mld_snooping group	[vlan <vlan_name 20> vlanid <vidlist 1-4094>]
show mld_snooping router_ports	[vlan <vlan_name 20> vlanid <vidlist 1-4094> all] [dynamic static]
show mld_snooping host	[vlan_name <string 20> vlanid <vidlist 1-4094> ports <portlist 1-10> group <ipv6_addr>]

Each command is listed in detail, as follows:

enable mld_snooping	
Purpose	To enable MLD snooping on the Switch.
Syntax	enable mld snooping
Description	The enable mld snooping command enables MLD snooping on the Switch.
Parameters	None.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To enable the MLD snooping:

```
DGS-1100-10/ME:5>enable mld_snooping
Command: enable mld_snooping

Success !
```

```
DGS-1100-10/ME:5>
```

disable mld_snooping

Purpose	To disable MLD snooping on the Switch.
Syntax	disable mld snooping
Description	The disable mld snooping command disables MLD snooping on the Switch.
Parameters	None.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To disable the MLD snooping:

```
DGS-1100-10/ME:5>disable mld_snooping
```

```
Command: disable mld_snooping
```

```
Success !
```

```
DGS-1100-10/ME:5>
```

config mld_snooping

Purpose	To configure mld snooping.
Syntax	config mld_snooping [vlan_name <vlan_name 20> vlanid <vidlist 1-4094> all] [state [enable disable] fast_leave [enable disable]]
Description	The config mld_snooping command defines mld snooping on the VLAN.
Parameters	<p><i>vlan_name</i> <vlan_name 20> – Specifies that the mld snooping applies only to this previously created VLAN.</p> <p><i>vlanid</i> <vidlist 1-4094> – Specifies that the mld snooping applies only to this VLAN ID.</p> <p><i>all</i> – specifies that MLD snooping is to be configured for all VLANs on the Switch.</p> <p><i>state</i> – Allows the user to enable or disable MLD snooping for the specified VLAN.</p> <p><i>fast_leave</i> – Allows the user to enable or disable MLD snooping for the specified VLAN.</p>
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure mld snooping:

```
DGS-1100-10/ME:5> config mld_snooping all state enable
```

```
Command: config mld_snooping all state enable
```

Success!

DGS-1100-10/ME:5>

config mld_snooping router_ports

Purpose	To enable mld mrouter ports.
Syntax	config mld_snooping router_ports [vlan_name <string 20> vlanid <vidlist 1-4094> all] [add delete] <portlist 1-10>
Description	The config mld_snooping router_ports command defines a port that is connected to a multicast router port.
Parameters	<p><i>vlan_name <string 20></i> – specifies that the mld snooping applies only to this previously created VLAN.</p> <p><i>vlanid <vidlist 1-4094></i> – specifies that the mld snooping applies only to this previously created VLAN id.</p> <p><i>all</i> – specifies that MLD snooping is to be configured for all VLANs on the Switch.</p> <p><i>add</i> – Adds a specified port to the mld snooping mrouter port.</p> <p><i>delete</i> – Deletes a specified port to the mld snooping mrouter port.</p> <p><i><portlist 1-10></i> – Defines the ports to be included from the mld snooping mrouter group.</p>
Restrictions	<p>Only administrator or operator–level users can issue this command</p> <p>Separate non–consecutive Ethernet ports with a comma and no spaces; use a hyphen to designate a range of ports. These ports are defined as connected to a multicast router.</p>

Example usage:

To configure mld mrouter ports:

```
DGS-1100-10/ME:5> config mld_snooping router_ports vlanid 1 add 3
Command: config mld_snooping router_ports vlanid 1 add 3
```

Success!

DGS-1100-10/ME:5>

config mld_snooping querier

Purpose	Used to configure the timers and settings for the MLD snooping querier for the Switch.
Syntax	config mld_snooping querier [vlan_name <vlan_name 20> vlanid <vidlist 1-4094> all] [host_timeout <sec 130-153025> router_timeout <sec 60-600> last_member_query_interval <sec 1-25> max_response_time <sec 10-25> query_interval <sec 60-600> robustness_variable <value 2-255> state [enable disable] version <value 1-2>]
Description	The config mld_snooping querier command allows users to configure the time between general query transmissions, the

Parameters	<p>maximum time to wait for reports from listeners and the permitted packet loss guaranteed by MLD snooping.</p> <p><i>vlan_name</i> <<i>vlan_name</i> 20> – Specifies that the mld snooping applies only to this previously created VLAN.</p> <p><i>vlanid</i> <<i>vidlist</i> 1-4094> – specifies that the mld snooping applies only to this previously created VLAN id.</p> <p><i>all</i> – specifies that MLD snooping is to be configured for all VLANs on the Switch.</p> <p><i>host_timeout</i> <<i>sec</i> 130-153025> – Specifies the maximum amount of time a host can be a member of a multicast group without the switch receiving a host membership report. The default is 260 seconds.</p> <p><i>router_timeout</i> <<i>sec</i> 60-600> – Specifies the maximum amount of time a router can be a member of a multicast group without the Switch receiving a host membership report.</p> <p><i>last_member_query_interval</i> <<i>sec</i> 1-25> – The maximum amount of time to be set between group-specific query messages. This interval may be reduced to lower the amount of time it takes a router to detect the loss of a last listener group. The user may set this interval between 1 and 25 seconds with a default setting of 1 second.</p> <p><i>max_response_time</i> <<i>sec</i> 10-25> – The maximum time to wait for reports from listeners. The user may specify a time between 1 and 25 seconds with a default setting of 10 seconds.</p> <p><i>query_interval</i> <<i>sec</i> 60-600> – Specifies the amount of time between general query transmissions. The user may specify a time between 1 and 65535 seconds with a default setting of 125 seconds.</p> <p><i>robustness_variable</i> <<i>value</i> 2-255> – Provides fine-tuning to allow for expected packet loss on a subnet. The user may choose a value between 1 and 255 with a default setting of 2. If a subnet is expected to be lossy, the user may wish to increase this interval.</p> <p><i>state</i> [<i>enable</i> <i>disable</i>] – Enabling the querier state will set the Switch as a MLD querier and disabling it will set it as a Non-querier. The default setting is disabled.</p> <p><i>version</i> <<i>value</i> 1-2> – 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 forward from router ports or VLAN flooding. The value is between 1 and 2.</p>
Restrictions	Only administrator or operator–level users can issue this command.

Example usage:

To configure MLD snooping querier:

```
DGS-1100-10/ME:5>config mld_snooping querier vlan_name 2
last_member_query_interval 1 query_interval 60
Command: config mld_snooping querier vlan_name 2 last_ member
_query_interval 1 query_interval 60

Success!
DGS-1100-10/ME:5>
```

show mld_snooping

Purpose	To display mld snooping settings on the Switch.
Syntax	show mld_snooping [vlan <vlan_name 20> vlanid <vidlist 1-4094> all]
Description	The show mld_snooping command displays a port from being defined as a multicast router port by static configuration or by automatic learning.
Parameters	<p><i>vlan <vlan_name 20></i> – Displays that MLD snooping applies only to this previously created VLAN.</p> <p><i>vlanid <vidlist 1-4094></i> – Displays that MLD snooping applies only to this previously created VLAN ID.</p> <p><i>all</i> – Shows MLD snooping is configured for all VLANs on the Switch.</p>
Restrictions	None.

Example usage:

To show the MLD snooping:

```
DGS-1100-10/ME:5> show mld_snooping vlan default
Command: show mld_snooping vlan default
```

```
MLD Snooping Global State      : Enabled
```

```

VLAN Name          : default
Host Timeout       : 260
Router Timeout     : 250
Query Interval     : 125
Max Response Time  : 10
Robustness Value   : 2
Last Member Query Interval : 2
Querier State      : Disabled
State              : Enabled
Fast Leave         : Disabled
Version            : 2

```

```
Total Entries: 1
```

```
DGS-1100-10/ME:5>
```

show mld_snooping group

Purpose	To display mld snooping group settings on the Switch.
Syntax	show mld_snooping group [vlan <vlan_name 20> vlanid <vidlist 1-4094>]
Description	The show mld_snooping group command displays the multicast

	groups that were learned by MLD snooping.
Parameters	<i>vlan</i> < <i>vlan_name</i> 20> – The name of the VLAN for which to view the MLD snooping group configurations. <i>vlanid</i> < <i>vidlist</i> 1-4094> – The ID of the VLAN for which to view the MLD snooping group configurations.
Restrictions	None.

Example usage:

To show the MLD snooping groups:

```
DGS-1100-10/ME:5> show mld_snooping group vlan default
Command: show mld_snooping group vlan default

Total Entries: 0

DGS-1100-10/ME:5>
```

show mld_snooping router_ports

Purpose	To display information on dynamically learnt and static multicast router interfaces.
Syntax	show mld_snooping router_ports [<i>vlan</i> < <i>vlan_name</i> 20> <i>vlanid</i> < <i>vidlist</i> 1-4094> <i>all</i>] [<i>dynamic</i> <i>static</i>]
Description	The show mld_snooping router_ports command, displays both dynamically learnt and static multicast router interfaces.
Parameters	<i>vlan</i> < <i>vlan_name</i> 20> – Specifies on which VLAN MLD snooping groups should be shown. <i>vlanid</i> < <i>vidlist</i> 1-4094> – Displays that the MLD snooping applies only to this previously created VLAN ID. <i>all</i> – Displays that all MLD snooping was configured for all VLANs on the Switch. <i>static</i> – Displays statically configured MLD router ports. <i>dynamic</i> – Displays dynamically configured MLD router ports.
Restrictions	None.

Example usage:

To show the MLD_snooping mrouterport:

```
DGS-1100-10/ME:5> show mld_snooping router_ports vlanid 1
Command: show mld_snooping router_ports vlanid 1

VLAN Name       : default
Static Router Port : 3
Dynamic Router Port :
```

Success!

DGS-1100-10/ME:5>

show mld_snooping host

Purpose	To display information of MLD snooping host on the Switch.
Syntax	show mld_snooping host [vlan_name <string 20> vlanid <vidlist 1-4094> ports <portlist 1-10> group <ipv6_addr>]
Description	The show mld_snooping host command displays information about the MLD snooping host on the Switch.
Parameters	<p><i>vlan_name</i> <string 20> – Specifies which VLAN MLD snooping groups should be shown.</p> <p><i>vlanid</i> <vidlist 1-4094> – Shows that mld snooping applies only to this previously created VLAN ID.</p> <p><i>ports</i> <portlist 1-10> – Specifies which ports of MLD snooping host to be displayed.</p> <p><i>group</i> <ipv6_addr> – Specifies the IPv6 address.</p>
Restrictions	None.

Example usage:

To show the MLD_snooping host:

```

DGS-1100-10/ME:5> show mld_snooping host vlan_name default
Command: show mld_snooping host vlan_name default

VLAN ID      Group                Port No      Host
-----      -
Total Entries: 0
DGS-1100-10/ME:5>

```

LIMITED IP MULTICAST ADDRESS COMMANDS

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

Command	Parameter
create mcast_filter_profile	[ipv4 ipv6] profile_id <integer 1-24> profile_name string
config mcast_filter_profile	[profile_id <integer 1-24> profile_name <string 32>] [add delete] <mcast_addr>
config mcast_filter_profile ipv6	[profile_id <integer 1-24> profile_name <string 32>] [add delete] <ipv6_mcast_addr>
delete mcast_filter_profile	[ipv4 ipv6] [profile_id<integer 1-24> profile_name <string 32>]
show mcast_filter_profile	{[ipv4 ipv6]} {profile_id <integer 1-24> profile_name <string 32>}
config limited_multicast_addr ports	<portlist 1-10> [ipv4 ipv6] {[add delete] [max_group <integer 1-256> access [permit deny]]}
show limited_multicast_addr ports	<portlist 1-10> {[ipv4 ipv6]}
show max_mcast_group ports	<portlist 1-10> {[ipv4 ipv6]}

Each command is listed in detail, as follows:

create mcast_filter_profile	
Purpose	To create multicast filtering profile on the Switch.
Syntax	create mcast_filter_profile [ipv4 ipv6] profile_id <integer 1-24> profile_name string
Description	The create mcast_filter_profile command displays the multicast filtering profiles settings.
Parameters	<i>[ipv4 ipv6]</i> – Specifies which IPv4 or IPv6 multicast filter profile to be created on the Switch. <i>profile_id <integer 1-24></i> - Specifies the profile ID of the multicast filter on the Switch. <i>profile_name string</i> - Specifies the profile name of the multicast filter profile on the Switch.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To create an IPv4 multicast filtering profile on the Switch:

```
DGS-1100-10/ME:5> create mcast_filter_profile ipv4 profile_id 1 profile_name
string
Command: create mcast_filter_profile ipv4 profile_id 1 profile_name string

Success!
DGS-1100-10/ME:5>
```

config mcast_filter_profile

Purpose	To configure multicast filtering profile on the Switch.
Syntax	config mcast_filter_profile [profile_id <integer 1-24> profile_name <string 32>] [add delete] <mcast_addr>
Description	The config mcast_filter_profile command displays the multicast filtering profiles settings.
Parameters	<p><i>profile_id <integer 1-24></i> - Specify the profile ID to be added or deleted for the multicast filter.</p> <p><i>profile_name <string 32></i> - The name of the VLAN on which the MAC address resides.</p> <p><i>[add delete]</i> – Add or delete the profile ID which user specified.</p> <p><i><mcast_addr></i> – Specify the range of IPv4 address.</p>
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To add the multicast address range 225.1.1.1 to 225.1.1.10 to the profile on the Switch:

```
DGS-1100-10/ME:5>config mcast_filter_profile profile_id 3 add 225.1.1.1
225.1.1.10
Command: config mcast_filter_profile profile_id 3 add 225.1.1.1 225.1.1.10

Success!
DGS-1100-10/ME:5>
```

config mcast_filter_profile ipv6

Purpose	To configure IPv6 multicast filtering profile on the Switch.
Syntax	config mcast_filter_profile ipv6 [profile_id <integer 1-24> profile_name <string 32>] [add delete] <ipv6_mcast_addr>
Description	The config mcast_filter_profile ipv6 command is used to add or delete a range of IPv6 multicast addresses to the profile
Parameters	<p><i>profile_id <integer 1-24></i> - Specify the profile id to be added or deleted for the multicast filter.</p> <p><i>profile_name <string 32></i> - The name of the VLAN on which the MAC address resides.</p> <p><i>[add delete]</i> – Add or delete the profile ID which the user specified.</p> <p><i><ipv6_mcast_addr></i> – Lists the IPv6 multicast addresses to put in</p>

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

Example usage:

To add the IPv6 multicast address range FFF0E::100:0:0:20 – FFF0E::100:0:0:22 to profile ID 4 on the Switch:

```
DGS-1100-10/ME:5>config mcast_filter_profile ipv6 profile_id 4 add
FFF0E::100:0:0:20 FFF0E::100:0:0:22
Command: config mcast_filter_profile ipv6 profile_id 4 add
FFF0E::100:0:0:20 FFF0E::100:0:0:22

Success!
DGS-1100-10/ME:5>
```

delete mcast_filter_profile

Purpose	To delete an entry in the switch's forwarding database.
Syntax	delete mcast_filter_profile [<i>ipv4</i> <i>ipv6</i>] [profile_id <integer 1-24> profile_name <string 32>]
Description	The delete mcast_filter_profile command deletes a profile in the switch's multicast forwarding filtering database.
Parameters	<i>[ipv4 ipv6]</i> – Specify the IPv4 or IPv6 of multicast filter profile to be removed on the switch. <i>profile_id</i> <integer 1-24> – The profile id of the VLAN on which the multicast forwarding filtering database resides. <i>profile_name</i> <string 32> – The name of the VLAN on which the multicast forwarding filtering database resides.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To delete the IPv4 multicast address profile with a profile name of rd3:

```
DGS-1100-10/ME:5>delete mcast_filter_profile ipv4 profile_name rd3
Command: delete mcast_filter_profile ipv4 profile_name rd3

Success!
DGS-1100-10/ME:5>
```

show mcast_filter_profile

Purpose	To display multicast filtering settings on the Switch.
Syntax	show mcast_filter_profile {[<i>ipv4</i> <i>ipv6</i>]} { profile_id <integer 1-24> profile_name <string 32>}
Description	The show mcast_filter_profile command displays the multicast filtering profiles settings.
Parameters	<i>[ipv4 ipv6]</i> – Specify the IPv4 or IPv6 of multicast filter profile to be displayed on the Switch.

	<p><i>profile_id</i> <integer 1-24> - Specify the profile ID of the multicast filter profile to be displayed.</p> <p><i>profile_name</i> <string 32> - Specify the profile name of the multicast filter profile to be displayed.</p>
Restrictions	None.

Example usage:

To display all the defined multicast address profiles:

```
DGS-1100-10/ME:5> show mcast_filter_profile ipv4 profile_id 1
Command: show mcast_filter_profile ipv4 profile_id 1

Mcast Filter Profile:

Profile ID   Name           Multicast Addresses
-----
1           string

Total Profile Count: 1

DGS-1100-10/ME:5>
```

config limited_multicast_addr ports	
Purpose	To configure the multicast address filtering function on a port.
Syntax	config limited_multicast_addr ports <portlist 1-10> [<i>ipv4</i> <i>ipv6</i>] {[add delete] [max_group <integer 1-256> access [permit deny]}
Description	The config limited_multicast_addr ports command is used to configure the multicast address filtering function on a port. When there are no profiles specified with a port, the limited function is not effective.
Parameters	<p><i>ports</i> <portlist 1-10> – A port or range of ports on which the limited multicast address range to be configured has been assigned.</p> <p><i>[ipv4 ipv6]</i> – Specify the IPv4 or IPv6 of multicast filter profile to be configured.</p> <p><i>add</i> – Add a multicast address profile to a port.</p> <p><i>delete</i> – Delete a multicast address profile to a port.</p> <p><i>permit</i> – Specifies the packet that matches the addresses defined in the profiles will be permitted. The default mode is permit.</p> <p><i>deny</i> – Specifies that the packet matches the addresses defined in the profiles will be denied.</p>
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure ports 1 and 3 to set the IPv6 multicast address profile ID 1:

```
DGS-1100-10/ME:5> config limited_multicast_addr ports 1 ipv6 access permit
Command: config limited_multicast_addr ports 1 ipv6 access permit
```

Success!
DGS-1100-10/ME:5>

show limited_multicast_addr ports

Purpose	Used to show the per-port Limited IP multicast address range.
Syntax	show limited_multicast_addr ports <portlist 1-10> {[ipv4 ipv6]}
Description	The show limited_multicast_addr ports command is to display the multicast address range by port or by VLAN.
Parameters	<i><portlist 1-10></i> – Used to show the per-port Limited IP multicast address range. <i>[ipv4 ipv6]</i> – Specify the IPv4 or IPv6 of limited multicast address to be displayed.
Restrictions	None.

Example usage:

To show the IPv4 limited multicast address on ports 1 and 3:

```
DGS-1100-10/ME:5> show limited_multicast_addr ports 1
Command: show limited_multicast_addr ports 1

Port : 1
Access: permit

Profile ID      Name                Multicast Addresses
-----
DGS-1100-10/ME:5>
```

show max_mcast_group ports

Purpose	To display maximum multicast group ports on the Switch.
Syntax	show max_mcast_group ports <portlist 1-10> {[ipv4 ipv6]}
Description	The show max_mcast_group ports command displays the multicast filtering profiles settings.
Parameters	<i><portlist></i> - Specify a port or a range of ports to be displayed. <i>{[ipv4 ipv6]}</i> – Specify the IPv4 or IPv6 to be displayed.
Restrictions	None.

Example usage:

To show IPv6 maximum multicast group port 1 settings:

```
DGS-1100-10/ME:5> show max_mcast_group ports 1 ipv6
Command: show max_mcast_group ports 1 ipv6
```

Port	MaxMcastGroup
-----	-----
1	256

DGS-1100-10/ME:5>

802.1X COMMANDS

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

Command	Parameter
enable 802.1x	
disable 802.1x	
show 802.1x	
show 802.1x auth_state	{ports <portlist 1-10>}
show 802.1x auth_configuration	{ports <portlist 1-10>}
config 802.1x auth_parameter ports	[<portlist 1-10> all] [default { port_control [force_unauth auto force_auth] quiet_period <sec 0-65535> tx_period <sec 1-65535> supp_timeout <sec 1-65535> server_timeout <sec 1-65535> max_req <value 1-10> reauth_period <sec 1-65535> enable_reauth [enable disable] direction [both in]]]
config 802.1x auth_protocol	[radius_eap local]
config radius add	<server_index 1-3> [<ipaddr> <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 1-255>}
config radius delete	<server_index 1-3>
config radius	<server_index 1-3> { key <passwd 32> auth_port <udp_port_number 1-65535> acct_port <udp_port_number 1-65535> ipaddress [<ipaddr> <ipv6addr>] retransmit <int 1-255> timeout <int 1-255>}
show radius	
config 802.1x auth_mode	[port_based mac_based]
create 802.1x guest vlan	<vlan_name 20>
delete 802.1x guest vlan	<vlan_name 20>
config 802.1x guest_vlan ports	[<portlist 1-10> all] state [enable disable]
show 802.1x guest_vlan	
create 802.1x user	<username 15>
show 802.1x user	
delete 802.1x user	<username 15>

Command	Parameter
config 802.1x capability ports	[<portlist 1-10> all] [authenticator none]

Each command is listed in detail, as follows:

enable 802.1x

Purpose	To enable the 802.1x server on the Switch.
Syntax	enable 802.1x
Description	The enable 802.1x command enables the 802.1x Port-based Network Access control server application on the Switch.
Parameters	None.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To enable 802.1x switch wide:

```
DGS-1100-10/ME:5>enable 802.1x
Command: enable 802.1x

Success!
DGS-1100-10/ME:5>
```

disable 802.1x

Purpose	To disable the 802.1x server on the switch.
Syntax	disable 802.1x
Description	The disable 802.1x command disables the 802.1x port-based network access control server application on the switch.
Parameters	None.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To disable 802.1x on the Switch:

```
DGS-1100-10/ME:5>disable 802.1x
Command: disable 802.1x

Success!
DGS-1100-10/ME:5>
```

show 802.1x

Purpose	To display the 802.1x server information on the Switch.
---------	---

Syntax	show 802.1x
Description	The show 802.1x command displays the 802.1x port-based network access control server application on the switch.
Parameters	None.
Restrictions	None.

Example usage:

To display 802.1x on the Switch:

```
DGS-1100-10/ME:5>show 802.1x
Command: show 802.1x

802.1X           : Enable
Authentication Mode : Port_base
Authentication Method : Local
DGS-1100-10/ME:5>
```

show 802.1x auth_state	
Purpose	To display the current authentication state of the 802.1x server on the Switch.
Syntax	show 802.1x auth_state {ports <portlist 1-10>}
Description	<p>The show 802.1x auth_state command displays the current 802.1x authentication state of the specified ports of the port-based network access control server application on the switch.</p> <p>The following details are displayed:</p> <p>Port number – Shows the physical port number on the switch.</p> <p>Auth PAE State: Initialize / Disconnected / Connecting / Authenticating / Authenticated / Held / ForceAuth / ForceUnauth – Shows the current state of the Authenticator PAE.</p> <p>Backend State: Request / Response / Fail / Idle / Initialize / Success / Timeout – Shows the current state of the Backend Authenticator.</p> <p>Port Status: Authorized / Unauthorized – Shows the result of the authentication process. Authorized means that the user was authenticated, and can access the network. Unauthorized means that the user was not authenticated, and cannot access the network.</p>
Parameters	<i>ports <portlist 1-10></i> – A port or range of ports whose settings are to be displayed.
Restrictions	None.

Example usage:

To display the 802.1x authentication states for port 1~3 for Port-based 802.1x:

```
DGS-1100-10/ME:5> show 802.1x auth_state ports 1-3
Command: show 802.1x auth_state ports 1-3

Port  Auth PAE State  Backend State  Port Status
-----
1     Initialize         Initialize     Authorized
```

2	Initialize	Initialize	Authorized
3	Initialize	Initialize	Authorized

DGS-1100-10/ME:5>

show 802.1x auth_configuration

Purpose	To display the current configuration of the 802.1x server on the Switch.
Syntax	show 802.1x auth_configuration {ports <portlist 1-10>}
Description	<p>The show 802.1x auth_configuration command displays the current configuration of the 802.1x port-based network access control server application on the switch.</p> <p>The following details are displayed:</p> <p><i>802.1x</i>: Enabled/Disabled – Shows the current status of 802.1x functions on the switch.</p> <p><i>Authentication Mode</i>: Port-based/Mac-based/None – Shows the 802.1x authorization mode.</p> <p><i>Authentication Method</i>: Remote/none – Shows the type of authentication protocol suite in use between the switch and a RADIUS server.</p> <p><i>Port number</i> : Shows the physical port number on the switch.</p> <p><i>AdminCrDir</i>: Both/In – Shows whether a controlled Port that is unauthorized will exert control over communication in both receiving and transmitting directions, or just the receiving direction.</p> <p><i>OpenCrDir</i>: Both/In – Shows whether a controlled Port that is unauthorized will exert control over communication in both receiving and transmitting directions, or just the receiving direction.</p> <p><i>Port Control</i>: ForceAuth/ForceUnauth/Auto – Shows the administrative control over the port's authorization status. ForceAuth forces the authenticator of the port to become authorized. ForceUnauth forces the port to become unauthorized.</p> <p><i>QuietPeriod</i> : Shows the time interval between authentication failure and the start of a new authentication attempt.</p> <p><i>TxPeriod</i> : Shows the time to wait for a response from a supplicant (user) to send EAP Request/Identity packets.</p> <p><i>SuppTimeout</i> : Shows the time to wait for a response from a supplicant (user) for all EAP packets, except for the request/identity packets.</p> <p><i>ServerTimeout</i> : Shows the length of time to wait for a response from a RADIUS server.</p> <p><i>MaxReq</i> : Shows the maximum number of times that you can retry sending packets to the supplicant.</p> <p><i>ReAuthPeriod</i> : Shows the time interval between successive reauthentications.</p> <p><i>ReAuthenticate</i>: true/false – Shows whether or not to reauthenticate.</p>
Parameters	<i>ports <portlist 1-10></i> – Specifies a port or range of ports to be viewed.
Restrictions	None.

Example usage:

To display the 802.1x configurations of port 2:

```
DGS-1100-10/ME:5> show 802.1x auth_configuration ports 2
Command: show 802.1x auth_configuration ports 2

Port number      : 2
Capability       : none
AdminCrIDir     : Both
OperCrIDir      : Both
Port Control     : ForceAuthorized
QuietPeriod     : 60  sec
TxPeriod        : 30  sec
SuppTimeout     : 30  sec
ServerTimeout   : 30  sec
MaxReq          : 2   times
ReAuthPeriod    : 3600 sec
ReAuthenticate  : Disabled

Success!
DGS-1100-10/ME:5>
```

config 802.1x auth_parameter ports

Purpose	To configure the 802.1x authentication parameters on a range of ports. The default parameter returns all ports in the specified range to their default 802.1x settings.
Syntax	config 802.1x auth_parameter ports [<portlist 1-10> all] [default { port_control [force_unauth auto force_auth] quiet_period <sec 0-65535> tx_period <sec 1-65535> supp_timeout <sec 1-65535> server_timeout <sec 1-65535> max_req <value 1-10> reauth_period <sec 1-65535> enable_reauth [enable disable] direction [both in]}]
Description	The config 802.1x auth_parameter ports command configures the 802.1x authentication parameters on a range of ports. The default parameter returns all ports in the specified range to their default 802.1x settings.
Parameters	<p><i>[<portlist 1-10> all]</i> – A port, range of ports or all ports to be configured.</p> <p><i>all</i> – Specifies all of the ports on the Switch.</p> <p><i>default</i> – Returns all of the ports in the specified range to their 802.1x default settings.</p> <p><i>port_control</i> – Configures administrative control over the authentication process for a range of ports. The options are:</p> <ul style="list-style-type: none"> <i>force_auth</i> – Forces the Authenticator for the port to become authorized. Network access is allowed. <i>auto</i> – Allows the port's status to reflect the outcome of the authentication process. <i>force_unauth</i> – Forces the Authenticator for the port to become unauthorized. Network access is blocked. <p><i>quiet_period <sec 0-65535></i> – Configures the time interval between</p>

authentication failure and the start of a new authentication attempt.

tx_period <sec 1-65535> - Configures the time to wait for a response from a supplicant (user) to send EAP Request/Identity packets.

supp_timeout <sec 1-65535> - Configures the time to wait for a response from a supplicant (user) for all EAP packets, except for the Request/Identity packets.

server_timeout <sec 1-65535> - Configures the length of time to wait for a response from a RADIUS server.

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

reauth_period <sec 300-4294967295> – Configures the time interval between successive re-authentications.

enable_reauth [*enable* | *disable*] – Determines whether or not the switch will re-authenticate. Enabling will cause re-authentication of users at the time interval specified in the Re-authentication Period field, above.

direction [*both* | *in*] – Sets the administrative-controlled direction to *Both*. If *Both* is selected, control is exerted over both incoming and outgoing traffic through the controlled port selected in the first field. The *In* option is not supported in the present firmware release.

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

Example usage:

To configure 802.1x authentication parameters for ports 1 – 3:

```
DGS-1100-10/ME:5>config 802.1x auth_parameter ports 1-3 direction both
Command: config 802.1x auth_parameter ports 1-3 direction both

Success!
DGS-1100-10/ME:5>
```

config 802.1x auth_protocol

Purpose	To configure the 802.1x authentication protocol on the switch .
Syntax	config 802.1x auth_protocol [radius_eap local]
Description	The config 802.1x auth_protocol command enables configuration of the authentication protocol.
Parameters	<i>radius_eap</i> – Uses the list of RADIUS EAP servers for authentication. <i>local</i> – Uses no authentication.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

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

```
DGS-1100-10/ME:5>config 802.1x auth_protocol local
Command: config 802.1x auth_protocol local

Success!
DGS-1100-10/ME:5>
```

config radius add

Purpose	To configure the settings that the switch uses to communicate with a RADIUS server.
Syntax	config radius add <server_index 1-3> [<ipaddr> <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 1-255>}
Description	The config radius add command configures the settings the Switch uses to communicate with a RADIUS server.
Parameters	<p><i><server_index 1-3></i> – The index of the RADIUS server.</p> <p><i>[<ipaddr> <ipv6_addr>]</i> – The IPv4 or IPv6 address of the RADIUS server.</p> <p><i>key</i> – Specifies that a password and encryption key are to be used between the Switch and the RADIUS server.</p> <p><i><passwd 32></i> – The shared-secret key used by the RADIUS server and the Switch. Up to 128 characters can be used.</p> <p><i>default</i> – Uses the default udp port number in both the <i>auth_port</i> and <i>acct_port</i> settings.</p> <p><i>auth_port <udp_port_number 1-65535></i> – The UDP port number for authentication requests. The default is 1812.</p> <p><i>acct_port <udp_port_number 1-65535></i> – The UDP port number for accounting requests. The default is 1813.</p> <p><i>retransmit <int 1-255></i> –The number of times the device resends an authentication request when the server does not respond. The value is between 1 and 255.</p> <p><i>timeout <int 1-255></i> –Specifies the connection timeout. The value may be between 1 and 255 seconds.</p>
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure the RADIUS server communication settings:

```
DGS-1100-10/ME:5> config radius add 1 10.90.90.99 key dfjk auth_port 100
acct_port 1000 timeout 1 retransmit 10
Command: config radius add 1 10.90.90.99 key dfjk auth_port 100 acct_port
1000 t
imeout 1 retransmit 10

Success!
DGS-1100-10/ME:5>
```

config radius delete

Purpose	To delete a previously entered RADIUS server configuration.
Syntax	config radius delete <server_index 1-3>
Description	The config radius delete command deletes a previously entered RADIUS server configuration.
Parameters	<server_index 1-3> – The index of the RADIUS server.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To delete previously configured RADIUS server communication settings:

```
DGS-1100-10/ME:5>config radius delete 1
```

```
Command: config radius delete 1
```

```
Success!
```

```
DGS-1100-10/ME:5>#
```

config radius

Purpose	To configure the Switch's RADIUS settings.
Syntax	config radius <server_index 1-3> { key <passwd 32> auth_port <udp_port_number 1-65535> acct_port <udp_port_number 1-65535> ipaddress [<ipaddr> <ipv6addr>] retransmit <int 1-255> timeout <int 1-255>}
Description	The config radius command configures the Switch's RADIUS settings.
Parameters	<p><server_index 1-3> – The index of the RADIUS server.</p> <p>key – Specifies that a password and encryption key are to be used between the Switch and the RADIUS server.</p> <ul style="list-style-type: none"> • <passwd 32> – The shared-secret key used by the RADIUS server and the Switch. Up to 128 characters can be used. <p>auth_port <udp_port_number 1-65535> – The UDP port number for authentication requests. The default is 1812.</p> <p>acct_port <udp_port_number 1-65535> – The UDP port number for accounting requests. The default is 1813.</p> <p>ipaddress [<ipaddr> <ipv6addr>] – The IPv4 or IPv6 address of the RADIUS server.</p> <p>retransmit <int 1-255> –The number of times the device resends an authentication request when the server does not respond. The value is between 1 and 255.</p> <p>timeout <int 1-255> –Specifies the connection timeout. The value may be between 1 and 255 seconds.</p>
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure the RADIUS settings:

```
DGS-1100-10/ME:5>config radius 1 ipaddress 10.48.47.11
Command: config radius 1 ipaddress 10.48.47.11

Success!
DGS-1100-10/ME:5>
```

show radius

Purpose	To display the current RADIUS configurations on the Switch.
Syntax	show radius
Description	The show radius command displays the current RADIUS configurations on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display RADIUS settings on the Switch:

```
DGS-1100-10/ME:5>show radius
Command: show radius

Index Ip Address      Auth-Port Acct-Port Timeout Retransmit Key
-----
1      10.48.74.121      1812     1813     5       10       dlink

Total Entries : 1
DGS-1100-10/ME:5>
```

config 802.1x auth_mode

Purpose	To configure the 802.1x authentication mode on the switch.
Syntax	config 802.1x auth_mode [port_based mac_based]
Description	The config 802.1x auth_mode command enables either the port-based or MAC-based 802.1x authentication feature on the switch.
Parameters	<i>[port_based mac_based]</i> – Specifies whether 802.1x authentication is by port or MAC address.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure 802.1x authentication by port address:

```
DGS-1100-10/ME:5>config 802.1x auth_mode port_based
Command: config 802.1x auth_mode port_based

Success!
DGS-1100-10/ME:5>
```

create 802.1x guest_vlan

Purpose	Enables network access to a Guest VLAN.
Syntax	create 802.1x guest_vlan <vlan_name 20>
Description	The create 802.1x guest_vlan command enables network access to a 802.1x Guest VLAN. A network administrator can use 802.1x Guest VLANs to deny network access via port-based authentication, but grant Internet access to unauthorized users.
Parameters	<vlan_name 20> – The name of the 802.1x Guest VLAN to be created.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To create a 802.1x Guest VLAN:

```
DGS-1100-10/ME:5>create 802.1x guest_vlan default
Command: create 802.1x guest_vlan default

Success!
DGS-1100-10/ME:5>
```

delete 802.1x guest_vlan

Purpose	Disables network access to a Guest VLAN.
Syntax	delete 802.1x guest_vlan <vlan_name 20>
Description	The delete 802.1x guest_vlan command disables network access to a 802.1x Guest VLAN. A network administrator can use 802.1x Guest VLANs to deny network access via port-based authentication, but grant Internet access to unauthorized users.
Parameters	<vlan_name 20> – The name of the 802.1x Guest VLAN to be deleted.
Restrictions	Only administrator or operator-level users can issue this command. The user is required to disable Guest VLAN before deleting a specific the VLAN.

Example usage:

To delete a 802.1x Guest VLAN

```
DGS-1100-10/ME:5>delete 802.1x guest_vlan default
Command: delete 802.1x guest_vlan default
```

```
Success!
DGS-1100-10/ME:5>
```

config 802.1x guest_vlan ports

Purpose	Defines a port or range of ports to be members of the Guest VLAN.
Syntax	config 802.1x guest_vlan ports [<portlist 1-10> all] state [enable disable]
Description	The config 802.1x guest_vlan ports command defines a port or range of ports to be members of the 802.1x Guest VLAN. The 802.1x Guest VLAN can be configured to provide limited network access to authorized member ports. If a member port is denied network access via port-based authorization, but the 802.1x Guest VLAN is enabled, the member port receives limited network access. For example, a network administrator can use the 802.1x Guest VLAN to deny internal network access via port-based authentication, but grant Internet access to unauthorized users.
Parameters	<portlist 1-10> – A port or range of ports to be configured to the Guest VLAN. all – Indicates all ports to be configured to the guest vlan. state [enable disable] – Specifies the guest vlan port is enabled or disabled of the switch.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure ports to the Guest VLAN:

```
DGS-1100-10/ME:5>config 802.1x guest_vlan ports 1-3 state enable
Command: config 802.1x guest_vlan ports 1-3 state enable
```

```
Success!
DGS-1100-10/ME:5>
```

show 802.1x guest_vlan

Purpose	Displays configuration information for the Guest VLAN.
Syntax	show 802.1x guest_vlan
Description	The show 802.1x guest_vlan command displays the Guest VLAN name, state, and member ports.
Parameters	None.
Restrictions	None.

Example usage:

To display the Guest VLAN configuration information:

```
DGS-1100-10/ME:5>show 802.1x guest_vlan
```

```
Command: show 802.1x guest_vlan
```

Guest VLAN Settings

```
-----
Guest VLAN                : default
Enabled Guest VLAN Ports  : 1,2,3,4,5,6
```

```
DGS-1100-10/ME:5>
```

create 802.1x user

Purpose	Enable network access to a 802.1x user.
Syntax	create 802.1x user <username 15>
Description	The create 802.1x user command enables network access to a 802.1x user.
Parameters	<vlan_name 15> – The name of the 802.1x user to be created.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To create a 802.1x user:

```
DGS-1100-10/ME:5> create 802.1x user dlink
```

```
Command: create 802.1x user dlink
```

```
Enter a case-sensitive new password:****
```

```
Enter the new password again for confirmation:****
```

```
Success!
```

```
DGS-1100-10/ME:5>
```

show 802.1x user

Purpose	Displays the user information for the 802.1x.
Syntax	show 802.1x user
Description	The show 802.1x user command displays the 802.1x user information on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display the 802.1x user information:

```
DGS-1100-10/ME:5>show 802.1x user
```

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

Index	Username
1	dlink

```
Total Entries: 1
```

```
Success!
```

```
DGS-1100-10/ME:5>
```

delete 802.1x user

Purpose	Deletes network access to 802.1x users.
Syntax	delete 802.1x user <username 15>
Description	The delete 802.1x user command deletes network access to a 802.1x user.
Parameters	<vlanname 15> – The name of the 802.1x user to be deleted.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To delete the 802.1x user:

```
DGS-1100-10/ME:5>delete 802.1x user dlink
```

```
Command: delete 802.1x user dlink
```

```
Success!
```

```
DGS-1100-10/ME:5>
```

config 802.1x capability ports

Purpose	Defines a port or range of ports to be members of the 802.1x.
Syntax	config 802.1x capability ports [<portlist 1-10> all] [authenticator none]
Description	The config 802.1x capability ports is used to configure the capability for the 802.1x on the Switch.
Parameters	<portlist 1-10> – A port or range of ports to be configured to the 802.1x capability. all – Indicates all ports to be configured to the 802.1x capability. [authenticator none] – Specifies the 802.1x capability port to be authenticator or none.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure capability ports to the 802.1x on the Switch:

```
DGS-1100-10/ME:5>config 802.1x capability ports all authenticator  
Command: config 802.1x capability ports all authenticator
```

```
Success!
```

```
DGS-1100-10/ME:5>
```

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	Parameter
config port_security	[<portlist 1-10> all] [admin_state [enable disable] max_learning_addr <max_lock_no 0-64> lock_address_mode [Permanent DeleteOnTimeout DeleteOnReset]
show port_security	{ports <portlist 1-10>}

Each command is listed in detail, as follows:

config port_security	
Purpose	To configure port security settings.
Syntax	config port_security [<portlist 1-10> all] [admin_state [enable disable] max_learning_addr <max_lock_no 0-64> lock_address_mode [Permanent DeleteOnTimeout DeleteOnReset]
Description	The config port_security command configures port security settings for specific ports.
Parameters	<p><portlist 1-10> – A port or range of ports to be configured.</p> <p>all – Configures port security for all ports on the Switch.</p> <p>admin_state [enable disable] – Enables or disables port security for the listed ports.</p> <p>max_learning_addr <int 0-64> - Specify the max learning address. The range is 0 to 64.</p> <p>1-64 Limits the number of MAC addresses dynamically listed in the FDB for the ports.</p> <p>lock_address_mode – Defines the TBD and contains the following options:</p> <ul style="list-style-type: none"> • <i>Permanent</i> – Learns up to the maximum number of dynamic addresses allowed on the port. The learned addresses are not aged out or relearned on other ports as long as the port is locked. • <i>DeleteOnReset</i> – Deletes the current dynamic MAC addresses associated with the port. Learn up to the maximum addresses allowed on the port (this number is also configurable). Aging is disabled; the addresses are deleted on reset • <i>DeleteOnTimeout</i> – Deletes the current dynamic MAC addresses associated with the port. The port learns up to the maximum addresses allowed on the port. Re-learned MAC addresses and address aging out are also enabled. The MAC addresses are deleted when the device is reset and when the address is aged out.

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

Example usage:

To configure port security:

```
DGS-1100-10/ME:5>config port_security 1-5 admin_state enable
max_learning_addr 5 lock_address_mode DeleteOnReset
Command: config port_security 1-5 admin_state enable max_learning_addr 5
lock_address_mode DeleteOnReset

Success!

DGS-1100-10/ME:5>
```

show port_security

Purpose	To display the current port security configuration.
Syntax	show port_security {ports <portlist 1-10>}
Description	The show port_security command displays port security information for the Switch's ports. The information displayed includes port security, admin state, the maximum number of learning addresses, lock mode and trap interval.
Parameters	<i>ports <portlist 1-10></i> – A port or range of ports whose settings are to be displayed.
Restrictions	None.

Example usage:

To display the port security configuration:

```
DGS-1100-10/ME:5>show port_security ports 1-5
Command: show port_security ports 1-5

Port Admin state Max.Learning Addr. Lock Address Mode
-----
1 enabled 5 DeleteOnReset
2 enabled 5 DeleteOnReset
3 enabled 5 DeleteOnReset
4 enabled 5 DeleteOnReset
5 enabled 5 DeleteOnReset

DGS-1100-10/ME:5>
```

PORT PRIORITY COMMANDS

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

Command	Parameter
config port_priority	[<portlist 1-10> all] priority <value 0-7>
show port_priority	{ all <portlist 1-10> }

Each command is listed in detail, as follows:

config port_priority	
Purpose	To configure port priority settings.
Syntax	config port_priority [<portlist 1-10> all] priority [highest low medium high]
Description	The config port_priority command configures port priority settings for specific ports.
Parameters	<i>{all <portlist 1-10>}</i> – Specifies all ports or a range of ports to be configured. <value 0-7> – Specifies the priority of ports mapping priority queue.
Restrictions	Only administrator or operator-level users can issue this command

Example usage:

To configure port priority:

```
DGS-1100-10/ME:5> config port_priority 3 priority 7
Command: config port_priority 3 priority 7

Success!
DGS-1100-10/ME:5>
```

show port_priority	
Purpose	To display the current port priority configuration.
Syntax	show port_priority { all <portlist 1-10> }
Description	The show port_priority command displays port priority information for the switch's ports.
Parameters	<i>{all <portlist 1-10>}</i> – All ports or range of ports whose settings are to be displayed.
Restrictions	None.

Example usage:

To display the port 1~3 priority configuration:

```
DGS-1100-10/ME:5> show port_priority 1-3
```

```
Command: show port_priority 1-3
```

```
Port Priority Effective Priority
```

```
-----  
1      0      0  
2      0      0  
3      7      7
```

```
DGS-1100-10/ME:5>
```

TIME AND SNTP COMMANDS

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

Command	Parameter
config sntp	{primary [<ipaddr> <ipv6addr>] secondary [<ipaddr> <ipv6addr>] poll-interval <sec 30-99999>}
show sntp	
enable sntp	
disable sntp	
config time	<date> <systemtime>
config time_zone operator	[+ hour <gmt_hour 0-13> minute <minute 0-59> - hour <gmt_hour 0-12> minute <minute 0-59>]
config dst	[disable [annual s_date <start_date 1-31> s_mth <start_mth 1-12> s_time <start_time> end_date <int 1-31> e_mth <end_mth 1-12> e_time <end_time> offset [30 60 90 120]]]
show time	

Each command is listed in detail, as follows:

config sntp	
Purpose	To setup SNTP service.
Syntax	config sntp {primary [<ipaddr> <ipv6addr>] secondary [<ipaddr> <ipv6addr>] poll-interval <sec 30-99999>}
Description	The config sntp command configures SNTP service from an SNTP server. SNTP must be enabled for this command to function (See enable sntp).
Parameters	<p><i>primary</i> [<ipaddr> <ipv6addr>] – Specifies the IPv4 or IPv6 address of the primary SNTP server.</p> <p><i>secondary</i> [<ipaddr> <ipv6addr>] – Specifies the IPv4 or IPv6 address of the secondary SNTP server.</p> <p><i>poll-interval</i> <sec 30-99999> – The interval between requests for updated SNTP information. The polling interval ranges from 60 seconds (1 minute) to 86,400 seconds (1 day).</p>
Restrictions	Only administrator or operator-level users can issue this command. SNTP service must be enabled for this command to function (<i>enable sntp</i>).

Example usage:

To configure SNTP settings:

```
DGS-1100-10/ME:5>config sntp primary 10.1.1.1 secondary 10.1.1.2 poll-
interval 60
Command: config sntp primary 10.1.1.1 secondary 10.1.1.2 poll-interval 60

Success!
DGS-1100-10/ME:5>
```

show sntp

Purpose	To display the SNTP information.
Syntax	show sntp
Description	The show sntp command displays SNTP settings information, including the source IP address, time source and poll interval.
Parameters	None.
Restrictions	None.

Example usage:

To display SNTP configuration information:

```
DGS-1100-10/ME:5>show sntp
Command: show sntp

SNTP Information
-----
Current Time Source      : Local
SNTP                     : Disabled
SNTP Primary Server     : 10.1.1.1
SNTP Secondary Server   : 10.1.1.2
SNTP Poll Interval      : 60 sec

DGS-1100-10/ME:5>
```

enable sntp

Purpose	To enable SNTP server support.
Syntax	enable sntp
Description	The enable sntp command enables SNTP server support. SNTP service must be separately configured (see config sntp). Enabling and configuring SNTP support 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-1100-10/ME:5>enable sntp
Command: enable sntp

Success!
DGS-1100-10/ME:5>
```

disable sntp

Purpose	To disable SNTP server support.
Syntax	disable sntp
Description	The disable sntp command disables SNTP support.
Parameters	None.
Restrictions	Only administrator or operator level users can issue this command.

Example usage:

To disable SNTP support:

```
DGS-1100-10/ME:5>disable sntp
Command: disable sntp

Success!
DGS-1100-10/ME:5>
```

config time

Purpose	To manually configure system time and date settings.
Syntax	config time <date> <systemtime>
Description	The config time date command configures the system time and date settings. These will be overridden if SNTP is configured and enabled.
Parameters	<p><i><date></i> – Specifies the date, using two numerical characters for the day of the month, English abbreviation for the name of the month, and four numerical characters for the year. For example: 19jan2011.</p> <p><i><systemtime ></i> – Specifies the system time, using the format hh:mm:ss; that is, two numerical characters each for the hour using a 24-hour clock, the minute and second. For example: 19:42:30.</p>
Restrictions	Only administrator or 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-1100-10/ME:5>config time 09jan2012 15:50:50
Command: config time 09jan2012 15:50:50

Success!
DGS-1100-10/ME:5>
```

config time_zone operator

Purpose	To determine the time zone used in order to adjust the system clock.
Syntax	config time_zone operator [+ hour <gmt_hour 0-13> minute <minute 0-59> - hour <gmt_hour 0-12> minute <minute 0-59>]
Description	The config time_zone operator command adjusts the system clock settings according to the time zone. Time zone settings adjust SNTP information accordingly.
Parameters	<p><i>operator</i> – May be (+) to add or (-) to subtract time to adjust for a time zone relative to GMT.</p> <p><i>hour <gmt_hour 0-13></i> – Specifies the number of hours difference from GMT.</p> <p><i>minute <minute 0-59></i> – Specifies the number of minutes added or subtracted to adjust the time zone.</p>
Restrictions	Only administrator or operator level users can issue this command.

Example usage:

To configure time zone settings:

```
DGS-1100-10/ME:5>config time_zone operator + hour 2 minute 30
Command: config time_zone operator + hour 2 minute 30

Success!
DGS-1100-10/ME:5>
```

config dst

Purpose	To configure time adjustments to allow for the use of Daylight Saving Time (DST).
Syntax	config dst [<i>disable</i> [<i>annual</i> <i>s_date</i> < <i>start_date</i> 1-31> <i>s_mth</i> < <i>start_mth</i> 1-12> <i>s_time</i> < <i>start_time</i> > <i>end_date</i> < <i>int</i> 1-31> <i>e_mth</i> < <i>end_mth</i> 1-12> <i>e_time</i> < <i>end_time</i> > <i>offset</i> [30 60 90 120]]]
Description	The config dst command disables or configures Daylight Saving Time (DST). When enabled, this adjusts the system clock to comply with any DST requirement. DST adjustment affects system time for both manually configured time and time set using SNTP service.
Parameters	<p><i>disable</i> – Disables the DST seasonal time adjustment for the switch.</p> <p><i>annual</i> – Enables DST seasonal time adjustment on an annual basis. Annual mode requires that the DST beginning and ending date be specified concisely. For example, specify to begin DST on April 3 and end DST on October 14. The format for annual mode is as follows, and in the order listed:</p> <ul style="list-style-type: none"> • <i>s_date</i> <<i>start_date</i> 1-31> - The day of the month to begin DST, expressed numerically. • <i>s_mth</i> <<i>start_mth</i> 1-12> - The month of the year to begin DST, expressed numerically. • <i>s_time</i> <<i>start_time</i>> - The time of day to begin DST in hours and minutes, expressed using a 24-hour clock. • <i>end_date</i> <<i>int</i> 1-31> - The day of the month to end DST, expressed numerically. • <i>e_mth</i> <<i>end_mth</i> 1-12> - The month of the year to end DST, expressed numerically. • <i>e_time</i><<i>end_time</i>> - The time of day to end DST, in hours and minutes, expressed using a 24-hour clock. <p><i>offset</i> [30 60 90 120] – Indicates the number of minutes to add during the summertime. The possible offset times are 30, 60, 90, and 120. The default value is 60.</p>
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure daylight savings time on the switch to run from 3PM on Tuesday the 2nd of April until 3:30 PM on Wednesday the 2nd of October and add 30 minutes at the onset of DST:

```
DGS-1100-10/ME:5>config dst annual s_date 2 s_mth 4 s_time 3 end_date 2
e_mth 10 e_time 3 offset 30
Command: config dst annual s_date 2 s_mth 4 s_time 3 end_date 2 e_mth 10
e_time 3 offset 30
```

Success!

```
DGS-1100-10/ME:5>
```

show time

Purpose	To display the current time settings and status.
Syntax	show time
Description	The show time command displays the system time and date configuration, as well as displays the current system time.
Parameters	None.
Restrictions	None.

Example usage:

To show the time currently set on the switch's system clock:

```
DGS-1100-10/ME:5>show time
Command: show time

Time information
-----
Current Time Source           : Local
Current Time                  : 09 Jan 2012 15:56:02
GMT Time Zone offset         : GMT +02:30
Daylight Saving Time Status  : Annual
Offset in Minutes            : 60
Annual From                   : 01 Jan 0:0
To                            : 01 Jan 0:0

DGS-1100-10/ME:5>
```

ARP COMMANDS

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

Command	Parameter
config arp_aging time	<value 0-65535 >
show arpentry	{ interface_Name {System} {static} ip_address <ipaddr>}

Each command is listed in detail, as follows:

config arp_aging time	
Purpose	To configure the age-out timer for ARP table entries on the Switch.
Syntax	config arp_aging time <value 0-65535>
Description	The config arp_aging time command sets the maximum amount of time, in minutes, that an ARP entry can remain in the Switch's ARP table, without being accessed, before it is dropped from the table.
Parameters	<i>time</i> <value 0-65535> – The ARP age-out time, in minutes. The value may be in the range of 0-65535 minutes, with a default setting of 20 minutes.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure ARP aging time:

```
DGS-1100-10/ME:5>config arp_aging time 30
Command: config arp_aging time 30

Success!
DGS-1100-10/ME:5>
```

show arpentry	
Purpose	To displays all ARP entries on the Switch.
Syntax	show arpentry { interface_Name {System} {static} ip_address <ipaddr>}
Description	The show arpentry command displays all ARP entries on the Switch.
Parameters	<i>interface_name {system}</i> – Displays the interface name of ARP entry. <i>ip_address <ipaddr></i> – Displays the IP address of ARP entry.
Restrictions	None.

Example usage:

To display all ARP entries on the Switch:

```
DGS-1100-10/ME:5> show arpentry
Command: show arpentry

ARP Aging Time : 30 min

Interface  IP Address  MAC Address  Type
-----  -
System     10.90.90.99  00:11:6b:66:15:e7  dynamic

Total Entries : 1

DGS-1100-10/ME:5>
```

IPv6 Neighbor Discovery Commands

The IPv6 Neighbor Discovery commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameter
create ipv6 neighbor_cache ipif	System <ipv6_addr> <mac_addr>
delete ipv6 neighbor_cache	[<ipv6_addr> static dynamic all]
show ipv6 neighbor_cache	[ipv6address <ipv6_addr> static dynamic all]
config ipv6 nd ns ipif	System retrans_time <integer 1-3600>
show ipv6 nd	
create ipv6route default	<ipv6addr>
delete ipv6route default	
show ipv6route	
enable ipif_ipv6_link_local_auto System	
disable ipif_ipv6_link_local_auto System	

Each command is listed in detail, as follows:

create ipv6 neighbor_cache ipif

Purpose	Used to add a static neighbor on an IPv6 interface.
Syntax	create ipv6 neighbor_cache ipif System <ipv6_addr> <mac_addr>
Description	This create ipv6 neighbor_cache ipif command is used to add a static neighbor on an IPv6 interface.
Parameters	<ipv6_addr> –The IPv6 address of the neighbor. <mac_addr> –The MAC address of the neighbor.
Restrictions	Only administrator or 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 00:01:02:03:04:05:

```
DGS-1100-10/ME:5>create ipv6 neighbor_cache ipif System 3ffc::1 00:01:02:03:04:05
Command: create ipv6 neighbor_cache ipif System 3ffc::1 00:01:02:03:04:05

Success!
DGS-1100-10/ME:5>
```

delete ipv6 neighbor_cache

Purpose	Used to remove a static neighbor on an IPv6 interface.
Syntax	delete ipv6 neighbor_cache [<ipv6_addr> static dynamic all]
Description	This delete ipv6 neighbor_cache ipif command is used to remove a static neighbor on an IPv6 interface.
Parameters	<p><i><ipv6_addr></i> –The IPv6 address of the neighbor.</p> <p><i>static</i> – Delete matching static entries.</p> <p><i>dynamic</i> – Delete matching dynamic entries.</p> <p><i>all</i> – All entries including static and dynamic entries will be deleted.</p>
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To delete a static neighbor cache entry on the interface System, with an IPv6 address of 3ffc::1:

```
DGS-1100-10/ME:5>delete ipv6 neighbor_cache 3ffc::1
Command: delete ipv6 neighbor_cache 3ffc::1

Success!
DGS-1100-10/ME:5>
```

show ipv6 neighbor_cache

Purpose	Used to display the IPv6 neighbor cache.
Syntax	show ipv6 neighbor_cache [ipv6address <ipv6_addr> static dynamic all]
Description	This show ipv6 neighbor_cache ipif command is used to display the neighbor cache entry for the specified interface. You can display a specific entry, all static entries, all dynamic entries, or all entries.
Parameters	<p><i>ipv6address <ipv6_addr></i> –The IPv6 address of the neighbor.</p> <p><i>static</i> – Display all static neighbor cache entries.</p> <p><i>dynamic</i> – Display all dynamic entries.</p> <p><i>all</i> – Displays all entries including static and dynamic entries.</p>
Restrictions	None.

Example usage:

To show all neighbor cache entries on the switch:

```
DGS-1100-10/ME:5> show ipv6 neighbor_cache ipif all static
Command: show ipv6 neighbor_cache ipif all static

IPv6 Address          Link-layer Addr    State    Interface
-----
Total Entries: 0

DGS-1100-10/ME:5>
```

config ipv6 nd ns ipif

Purpose	Configures the IPv6 ND neighbor solicitation retransmission time. This is the time between the retransmission of neighbor solicitation messages to a neighbor, when either resolving the address or probing the reachability of a neighbor.
Syntax	config ipv6 nd ns ipif System retrans_time <integer 1-3600>
Description	This config ipv6 neighbor_cache ipif command is used to configures the retransmit time of IPv6 ND neighbor solicitation
Parameters	<i>retrans_time <integer 1 - 3600></i> – Neighbor solicitation’s retransmit timer is in milliseconds. It has the same value as the RA <i>retrans_time</i> in the config IPv6 ND RA command. If the <i>retrans_time</i> parameter is configured in one of the commands, the <i>retrans_time</i> value in the other command will also change so that the values in both commands are the same. The range is 1 to 3600.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure the *retrans_time* of IPv6 ND neighbor solicitation to be 100:

```
DGS-1100-10/ME:5>config ipv6 nd ns ipif System retrans_time 100
Command: config ipv6 nd ns ipif System retrans_time 100

Success!
DGS-1100-10/ME:5>
```

show ipv6 nd

Purpose	Used to display information regarding neighbor detection on the switch.
Syntax	show ipv6 nd
Description	This show ipv6 nd command is used to display information regarding neighbor detection on the switch.
Parameters	None.
Restrictions	None.

Example usage:

To show IPv6 ND related configuration:

```
DGS-1100-10/ME:5> show ipv6 nd
Command: show ipv6 nd

Interface Name      : System
NS Retransmit Time  : 1(ms)

DGS-1100-10/ME:5>
```

create ipv6route default

Purpose	Used to create IPv6 route entries to the switch's IP routing table.
Syntax	create ipv6route default <ipv6addr>
Description	This create ipv6route default command is used to create a primary and backup IP route entry to the switch's IP routing table.
Parameters	<ipv6addr> – Specify the IPv6 address to be created.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To add a single static IPv6 entry in IPv6 format:

```
DGS-1100-10/ME:5>create ipv6route default 3ffc::1
Command: create ipv6route default 3ffc::1

Success!
DGS-1100-10/ME:5>
```

delete ipv6route default

Purpose	Used to delete a static IPv6 route entry from the switch's IP routing table.
Syntax	delete ipv6route default
Description	This delete ipv6route default command will delete an existing static IPv6 entry from the switch's IP routing table.
Parameters	None.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To delete a static IPv6 entry from the routing table:

```
DGS-1100-10/ME:5>delete ipv6route default
Command: delete ipv6route default

Success!
DGS-1100-10/ME:5>
```

show ipv6route

Purpose	Used to display IPv6 routes.
Syntax	show ipv6route
Description	This show ipv6route command displays the IPv6 routes.
Parameters	None.
Restrictions	None.

Example usage:

To show IPv6 route:

```
DGS-1100-10/ME:5> show ipv6route
Command: show ipv6route

Prefix      Next Hop          IP Interface      Protocol
Metric
-----      -
::/0        3ffc::1           System            Static
1

Total Entries: 1

DGS-1100-10/ME:5>
```

enable ipif_ipv6_link_local_auto System

Purpose	Used to enable the auto configuration of the link local address when no IPv6 address is configured.
Syntax	enable ipif_ipv6_link_local_auto System
Description	This enable ipif_ipv6_link_local_auto System command will automatically create an IPv6 link local address for the Switch if no IPv6 address has previously been configured.
Parameters	None.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To enable the IP interface IPv6 link-local settings on the switch:

```
DGS-1100-10/ME:5>enable ipif_ipv6_link_local_auto System
Command: enable ipif_ipv6_link_local_auto System

Success!
DGS-1100-10/ME:5>
```

disable ipif_ipv6_link_local_auto System

Purpose	Used to disable the auto configuration of the IPv6 link local address.
Syntax	disable ipif_ipv6_link_local_auto System
Description	This disable ipif_ipv6_link_local_auto System command will disable the automatic creation of an IPv6 link local address for the Switch. Once this command is entered, any previous IPv6 link local address that has been created for the IP interface selected, will be deleted from the switch.
Parameters	None.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To disable the IP interface IPv6 link-local settings on the switch:

```
DGS-1100-10/ME:5>disable ipif_ipv6_link_local_auto System
Command: disable ipif_ipv6_link_local_auto System

Success!
DGS-1100-10/ME:5>
```

BANNER COMMANDS

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

Command	Parameter
config log_save_timing	[log_trigger on_demand time_interval <min 1-65535>]
show log	

Each command is listed in detail, as follows:

config log_save_timing	
Purpose	Used to configure the method of saving logs to the switch's flash memory.
Syntax	config log_save_timing [log_trigger on_demand time_interval <min 1-65535>]
Description	This config log_save_timing command is used to configure the method used in saving logs to the switch's flash memory.
Parameters	<p><i>log_trigger</i> – Users who choose this method will have logs saved to the switch every time a log event occurs on the switch.</p> <p><i>on_demand</i> – Users who choose this method will only save logs when they manually tell the Switch to do so, using the save all or save log command.</p> <p><i>time_interval <min 1-65535></i>– Use this parameter to configure the time interval that will be implemented for saving logs. The logs will be saved every x number of minutes that are configured here.</p>
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure the time interval as every 30 minutes for saving logs:

```
DGS-1100-10/ME:5>config log_save_timing time_interval 30
Command: config log_save_timing time_interval 30

Success!
DGS-1100-10/ME:5>
```

show log

Purpose	Used to show the login banner.
Syntax	show log
Description	This command allows display of the log.
Parameters	None.
Restrictions	None.

Usage Example:

To show the log on the Switch:

```
DGS-1100-10/ME:5> show log
Command: show log

Index  Time                Log Text
-----
  2   Jan  1 00:01:13 2012:CLI-6:Successful login through console port( User:
root )
  1   Jan  1 00:00:18 2012:SYSTEM-2:System started up

DGS-1100-10/ME:5>
```

COMMAND HISTORY LIST COMMANDS

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

Command	Parameter
?	
show command_history	
dir	

Each command is listed in detail, as follows:

?	
Purpose	To display all commands in the Command Line Interface (CLI).
Syntax	?
Description	The ? command displays all of the commands available through the Command Line Interface (CLI).
Parameters	{<command>} – Lists all the corresponding parameters for the specified command, along with a brief description of the command's 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-1100-10/ME:5> ?
Command: ?

USEREXEC commands :
? {<command>}
cable diagnostic port [<portlist 1-10> | all]
clear
clear counters ports <portlist 1-10>
clear ethernet_oam ports [<portlist 1-10> | all] {[ event_log | statistics]}
clear fdb [vlan <vlan_name 20> | port <port 1-10> | all]
clear log
clear port_security_entry port <portlist 1-10>
cmdebug flag ([ip] [icmp] [udp] [rarp] ) {enable| disable}
cmdebug flag fdb ([img] [info] [runtime]) {enable| disable}
cmdebug flag led ([read] [write] [debug] [cli] [watchdog] [path] [error])
{enable|
disable}
cmdebug killme
cmdebug lock msg
cmdebug memory
cmdebug multicast dump
cmdebug private inter mib { enable | disable}
cmdebug sem
cmdebug sig <pid> <sig_id>
cmdebug sli <integer(0-2048)>
cmdebug syscall <command1> [<command2>] [<command3>]
cmdebug task <integer(1-200)> pri <integer(1-99)>
cmdebug tcp <tcb-dump|tcp-trace> <integer(0-2048)>
cmdebug timing add <tag (32)>
cmdebug timing clear
cmdebug timing dump [<tag (32)>]
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a ALL

```

show command_history

Purpose	To display the command history.
Syntax	show command_history
Description	The show command_history command displays the command history.
Parameters	None.
Restrictions	None.

Example usage:

To display the command history:

```
DGS-1100-10/ME:5>show command_history
Command: show command_history

?
show log
show log_save_timing
show log_save_timing

DGS-1100-10/ME:5>
```

dir	
Purpose	To display all commands.
Syntax	dir
Description	The dir command displays all commands.
Parameters	None.
Restrictions	None.

Example usage:

To display all of the commands:

```
DGS-1100-10/ME:5> dir

Available commands :
?          cable      clear      cmdebug
compute    config     create     debug
delete     disable    download   echo
enable     logout     npapi      ping
ping6      reboot     reset      rpc
save       show       traceroute upload

DGS-1100-10/ME:5>
```

ACCESS AUTHENTICATION CONTROL COMMANDS

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

Command	Parameter
create authen_login method_list_name	<string 15>
config authen_login	[default method_list_name <string 15>] method [radius local server_group <string 15> none]
delete authen_login method_list_name	<string 15>
show authen_login	[all default method_list_name <string 15>]
create authen_enable method_list_name	<string 15>
config authen_enable	[default method_list_name <string 15>] method {radius local server_group <string 15> none}
delete authen_enable method_list_name	<string 15>
show authen_enable	[all default method_list_name <string 15>]
enable authen_policy	
disable authen_policy	
show authen_policy	
config authen application	[console http all] [login enable] [default method_list_name <string 15>]
show authen application	
config authen parameter	[attempt <int 1-255> response_timeout <int 0-255>]
show authen parameter	
create authen server_host	[<ipaddr> <ipv6addr>] protocol radius {port <int 1-65535> key <string 254> timeout <int 1-255> retransmit <int 1-255>}
config authen server_host	[<ipaddr> <ipv6addr>] protocol radius {port <int 1-65535> key [<string 254>] timeout <int 1-255> retransmit <int 1-255>}
delete authen server_host	[<ipaddr> <ipv6addr>] protocol radius
show authen server_host	
create authen	<string 15>

Command	Parameter
server_group	
config authn server_group	[<string 15> radius] [add delete] server_host [<ipaddr> <ipv6addr>] protocol radius
delete authn server_group	<string 15>
show authn server_group	{<string 15>}
enable admin	

Each command is listed in detail, as follows:

create authn_login method_list_name	
Purpose	To create a user-defined list of authentication methods for users logging on to the Switch.
Syntax	create authn_login method_list_name <string 15>
Description	The create authn_login method_list_name command creates a list of authentication techniques for the user to login. The Switch can support up to eight method lists, but one is reserved as a default and cannot be deleted. Multiple method lists must be created and configured separately.
Parameters	<string 15> - Defines the <i>method_list_name</i> to be created as a string of up to 15 alphanumeric characters.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To create the method list 'Trinity':

```
DGS-1100-10/ME:5>create authn_login method_list_name Trinity
Command: create authn_login method_list_name Trinity

Success!
DGS-1100-10/ME:5>
```

config authn_login	
Purpose	To configure a user-defined or default <i>method list</i> of authentication methods for user login.
Syntax	config authn_login [default method_list_name <string 15>] method [radius local server_group <string 15> none]
Description	The config authn_login command configures a user-defined or default <i>method list</i> of authentication methods for users logging on to the switch. The sequence of methods implemented in this command affects the authentication result. For example, if a user enters a sequence of methods like <i>tacacs – local</i> , the switch sends an authentication request to the first <i>tacacs</i> host in the server group. If no response comes from the server host, the switch sends an

	<p>authentication request to the second <i>tacacs</i> host in the server group and so on, until the list is exhausted. When the local method is used, the privilege level is dependant on the local account privilege configured on the Switch.</p> <p>Successful login using any of these methods gives the user a 'user' priviledge only. If the user wishes to upgrade his or her status to the administrator level, the user must implement the <i>enable admin</i> command, followed by a previously configured password. (See the <i>enable admin</i> part of this section for more detailed information, concerning the <i>enable admin</i> command.)</p>
Parameters	<p><i>default</i> – The default method list for access authentication, as defined by the user. The user may choose one or more of the following authentication methods:</p> <ul style="list-style-type: none"> ▪ <i>radius</i> - Specifies that the user is to be authenticated using the <i>RADIUS</i> protocol from the remote <i>RADIUS server hosts</i> of the <i>RADIUS server group</i> list. ▪ <i>local</i> - Specifies that the user is to be authenticated using the local <i>user account</i> database on the Switch. ▪ <i>server_group <string 15></i> –Specifies that the user is to be authenticated using the server group <i>account</i> database on the Switch. ▪ <i>none</i> – Specifies that no authentication is required to access the Switch. <p><i>method_list_name <string 15></i> – Specifies a previously created method list name defined by the user. One or more of the following authentication methods may be added to this method list:</p> <ul style="list-style-type: none"> ▪ <i>radius</i> - Specifies that the user is to be authenticated using the <i>RADIUS</i> protocol from a remote <i>RADIUS</i> server. ▪ <i>local</i> - Specifies that the user is to be authenticated using the local <i>user account</i> database on the switch. ▪ <i>server_group <string 15></i> –Specifies that the user is to be authenticated using the server group <i>account</i> database on the switch. ▪ <i>none</i> – Specifies that no authentication is required to access the switch.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure the user defined method list 'Trinity' with authentication methods RADIUS and local, in that order.

```
DGS-1100-10/ME:5>config authen_login method_list_name Trinity method radius local
Command: config authen_login method_list_name Trinity method radius local
```

Success!

```
DGS-1100-10/ME:5>
```

delete authen_login method_list_name

Purpose	To delete a previously configured user defined list of authentication methods for users logging on to the Switch.
Syntax	delete authen_login method_list_name <string 15>

Description	The delete authen_login method_list_name command deletes a list of authentication methods for user login.
Parameters	<string 15> - The previously created <i>method_list_name</i> to delete.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To delete the method list name 'Trinity':

```
DGS-1100-10/ME:5>delete authen_login method_list_name Trinity
Command: delete authen_login method_list_name Trinity

Success!
DGS-1100-10/ME:5>
```

show authen_login

Purpose	To display a previously configured user defined method list of authentication methods for users logging on to the Switch.
Syntax	show authen_login [all default method_list_name <string 15>]
Description	The show authen_login command displays a list of authentication methods for user login.
Parameters	<p><i>default</i> – Displays the default method list for users logging on to the switch.</p> <p><i>method_list_name</i> <string 15> - Specifies the <i>method_list_name</i> to display.</p> <p><i>all</i> – Displays all the authentication login methods currently configured on the switch.</p> <ul style="list-style-type: none"> • Method List Name – The name of a previously configured method list name. • Method Name – Defines which security protocols are implemented, per method list name.
Restrictions	None.

Example usage:

To view all authentication login method list names:

```
DGS-1100-10/ME:5> show authen_login all
Command: show authen_login all
```

Method List Name	Priority	Method Name	Comment
Trinity	1	none	Keyword
Trinity	2	none	Keyword
Trinity	3	none	Keyword
Trinity	4	none	Keyword
default	1	local	Keyword
default	2	none	Keyword
default	3	none	Keyword
default	4	none	Keyword

```
DGS-1100-10/ME:5>
```

create authen_enable method_list_name

Purpose	To create a user-defined method list of authentication methods for promoting normal user level privileges to administrator level privileges on the switch.
Syntax	create authen_enable method_list_name <string 15>
Description	The create authen_enable method_list_name command creates a list of authentication methods for promoting users with normal level privileges to administrator level privileges using authentication methods on the Switch. Once a user acquires normal user level privileges on the switch, he or she must be authenticated by a method on the switch to gain administrator privileges on the switch, which is defined by the administrator. A maximum of eight (8) enable method lists can be implemented on the switch.
Parameters	<string 15> - Defines the <i>authen_enable method_list_name</i> to be created as a string of up to 15 alphanumeric characters.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

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

```
DGS-1100-10/ME:5>create authen_enable method_list_name Permit
Command: create authen_enable method_list_name Permit

Success!
DGS-1100-10/ME:5>
```

config authen_enable

Purpose	To configure a user-defined method list of authentication methods for promoting normal user level privileges to administrator level
---------	---

	privileges on the Switch.
Syntax	config authen_enable [default method_list_name <string 15>] method {radius local server_group <string 15> none}
Description	<p>The config authen_enable command configures a user-defined list of authentication methods for promoting normal user level privileges to administrator level privileges using authentication methods on the switch. Once a user acquires normal user level privileges on the switch, he or she must be authenticated by a method on the switch in order to gain administrator privileges. This is defined by the administrator. A maximum of eight (8) enable method lists can be implemented simultaneously on the switch.</p> <p>The sequence of methods implemented in this command affects the authentication result. For example, if a user enters a sequence of methods like <i>radius – local_enable</i>, the switch sends an authentication request to the first RADIUS host in the server group. If no verification is found, the switch sends an authentication request to the second RADIUS host in the server group and so on, until the list is exhausted. At that point, the switch restarts the same sequence with the following protocol listed, <i>radius</i>. If no authentication takes place using the <i>radius</i> list, the <i>local_enable</i> password set in the switch is used to authenticate the user.</p> <p>Successful authentication using any of these methods gives the user an 'Admin' level privilege.</p>
Parameters	<p><i>default</i> – The default method list for administration rights authentication, as defined by the user. The user may choose one or more of the following authentication methods:</p> <ul style="list-style-type: none"> • <i>radius</i> – Specifies that the user is to be authenticated using the RADIUS protocol from the remote RADIUS <i>server hosts</i> of the RADIUS <i>server group</i> list. • <i>local</i> - Specifies that the user is to be authenticated using the local <i>user account</i> database on the switch. • <i>server_group <string 15></i> – Specifies the server group name for authentication. • <i>none</i> – Specifies that no authentication is required to access the switch. <p><i>method_list_name <string 15></i> – Specifies a previously created <i>authen_enable method_list_name</i>. The user may add one or more of the following authentication methods to this method list:</p> <ul style="list-style-type: none"> • <i>radius</i> - Specifies that the user is to be authenticated using the RADIUS protocol from a remote RADIUS server. • <i>local</i> - Specifies that the user is to be authenticated using the local <i>user account</i> database on the switch. The local enable password of the device can be configured using the 'config admin local_password' command. • <i>server_group <string 15></i> – Specifies that the user is to be authenticated using the server group account database on the switch. • <i>none</i> – Specifies that no authentication is required to access the switch.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure the user defined method list 'Permit' with authentication methods RADIUS and local_enable, in that order.

```
DGS-1100-10/ME:5>config authen_enable method_list_name Trinity method
radius local
Command: config authen_enable method_list_name Trinity method radius local

Success!
DGS-1100-10/ME:5>
```

delete authen_enable method_list_name

Purpose	To delete a user-defined list of authentication methods for promoting normal user level privileges to administrator level privileges on the switch.
Syntax	delete authen_enable method_list_name <string 15>
Description	The delete authen_enable method_list_name command deletes a user-defined list of authentication methods for promoting user level privileges to administrator level privileges.
Parameters	<i><string 15></i> - The previously created <i>authen_enable method_list_name</i> to be deleted.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To delete the user-defined method list 'Permit'

```
DGS-1100-10/ME:5>delete authen_enable method_list_name Permit
Command: delete authen_enable method_list_name Permit

Success!
DGS-1100-10/ME:5>
```

show authen_enable

Purpose	To display the list of authentication methods for promoting normal user level privileges to administrator level privileges on the switch.
Syntax	show authen_enable [all default method_list_name <string 15>]
Description	The show authen_enable command displays a user-defined list of authentication methods for promoting user level privileges to administrator level privileges.
Parameters	<i>default</i> – Displays the default method list for users attempting to gain access to administrator level privileges on the switch. <i>method_list_name <string 15></i> – The <i>method_list_name</i> to be displayed. <i>all</i> – Displays all the authentication login methods currently configured on the switch. The command displays the following parameters:

	<ul style="list-style-type: none"> • Method List Name – The name of a previously configured method list name. • Method Name – Defines which security protocols are implemented, per method list name.
Restrictions	None.

Example usage:

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

```
DGS-1100-10/ME:5>show authen_enable all
Command: show authen_enable all

Method List Name Priority Method Name Comment
-----
default          1      local      Keyword

DGS-1100-10/ME:5>
```

enable authen_policy	
Purpose	To enable the authentication policy on the Switch.
Syntax	enable authen_policy
Description	The enable authen_policy command enables the authentication policy on the Switch.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To enable the authentication policy:

```
DGS-1100-10/ME:5>enable authen_policy
Command: enable authen_policy

Success!
DGS-1100-10/ME:5>
```

disable authen_policy	
Purpose	To disable the authentication policy on the switch.
Syntax	disable authen_policy
Description	The disable authen_policy command disables the authentication policy on the switch.
Parameters	None.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To disable the authentication policy:

```
DGS-1100-10/ME:5>disable authen_policy
Command: disable authen_policy

Success!
DGS-1100-10/ME:5>
```

show authen_policy

Purpose	Used to display the system access authentication policy status on the switch.
Syntax	show authen_policy
Description	The show authen_policy command displays the system access authentication policy status on the switch.
Parameters	None.
Restrictions	None.

Example usage:

To display the system access authentication policy:

```
DGS-1100-10/ME:5>show authen_policy
Command: show authen_policy

Authentication Policy : Disabled
DGS-1100-10/ME:5>
```

config authen application

Purpose	To configure various applications on the switch for authentication using a previously configured method list.
Syntax	config authen application [console http all] [login enable] [default method_list_name <string 15>]
Description	The config authen application command configures switch applications (console, Telnet) for login at the user level and at the administration level (<i>authen_enable</i>), utilizing a previously configured method list.
Parameters	<p><i>application</i> – Specifies the application to configure. One of the following four options may be selected:</p> <ul style="list-style-type: none"> • <i>console</i> – Configures the command line interface login method. • <i>http</i> – Configures the http login method. • <i>all</i> – Configures all applications as (console, Telnet, SSH) login methods. <p><i>login</i> – Configures an application for normal login on the user level, using a previously configured method list.</p> <p><i>enable</i> – Configures an application for upgrading a normal user level</p>

	to administrator privileges, using a previously configured method list. <i>default</i> – Configures an application for user authentication using the default method list. <i>method_list_name</i> <string 15> – Configures an application for user authentication using a previously configured <i>method_list_name</i> .
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure the default method list for the command line interface:

```
DGS-1100-10/ME:5>config authen application http login default
Command: config authen application http login default

Success!
DGS-1100-10/ME:5>
```

show authen application

Purpose	To display authentication methods for the various applications on the switch.
Syntax	show authen application
Description	The show authen application command displays all of the authentication method lists (login, enable administrator privileges) for switch configuration applications (console, Telnet, SSH) currently configured on the switch.
Parameters	None.
Restrictions	None.

Example usage:

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

```
DGS-1100-10/ME:5> show authen application
Command: show authen application

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

DGS-1100-10/ME:5>
```

config authen parameter

Purpose	To enable the user to configure the authentication parameters on the Switch.
Syntax	config authen parameter [attempt <int 1-255> response_timeout <int 0-255>]

Description	The config authen parameter attempt command enables to user to configure authentication parameters on the Switch.
Parameters	<i>attempt</i> <integer 1-255> – Specifies the attempt of authentication parameter on the Switch. The value range is between 1 and 255. <i>response_timeout</i> <integer 0-255> – Specifies the response timeout of authentication parameter on the Switch. The value range is between 0 and 255.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure the default method list for the command line interface:

```
DGS-1100-10/ME:5>config authen parameter attempt 10
Command: config authen parameter attempt 10

Success!
DGS-1100-10/ME:5>
```

show authen parameter

Purpose	To display authentication parameters for the various applications on the switch.
Syntax	show authen parameter
Description	The show authen parameter command displays the authentication parameter on the switch.
Parameters	None.
Restrictions	None.

Example usage:

To display the authentication parameters for all applications on the Switch:

```
DGS-1100-10/ME:5>show authen parameter
Command: show authen parameter

Response Timeout : 30 seconds
User Attempts    : 10 times
DGS-1100-10/ME:5>
```

create authen server_host

Purpose	To create an authentication server host.
Syntax	create authen server_host [<ipaddr> <ipv6addr>] protocol radius {port <int 1-65535> key <string 254> timeout <int 1-255> retransmit <int 1-255>}
Description	The create authen server_host command creates an authentication server host for the RADIUS security protocols on the switch. When a user attempts to access the switch with authentication protocol enabled, the switch sends authentication

	<p>packets to a remote RADIUS server host on a remote host. The RADIUS server host then verifies or denies the request and returns the appropriate message to the switch. More than one authentication protocol can be run on the same physical server host but, remember that RADIUS has separate entities that are not compatible with each other. The maximum supported number of server hosts is 16.</p>
Parameters	<p><i><ipaddr></i> – The IPv4 address of the remote server host to add.</p> <p><i><ipv6addr></i> – The IPv6 address of the remote server host to add.</p> <p><i>protocol radius</i> – Specifies that the server host utilizes the RADIUS protocol.</p> <p><i>port <int 1-65535></i> – The virtual port number of the authentication protocol on a server host. The value must be between 1 and 65535. The default port numbers are 1812 and 1813 for RADIUS servers but the user may set a unique port number for higher security.</p> <p><i>key [<string 254>]</i> – The authentication key can only be shared with a configured RADIUS server. The value is a string of up to 254 alphanumeric characters.</p> <p><i>timeout <int 1-255></i> – The time in seconds the switch waits for the server host to reply to an authentication request. The default value is 5 seconds.</p> <p><i>retransmit <int 1-255></i> – The number of times the device resends an authentication request when the server does not respond. The value is between 1 and 255.</p>
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

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

```
DGS-1100-10/ME:5> create authn server_host 10.1.1.121 protocol radius port
1234 timeout 10 retransmit 5
Command: create authn server_host 10.1.1.121 protocol radius port 1234
timeout10 retransmit 5

Success!
DGS-1100-10/ME:5>
```

config authn server_host

Purpose	To configure a user-defined authentication server host.
Syntax	config authn server_host [<ipaddr> <ipv6addr>] protocol radius {port <int 1-65535> key [<string 254>] timeout <int 1-255> retransmit <int 1-255>}
Description	The config authn server_host command configures a user-defined authentication server host for the RADIUS security protocols on the switch. When a user attempts to access the switch with the authentication protocol enabled, the switch sends authentication packets to a remote RADIUS server host on a remote host. The RADIUS server host then verifies or denies the request and returns the appropriate message to the switch. More than one authentication protocol can be run on the same physical server host but, remember that RADIUS is separate entities and are not compatible with each

Parameters	<p>other. The maximum supported number of server hosts is 16.</p> <p><i><ipaddr></i> – The IPv4 address of the remote server host the user wishes to alter.</p> <p><i><ipv6addr></i> – The IPv6 address of the remote server host the user wishes to alter.</p> <p><i>protocol radius</i> – Specifies that the server host utilizes the RADIUS protocol.</p> <p><i>port <int 1-65535></i> – The virtual port number of the authentication protocol on a server host. The value must be between 1 and 65535. The default port numbers are 1812 and 1813 for RADIUS servers but the user may set a unique port number for higher security.</p> <p><i>key [<string 254>]</i> – The authentication key to be shared with a configured RADIUS server only. The value is a string of up to 254 alphanumeric characters.</p> <p><i>timeout <int 1-255></i> – The time in seconds the switch will wait for the server host to reply to an authentication request. The default value is 5 seconds.</p> <p><i>retransmit <int 1-255></i> – The number of times the device resends an authentication request when the server does not respond. The value is between 1 and 255.</p>
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

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

```
DGS-1100-10/ME:5> config authn server_host 10.1.1.121 protocol radius port
4321 timeout 12 retransmit 4
Command: config authn server_host 10.1.1.121 protocol radius port 4321
timeout 12 retransmit 4

Success!
DGS-1100-10/ME:5>
```

delete authn server_host

Purpose	To delete a user-defined authentication server host.
Syntax	delete authn server_host [<ipaddr> <ipv6addr>] protocol radius
Description	The delete authn server_host command deletes a user-defined authentication server host previously created on the switch.
Parameters	<p><i><ipaddr></i> - The IPv4 address of the remote server host to be deleted.</p> <p><i><ipv6addr></i> - The IPv6 address of the remote server host to be deleted.</p> <p><i>protocol radius</i> – Specifies that the server host utilizes the RADIUS protocol.</p>
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To delete a user-defined RADIUS authentication server host:

```
DGS-1100-10/ME:5>delete authen server_host 10.1.1.121 protocol radius
Command: delete authen server_host 10.1.1.121 protocol radius

Success!
DGS-1100-10/ME:5>
```

show authen server_host	
Purpose	To view a user-defined authentication server host.
Syntax	show authen server_host
Description	<p>The show authen server_host command displays user-defined authentication server hosts previously created on the switch.</p> <p>The following parameters are displayed:</p> <p>IP Address – The IPv4 or IPv6 address of the authentication server host.</p> <p>Protocol – The protocol used by the server host.</p> <p>Port – The virtual port number on the server host. The default value is 49.</p> <p>Timeout - The time in seconds the switch will wait for the server host to reply to an authentication request.</p> <p>Retransmit - The value in the retransmit field denotes how many times the device resends an authentication request.</p> <p>Key - Authentication key to be shared with a configured RADIUS server only.</p>
Parameters	None.
Restrictions	None.

Example usage:

To view authentication server hosts currently set on the Switch:

```
DGS-1100-10/ME:5> show authen server_host
Command: show authen server_host

IP Address : 10.90.90.97
Protocol   : radius
Port       : 10
Timeout    : 2
Retransmit : 5
Key        : kdjfl

Total Entries: 1
DGS-1100-10/ME:5>
```

create authen server_group

Purpose	To create an authentication server host.
Syntax	create authen server_group <string 15>
Description	The create authen server_group command creates an authentication server group for the protocols on the switch.
Parameters	<string 15> – Defines the authentication group name as a string of up to 15 alphanumeric characters.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To create a server group “dlinkgroup”:

```
DGS-1100-10/ME:5>create authen server_group dlinkgroup
Command: create authen server_group dlinkgroup

Success!
DGS-1100-10/ME:5>
```

config authen server_group

Purpose	To configure a user-defined authentication server host.
Syntax	config authen server_group [<string 15> radius] [add delete] server_host [<ipaddr> <ipv6addr>] protocol radius
Description	The config authen server_group command configures a user-defined authentication server group for the RADIUS security protocols on the switch. When a user attempts to access the switch with the authentication protocol enabled, the switch sends authentication packets to a remote RADIUS server group on a remote host. The RADIUS server group then verifies or denies the request and returns the appropriate message to the Switch. More than one authentication protocol can be run on the same physical server host but, remember that RADIUS has separate entities that are not compatible with each other. The maximum supported number of server group is 16.
Parameters	<string 15> – Defines the authentication group name as a string of up to 15 alphanumeric characters. <ipaddr> – The IPv4 address of the remote server group the user wishes to alter. <ipv6addr> – The IPv6 address of the remote server group the user wishes to alter. [add delete] – Specifies if the authentication server host will be added or deleted from the server group. protocol radius – Specifies that the server host utilizes the RADIUS protocol.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure a RADIUS authentication server group:

```
DGS-1100-10/ME:5>config authn server_group dlinkgroup add server_host
10.1.1.121 protocol radius
Command: config authn server_group dlinkgroup add server_host 10.1.1.121
protocol radius

Success!
DGS-1100-10/ME:5>
```

delete authn server_group

Purpose	To delete a user-defined authentication server host.
Syntax	delete authn server_group <string 15>
Description	The delete authn server_group command deletes a user-defined authentication server group previously created on the switch.
Parameters	<string 15> –Specifies the authentication server group name to be deleted.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To delete a user-defined rd1 authentication server group:

```
DGS-1100-10/ME:5>delete authn server_group dlinkgroup
Command: delete authn server_group dlinkgroup

Success!
DGS-1100-10/ME:5>
```

show authn server_group

Purpose	To view a user-defined authentication server group.
Syntax	show authn server_group {<string 15>}
Description	The show authn server_group command displays user-defined authentication server groups previously created on the switch. The following parameters are displayed: Group Name – The name of the server group. IP Address – The IP address of the authentication server group. Protocol – The protocol used by the server group.
Parameters	None.
Restrictions	None.

Example usage:

To view authentication server hosts currently set on the Switch:

```
DGS-1100-10/ME:5> show authen server_group
Command: show authen server_group

Group Name : radius
  IP Address : 10.90.90.97
  Protocol   : radius

Group Name : dlinkgroup

Total Entries: 2
DGS-1100-10/ME:5>
```

enable admin

Purpose	To promote user level privileges up to administrator level privileges.
Syntax	enable admin
Description	The enable admin command enables a user to be granted administrative privileges on to the switch. After logging on to the switch, users have only 'user' level privileges. To gain access to administrator level privileges, the user may enter this command. The system then prompts for an authentication password. Possible authentication methods for this function include TACACS, RADIUS, user defined server groups, local enable (local account on the Switch), or no authentication (none). Because TACACS does not support the enable function, the user must create a special account on the server host which has the username 'enable', and a password configured by the administrator that will support the 'enable' function. This function becomes inoperable when the authentication policy is disabled.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To enable administrator privileges on the switch:

```
DGS-1100-10/ME:5>enable admin
Command: enable admin

Success!
DGS-1100-10/ME:5>
```

POWER SAVING COMMANDS

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

Command	Parameter
config power_saving mode	[hibernation led length_detection port] [enable disable]
config power_saving	[hibernation led [all <portlist>] port [all <portlist 1-10>]] [add delete] time_range1 <range_name 20> time_range2 <range_name 20> {clear_time_range}
show power_saving	{hibernation led length_detection port}

Each command is listed in detail, as follows:

config power_saving mode	
Purpose	To configure the power saving mode on the switch.
Syntax	config power_saving mode [hibernation led length_detection port] [enable disable]
Description	The config power_saving mode command is used to configure the power saving mode on the switch.
Parameters	<p><i>hibernation</i> – Configure the hibernation state to enable or disable. The default value is disabled.</p> <p><i>led</i> – Configure the led state to enable or disable. The default value is disabled.</p> <p><i>length_detection</i> – Configure the length detection state to enable or disable. The default value is disabled.</p> <p><i>port</i> – Configure ports state to be enabled or disabled.</p> <p><i>[enable disable]</i> – Enable or disable the power saving feature.</p>
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure the power saving mode on the switch:

```
DGS-1100-10/ME:5> config power_saving mode port hibernation enable
Command: config power_saving mode port hibernation enable

Success!
DGS-1100-10/ME:5>
```

config power_saving	
Purpose	To configure the power saving on the switch.

Syntax	config power_saving [hibernation led [all <portlist 1-10>] port [all <portlist>]] [add delete] time_range1 <range_name 20> time_range2 <range_name 20> {clear_time_range}
Description	The config power_saving command is used to configure the power saving on the switch.
Parameters	<p><i>hibernation</i> – Configure the hibernation.</p> <p><i>led [all <portlist 1-10>]</i> – Configure the ports for led.</p> <p><i>port</i> – Configure ports.</p> <p><i>[add delete]</i> – Add or delete time range for power saving mode.</p> <p><i>time_range1 <range_name 20></i> – Specifies the time range 1 to be configured.</p> <p><i>time_range2 <range_name 20></i> – Specifies the time range 2 to be configured.</p> <p><i>{clear_time_range}</i> – Clear the time range setting for power saving on the Switch.</p>
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure power saving on the switch:

```
DGS-1100-10/ME:5> config power_saving mode port hibernation enable
Command: config power_saving mode port hibernation enable

Success!
DGS-1100-10/ME:5>
```

show power_saving

Purpose	To display power saving information on the switch.
Syntax	show power_saving {hibernation led length_detection port}
Description	The show power_saving is used to display power saving information.
Parameters	<p><i>hibernation</i> – Display the hibernation state.</p> <p><i>led</i> –Display the led state.</p> <p><i>length_detection</i> –Display the length detection state.</p> <p><i>port</i> –Display ports state.</p>
Restrictions	None.

Example usage:

To display power saving information on the switch:

```
DGS-1100-10/ME:5> show power_saving length_detection
Command: show power_saving length_detection

Length Detection State : Enabled
DGS-1100-10/ME:5>
```

LLDP COMMANDS

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

Command	Parameter
enable lldp	
disable lldp	
config lldp message_tx_interval	<sec 5-32768>
config lldp message_tx_hold_multiplier	<int 2-10>
config lldp reinit_delay	<sec 1-10>
config lldp tx_delay	<sec 1-8192>
show lldp	
show lldp ports	{<portlist 1-10>}
show lldp local_ports	{<portlist 1-10>} {mode[brief normal detailed]}
show lldp remote_ports	{<portlist 1-10>} {mode[brief normal detailed]}
config lldp ports	[<portlist 1-10> all] notification [enable disable]
config lldp ports	[<portlist 1-10> all] admin_status [tx_only rx_only tx_and_rx disable]
config lldp ports	[<portlist 1-10> all] mgt_addr [ipv4 <ipaddr> ipv6 <ipv6addr>] [enable disable]
config lldp ports	[<portlist 1-10> all] basic_tlvs [all {port_description system_name system_description system_capabilities}] [enable disable]
config lldp ports	[<portlist 1-10> all] dot3_tlvs [all link aggregation mac_phy_configuration_status maximum_frame_size] [enable disable]
config lldp ports	[<portlist 1-10> all] dot1_tlv_pvid [disable enable]
config lldp ports	[<portlist 1-10> all] dot1_tlv_protocol_identity eapol [disable enable]
config lldp ports	[<portlist 1-10> all] dot1_tlv_vlan_name [vlan [<vlan_name 20> all] vlanid <vidlist 1-4094>] [disable enable]
show lldp mgt_addr	{ipv4 <ipaddr> ipv6 <ipv6addr>}
show lldp statistics	{ports <portlist 1-10>}

Each command is listed in detail, as follows:

enable lldp	
Purpose	To enable LLDP on the switch.
Syntax	enable lldp

Description	The enable lldp command enables the <i>Link Layer Discovery Protocol</i> (LLDP) on the switch.
Parameters	None
Restrictions	Only administrator or operator–level users can issue this command.

Example usage:

To enable LLDP on the switch:

```
DGS-1100-10/ME:5>enable lldp
Command: enable lldp

Success!
DGS-1100-10/ME:5>
```

disable lldp

Purpose	To disable LLDP on the switch.
Syntax	disable lldp
Description	The disable lldp command disables the <i>Link Discovery Protocol</i> (LLDP) on the switch.
Parameters	None
Restrictions	Only administrator or operator–level users can issue this command.

Example usage:

To disable LLDP on the switch:

```
DGS-1100-10/ME:5>disable lldp
Command: disable lldp

Success!
DGS-1100-10/ME:5>
```

config lldp message_tx_interval

Purpose	To define the lldp message tx interval
Syntax	config lldp message_tx_interval <sec 5-32768>
Description	The config lldp message_tx_interval defines the lldp message interval of the incoming messages.
Parameters	<sec 5-32768> – Defines the message interval time. The range is between 5 and 32768.
Restrictions	Only administrator or operator–level users can issue this command.

Example usage:

To configure LLDP message tx interval on the switch:

```
DGS-1100-10/ME:5>config lldp message_tx_interval 10
Command: config lldp message_tx_interval 10

Success!
DGS-1100-10/ME:5>
```

config lldp message_tx_hold_multiplier

Purpose	To define the lldp hold-multiplier on the switch.
Syntax	config lldp message_tx_hold_multiplier <int 2-10>
Description	The config lldp message_tx_hold_multiplier command specifies the amount of time the receiving device should hold a <i>Link Layer Discovery Protocol</i> (LLDP) packet before discarding it.
Parameters	<i>message_tx_hold_multiplier (int 2-10)</i> – Specifies the hold time to be sent in the LLDP update packets as a multiple of the timer value. (Range: 2-10). The default configuration is 4.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure LLDP Message tx hold multiplier settings:

```
DGS-1100-10/ME:5>config lldp message_tx_hold_multiplier 2
Command: config lldp message_tx_hold_multiplier 2

Success!
DGS-1100-10/ME:5>
```

config lldp reinit_delay

Purpose	To define the lldp reinit-delay on the switch.
Syntax	config lldp reinit_delay <sec 1-10>
Description	The lldp reinit_delay seconds command specifies the minimum time an LLDP port will wait before reinitializing LLDP transmission.
Parameters	<sec 1-10> – Specifies the minimum time in seconds an LLDP port will wait before reinitializing LLDP transmission. The range is 1 – 10 seconds. The default configuration is 2 seconds.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure LLDP reinit delay:

```
DGS-1100-10/ME:5>config lldp reinit_delay 1
Command: config lldp reinit_delay 1

Success!
DGS-1100-10/ME:5>
```

config lldp tx_delay

Purpose	To configure the lldp tx_delay on the switch.
Syntax	config lldp tx_delay <sec 1-8192>
Description	The config lldp tx_delay command specifies the delay between successive LLDP frame transmissions initiated by value/status changes in the LLDP local systems MIB, use the lldp tx_delay command in global configuration mode.
Parameters	<sec 1-8192> – Specifies the minimum time in seconds an LLDP port will wait before reinitializing LLDP transmission. The range is 1 – 8192 seconds. The default configuration is 2 seconds.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure LLDP tx delay:

```
DGS-1100-10/ME:5>config lldp tx_delay 1
Command: config lldp tx_delay 1

Success!
DGS-1100-10/ME:5>
```

show lldp

Purpose	To display the <i>Link Layer Discovery Protocol</i> (LLDP) on the switch.
Syntax	show lldp
Description	The show lldp displays the LLDP configuration on the switch.
Parameters	None.
Restrictions	None.

Example usage:

To show LLDP settings:

```

DGS-1100-10/ME:5> show lldp
Command: show lldp

LLDP System Information
-----
Chassis ID Subtype      : MAC Address
Chassis ID              : DE-AD-BE-EF-01-02
System Name             :
System Description      : DGS-1100-10/ME V1.00.002
System Capabilities     : bridge

LLDP Configurations
-----
LLDP Status             : Enabled
Message Tx Interval    : 10
Message Tx Hold Multiplier : 2
Reinit Delay           : 2
Tx Delay                : 2
DGS-1100-10/ME:5>

```

show lldp ports

Purpose	To display the <i>Link Layer Discovery Protocol</i> (LLDP) ports configuration on the switch.
Syntax	show lldp ports {<portlist 1-10>}
Description	The show lldp ports command displays the information regarding the ports.
Parameters	<portlist 1-10> – A port or range of ports to be displayed.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To show the information for port 1:

```

DGS-1100-10/ME:5> show lldp ports 1
Command: show lldp ports 1

Port ID                : 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 VLAN Name    : <None>
  Enabled Protocol_Identity
  <None>
  MAC/PHY Configuration/Status : Disabled
  Maximum Frame Size   : Disabled

DGS-1100-10/ME:5>

```

show lldp local_ports

Purpose	To display the <i>Link Layer Discovery Protocol</i> (LLDP) configuration that is advertised from a specific port.
Syntax	show lldp local_ports {<portlist 1-10>} {mode[brief normal detailed]}
Description	The show lldp local_ports command displays the configuration that is advertised from a specific port.
Parameters	<portlist 1-10> – A port or range of ports to be displayed. {mode[brief normal detailed]} – defines which mode of information want to be displayed, brief, normal or detailed.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To show the local port information for port 1 with mode brief:

```

DGS-1100-10/ME:5> show lldp local_ports 1 mode brief
Command: show lldp local_ports 1 mode brief

Port ID : 1
-----
Port Id Subtype           : Interface Alias
Port Id                   : Fa0/1
Port Description          :

DGS-1100-10/ME:5>

```

show lldp remote_ports

Purpose	To display information regarding the neighboring devices discovered
---------	---

	using LLDP.
Syntax	show lldp remote_ports {<portlist 1-10>} {mode[brief normal detailed]}
Description	The show lldp remote_ports command displays the information regarding neighboring devices.
Parameters	<portlist 1-10> – A port or range of ports to be displayed. [mode[brief normal detailed]] – defines which mode of information users want to be displayed, brief, normal or detailed.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To show the information for remote ports:

```
DGS-1100-10/ME:5>show lldp remote_ports 1 mode normal
Command: show lldp remote_ports 1 mode normal

Port ID : 1
-----
Remote Entities Count : 0
(NONE)

DGS-1100-10/ME:5>
```

config lldp ports

Purpose	To enable LLDP notification on a port or ports.
Syntax	config lldp ports [<portlist 1-10> all] notification [enable disable]
Description	The config lldp ports notification command defines lldp notification per port on the switch.
Parameters	ports [<portlist 1-10> all] – Specify a port or ports to be configured. notification [enable disable] – defines is notification is enabled or disabled.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure LLDP notification:

```
DGS-1100-10/ME:5>config lldp ports 1-3 notification enable
Command: config lldp ports 1-3 notification enable

Success!
DGS-1100-10/ME:5>
```

config lldp ports

Purpose	To define LLDP admin status on a port or ports.
Syntax	config lldp ports [<portlist 1-10> all] admin_status [tx_only rx_only tx_and_rx disable]
Description	The config lldp ports admin status command defines lldp admin status per port on the switch.

Parameters	<i>[<portlist> all]</i> – Specify a port or ports to be configured. <i>Admin status</i> – defines admin status of ports on the switch Tx- Tx only Rx – Rx only Both – Tx and RX Disable – admin status disabled.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure LLDP admin status

```
DGS-1100-10/ME:5>config lldp ports 2 admin_status disable
Command: config lldp ports 2 admin_status disable

Success!
DGS-1100-10/ME:5>
```

config lldp ports

Purpose	To define LLDP management address advertisement on a port or ports.
Syntax	config lldp ports [<i><portlist 1-10></i> all] <i>mgt_addr</i> [ipv4 <i><ipaddr></i> ipv6 <i><ipv6addr></i>] [<i>enable disable</i>]
Description	The config lldp ports <i>mgt_addr</i> command defines if lldp will advertise the switch's IP address the command is per port on the switch.
Parameters	<i>[<portlist 1-10> all]</i> – Specify a port or ports to be configured. <i>mgt_addr</i> [<i>ipv4 <ipaddr> ipv6 <ipv6addr></i>] – defines wether the management address (IPv4 or IPv6 address) advertisement will be enabled or disabled
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure LLDP management address advertisement

```
DGS-1100-10/ME:5>config lldp ports 1 mgt_addr ipv4 100.1.1.2 enabled
Command: config lldp ports 1 mgt_addr ipv4 100.1.1.2 enabled

Success!
DGS-1100-10/ME:5>
```

config lldp ports

Purpose	To define LLDP management basic TLVs advertisement on a port or ports.
Syntax	config lldp ports [<i><portlist 1-10></i> all] <i>basic_tlvs</i> [all {iport_description system_name system_description system_capabilities}] [<i>enable disable</i>]
Description	The config lldp ports basic TLVs command defines if lldp will advertise the switch's basic TLVs the command is per port on the

	switch.
Parameters	<i>[<portlist 1-10> all]</i> – Specify a port or ports to be configured. <i>Basic TLVs:</i> <i>all</i> – advertisement of all the basic TLVs <i>port description</i> – advertisement of <i>Port description</i> <i>system name</i> – advertisement of <i>system name</i> <i>system description</i> – advertisement of <i>System description</i> <i>system capabilities</i> – advertisement of system capabilities
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure LLDP Basis TLVs

```
DGS-1100-10/ME:5>config lldp ports 1 basic_tlvs all enable
Command: config lldp ports 1 basic_tlvs all enable

Success!
DGS-1100-10/ME:5>
```

config lldp ports

Purpose	To define LLDP management basic TLVs advertisement on a port or ports.
Syntax	config lldp ports [<portlist> all] dot3_tlvs [all link aggregation mac_phy_configuration_status maximum_frame_size] [enable disable]
Description	The config lldp ports dot3 TLVs command defines if lldp will advertise the mac_phy_configuration_status. The command is per port on the switch.
Parameters	<i>[<portlist 1-10> all]</i> – Specify a port or ports to be configured. <i>dot3_tlvs</i> – defines if the advertisement is enabled or disabled. The possible values are: link_aggregation, mac_phy_configuration_status, maximum_frame_size or all.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure LLDP mac_phy_configuration status:

```
DGS-1100-10/ME:5>config lldp ports 2 dot3_tlvs mac_phy_configuration_status
enable
Command: config lldp ports 2 dot3_tlvs mac_phy_configuration_status enable

Success!
DGS-1100-10/ME:5>
```

config lldp ports

Purpose	To define LLDP management basic TLVs advertisement on a port or ports.
Syntax	config lldp ports [<portlist 1-10> all] dot1_tlv_pvid [disable enable]
Description	The config lldp ports dot1 TLVs command defines if lldp will advertise the mac_phy_configuration_status. The command is per port on the switch.

Parameters	<i>[<portlist 1-10> all]</i> – Specify a port or ports to be configured. <i>[enable disable]</i> - Defines if the advertisement is enabled or disabled.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure LLDP TLV PVID:

DGS-1100-10/ME:5>config lldp ports all dot1_tlv_pvid disable Command: config lldp ports all dot1_tlv_pvid disable
Success! DGS-1100-10/ME:5>

config lldp ports

Purpose	To define LLDP management basic TLVs advertisement on a port or ports.
Syntax	config lldp ports [<portlist 1-10> all] dot1_tlv_protocol_identity eapol [disable enable]
Description	The config lldp ports dot1 TLVs command defines if lldp will advertise the mac_phy_configuration_status. The command is per port on the switch.
Parameters	<i>[<portlist 1-10> all]</i> – Specify a port or ports to be configured. <i>dot1_tlv_protocol_identity</i> – Defines if the advertisement is enabled or disabled. The possible value is eapol.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure LLDP ports configuration status:

DGS-1100-10/ME:5>config lldp ports all dot1_tlv_protocol_identity eapol enable Command: config lldp ports all dot1_tlv_protocol_identity eapol enable
Success! DGS-1100-10/ME:5>

config lldp ports

Purpose	To define LLDP management basic TLVs advertisement on a port or ports.
Syntax	config lldp ports [<portlist 1-10> all] dot1_tlv_vlan_name [vlan [<vlan_name 20> all] vlanid <vidlist 1-4094>] [disable enable]
Description	The config lldp ports dot1 TLVs command defines lldp admin status per port on the switch.
Parameters	<i>[<portlist 1-10> all]</i> – Specify a port or ports to be configured. <i>vlan [<vlan_name 20> all]</i> –The name of the VLAN to be configured. <i>dot1_tlv_vlan_name</i> – Defines if the advertisement is enabled or disabled. <i>vlanid <vidlist 1-4094></i> –The vid of the VLAN to be configured.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure LLDP mac_phy_configuration status:

```
DGS-1100-10/ME:5>config lldp ports all dot1_tlv_vlan_name vlanid 1 disable
Command: config lldp ports all dot1_tlv_vlan_name vlanid 1 disable

Success!
DGS-1100-10/ME:5>
```

show lldp mgt_addr

Purpose	To display the <i>Link Layer Discovery Protocol</i> (LLDP) configuration that is advertised from a specific port.
Syntax	show lldp mgt_addr {ipv4 <ipaddr> ipv6 <ipv6addr>}
Description	The show lldp mgt_addr command displays the information regarding the IPv4 or IPv6 address.
Parameters	<i>ipv4 <ipaddr> ipv6 <ipv6addr></i> – Specifies the lldp IPv4 or IPv6 address to be displayed.
Restrictions	None.

Example usage:

To show the LLDP management address advertisement:

```
DGS-1100-10/ME:5> show lldp mgt_addr
Command: show lldp mgt_addr

Address : 1
-----
Subtype           : IPv4
Address           : 10.90.90.90
IF Type          : ifIndex
OID              : 1.3.6.1.2.1.2.2.1.1
Advertising Ports : <NONE>

Address : 2
-----
Subtype           : IPv6
Address           : fe80::dcad:beff:feef:102
IF Type          : ifIndex
OID              : 1.3.6.1.2.1.2.2.1.1
Advertising Ports : <NONE>

Total Address : 2
DGS-1100-10/ME:5>
```

show lldp statistics

Purpose	To display the <i>Link Layer Discovery Protocol</i> (LLDP) statistics for the specified ports.
Syntax	show lldp statistics {ports <portlist 1-10>}
Description	The show lldp statistics command displays the statistics of LLDP on the switch.

Parameters	<i>{ports <portlist 1-10>}</i> – Specifies the ports to be displayed.
Restrictions	None.

Example usage:

To show the LLDP statistics for port 3:

```
DGS-1100-10/ME:5>show lldp statistics ports 3
Command: show lldp statistics ports 3

Port ID : 3
-----
lldpStatsTxPortFramesTotal      : 0
lldpStatsRxPortFramesDiscardedTotal : 0
lldpStatsRxPortFramesErrors     : 0
lldpStatsRxPortFramesTotal      : 0
lldpStatsRxPortTLVsDiscardedTotal : 0
lldpStatsRxPortTLVsUnrecognizedTotal : 0
lldpStatsRxPortAgeoutsTotal     : 0

DGS-1100-10/ME:5>
```

TRAFFIC SEGMENTATION COMMANDS

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

Command	Parameter
config traffic_segmentation	<portlist 1-10> forward_list [null <portlist 1-10>]
show traffic_segmentation	{<portlist 1-10>}

Each command is listed in detail, as follows:

config traffic_segmentation	
Purpose	To configure traffic segmentation on the switch.
Syntax	config traffic_segmentation <portlist 1-10> forward_list [null <portlist 1-10>]
Description	The config traffic_segmentation command configures traffic segmentation on the switch.
Parameters	<portlist 1-10> – A port or a port channel for which the current traffic segmentation configuration on the switch is to be displayed. forward_list – Specifies a port or a port channel to receive forwarded frames from the source ports specified in the portlist, above.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure ports 1~3 to be able to forward frames to port 5:

```
DGS-1100-10/ME:5>config traffic_segmentation 1-3 forward_list 5
Command: config traffic_segmentation 1-3 forward_list 5

Success!
DGS-1100-10/ME:5>
```

show traffic_segmentation	
Purpose	To display the current traffic segmentation configuration on the switch.
Syntax	show traffic_segmentation {<portlist 1-10>}
Description	The show traffic_segmentation command displays the current traffic segmentation configuration on the switch.
Parameters	<portlist 1-10> – A port or a port channel for which the current traffic segmentation configuration on the switch is to be displayed.

Restrictions	None.
--------------	-------

Example usage:

To display the current traffic segmentation configuration on the switch:

```
DGS-1100-10/ME:5> show traffic_segmentation
Command: show traffic_segmentation

Traffic Segmentation Table

Port Forward Portlist
-----
1    1-10
2    1-10
3    1-10
4    1-10
5    1-10
6    1-10
7    1-10
8    1-10
9    1-10
10   1-10

DGS-1100-10/ME:5>
```

ETHERNET OAM COMMANDS

Ethernet OAM (Operations, Administration, and Maintenance) is a data link layer protocol which provides network administrators the ability to monitor the health of the network and quickly determine the location of failing links or fault conditions on point-to-point and emulated point-to-point Ethernet link. The Ethernet OAM commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameter
config ethernet_oam ports (mode)	[all <portlist 1-10>] mode [active passive]
config ethernet_oam ports (state)	[all <portlist 1-10>] state [enable disable]
config ethernet_oam ports (link monitor error symbol)	[all <portlist 1-10>] link_monitor error_symbol {threshold <integer 1-4294967295> window < integer 1000-60000> notify_state [enable disable]}
config ethernet_oam ports (link monitor error frame)	[all <portlist 1-10>] link_monitor error_frame {threshold <integer> window < integer 1000-60000> notify_state [enable disable]}
config ethernet_oam ports (link monitor error frame seconds)	[all <portlist 1-10>] link_monitor error_frame_seconds {threshold < integer 1-4294967295> window < integer 1000-60000> notify_state [enable disable]}
config ethernet_oam ports (link monitor error frame period)	[all <portlist 1-10>] link_monitor error_frame_period {threshold < integer 1-4294967295> window < integer 148810-100000000> notify_state [enable disable]}
config ethernet_oam ports (remote loopback)	[all <portlist 1-10>] remote_loopback [start stop]
config ethernet_oam ports (received remote loopback)	[all <portlist 1-10>] received_remote_loopback [process ignore]
show ethernet_oam ports (status)	[all <portlist 1-10>] status
show ethernet_oam ports (configuration)	[all <portlist 1-10>] configuration
show ethernet_oam ports (statistics)	[all <portlist 1-10>] statistics
show ethernet_oam ports (event log)	[all <portlist 1-10>] event_log {index <value_list}
clear ethernet_oam ports	[all <portlist 1-10>] [event_log] statistics]

Each command is listed in detail, as follows:

config ethernet_oam ports (mode)

Purpose	Used to configure Ethernet OAM mode for ports.
Syntax	config ethernet_oam ports [all <portlist 1-10>] mode [active passive]
Description	The config ethernet_oam ports command is used to configure Ethernet OAM for ports to operate in active or passive mode.
Parameters	<p>The command is used to configure Ethernet OAM for ports to operate in active or passive mode.</p> <p>Port configured in <i>active</i> mode:</p> <ol style="list-style-type: none"> (1) Initiate the exchange of Information OAMPDUs as defined by the discovery state diagram. (2) Active port is permitted to send any OAMPDU while connected to a remote OAM peer entity in active mode. (3) Active port operates in a limited respect if the remote OAM entity is operating in passive mode. (4) Active port should not respond to OAM remote loopback commands and variable requests from a passive peer. <p>Port configured in <i>passive</i> mode:</p> <ol style="list-style-type: none"> (1) Do not initiate the discovery process (2) React to the initiation of the Discovery process by the remote. This eliminates the possibility of passive-to-passive links. (3) Shall not send Variable request or loopback Control OAMPDUs” for describe the active and passive mode.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure port 1 OAM mode to passive:

```
DGS-1100-10/ME:5> config ethernet_oam ports 1 mode passive
Command: config ethernet_oam ports 1 mode passive

Success!
DGS-1100-10/ME:5>
```

config ethernet_oam ports (state)

Purpose	Used to enable or disable Ethernet OAM per port.
Syntax	config ethernet_oam ports [all <portlist 1-10>] state [enable disable]
Description	<p>The config ethernet_oam ports command is used to enable or disable Ethernet OAM function on a per port basis.</p> <p>Enabling OAM initiates OAM discovery on a port. When OAM is enabled on a port in active mode, that port will initiate discovery; if the port is not OAM enabled, the port will not participate in the discovery process.</p>
Parameters	<p><i>[all <portlist 1-10>]</i> – Specifies a range of ports or all ports to be configured.</p> <p><i>state [enable disable]</i> – Specify to enable or disable the OAM function for the listed ports. The default state is disabled.</p>
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To enable Ethernet OAM on port 1:

```
DGS-1100-10/ME:5> config ethernet_oam ports 1 state enable
Command: config ethernet_oam ports 1 state enable

Success!
DGS-1100-10/ME:5>
```

config ethernet_oam ports (link monitor error symbol)

Purpose	Used to configure Ethernet OAM link monitoring symbol error configuration for ports.
Syntax	config ethernet_oam ports [all <portlist 1-10>] link_monitor error_symbol {threshold <integer> window < integer 1000-60000> notify_state [enable disable]}
Description	The config ethernet_oam ports command is used to configure Ethernet OAM link monitoring symbol error for ports. The link monitoring function provides a mechanism to detect and indicate link faults under a variety of conditions. OAM monitors the statistics on the number of frame errors as well as the number of coding symbol errors. When the number of symbol errors is equal to or greater than the specified threshold in a period and the event notification state is enabled, it generates an error symbol period event to notify the remote OAM peer.
Parameters	<i>[all <portlist 1-10>]</i> – Specifies a range of ports or all ports to be configured. <i>threshold <integer></i> – Specify the number of symbol errors in the period that must be equal to or greater than in order for the event to be generated. The default value of the threshold is 1 symbol error. <i>window <integer 1000-60000></i> –The range is 1000 to 60000 ms. The default value is 1000ms. <i>notify_state [enable disable]</i> – Specify to enable or disable event notification. The default state is enabled.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure the error symbol threshold to 2 and period to 1000ms for port 1:

```
DGS-1100-10/ME:5> config ethernet_oam ports 1 link_monitor error_symbol
threshold 2 window 1000 notify_state enable
Command: config ethernet_oam ports 1 link_monitor error_symbol threshold 2
window 1000 notify_state enable

Success!
DGS-1100-10/ME:5>
```

config ethernet_oam ports (link monitor error frame)

Purpose	Used to configure Ethernet OAM link monitoring error frame configuration for ports.
Syntax	config ethernet_oam ports [all <portlist 1-10>] link_monitor error_frame {threshold <integer> window < integer 1000-60000> notify_state [enable disable]}
Description	<p>The config ethernet_oam ports command is used to configure Ethernet OAM link monitoring error frames for ports.</p> <p>Link monitoring function provides a mechanism to detect and indicate link faults under a variety of conditions. OAM monitors the counts of the number of frame errors as well as the number of coding symbol errors. When the number of frame errors is equal to or greater than the specified threshold in a period and the event notification state is enabled, it generates an error frame event to notify the remote OAM peer.</p>
Parameters	<p><i>[all <portlist 1-10>]</i> – Specifies a range of ports or all ports to be configured.</p> <p><i>threshold <integer></i> – Specify the number of frame errors in the period that must be equal to or greater than in order for the event to be generated. The default value is 1 frame error.</p> <p><i>window <integer 1000-60000></i> –The range is 1000 to 60000 ms. The default value is 1000ms.</p> <p><i>notify_state [enable disable]</i> – Specify to enable or disable event notification. The default state is enabled.</p>
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure the error symbol threshold to 2 and period to 1000ms for port 1:

```
DGS-1100-10/ME:5> config ethernet_oam ports 1 link_monitor error_frame
threshold 2 window 1000 notify_state enable
Command: config ethernet_oam ports 1 link_monitor error_frame threshold 2
window 1000 notify_state enable

Success!
DGS-1100-10/ME:5>
```

config ethernet_oam ports (link monitor error frame seconds)	
Purpose	Used to configure Ethernet OAM link monitoring error frame seconds configuration for ports.
Syntax	config ethernet_oam ports [all <portlist 1-10>] link_monitor error_frame_seconds {threshold < integer> window < integer 1000-60000> notify_state [enable disable]}
Description	<p>The config ethernet_oam ports command is used to configure Ethernet OAM link monitoring error frame seconds for ports. An error frame second is one second interval wherein at least one frame error was detected.</p> <p>Link monitoring function provides a mechanism to detect and indicate link faults under a variety of conditions. OAM monitors the counts of the number of frame errors as well as the number of coding symbol errors. When the number of error frame seconds is equal to or greater than the specified threshold in a period and the event notification state is enabled, it generates an error frame seconds summary event to notify the remote OAM peer.</p>
Parameters	<p><i>[all <portlist 1-10>]</i> – Specifies a range of ports or all ports to be configured.</p> <p><i>threshold <integer></i> – Specify the number of error frame seconds in the period that must be equal to or greater than in order for the event to be generated. The default value is 1 frame error.</p> <p><i>window <integer 1000-60000></i> –Specify the period of error frame seconds summary event. The range is 1000ms-60000ms and the default value is 60000 ms.</p> <p><i>notify_state [enable disable]</i> – Specify to enable or disable event notification. The default state is enabled.</p>
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure the error frame seconds threshold to 2 and period to 10000 ms for port 1:

```
DGS-1100-10/ME:5> config ethernet_oam ports 1 link_monitor error_frame
threshold 2 window 10000 notify_state enable
Command: config ethernet_oam ports 1 link_monitor error_frame threshold 2
window 10000 notify_state enable

Success!
DGS-1100-10/ME:5>
```

config ethernet_oam ports (link monitor error frame period)

Purpose	Used to configure Ethernet OAM link monitoring error frame period for ports.
Syntax	config ethernet_oam ports [all <portlist 1-10>] link_monitor error_frame_period {threshold <integer> window <integer 148810-100000000> notify_state [enable disable]}
Description	The config ethernet_oam ports command is used to configure ports Ethernet OAM link monitoring error frame period. Link monitoring function provides a mechanism to detect and indicate link faults under a variety of conditions. OAM monitors the statistics on the number of frame errors as well as the number of coding symbol errors. When the number of error frames is equal to or greater than the specified threshold in a period and the event notification state is enabled, it generates an error frame period event to notify the remote OAM peer.
Parameters	<i>[all <portlist 1-10>]</i> – Specifies a range of ports or all ports to be configured. <i>threshold <integer></i> – Specify the number of error frames in the period that must be equal to or greater than in order for the event to be generated. The default value of threshold is 1 error frame. <i>window <integer 148810-100000000></i> – Specify the period of error frame period event. The period is specified by a number of received frames. The default value is 148810. <i>notify_state [enable disable]</i> – Specify to enable or disable event notification. The default state is enabled.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure the error frame threshold to 10 and period to 1000000 for port 1:

```
DGS-1100-10/ME:5> config ethernet_oam ports 1 link_monitor error_frame_period
threshold 10 window 1000000 notify_state enable
Command: config ethernet_oam ports 1 link_monitor error_frame_period threshold
10 window 1000000 notify_state enable

Success!
DGS-1100-10/ME:5>
```

config ethernet_oam ports (remote loopback)

Purpose	Used to start or stop Ethernet OAM remote loopback mode for the remote peer of the port.
Syntax	config ethernet_oam ports [all <portlist 1-10>] remote_loopback [start stop]
Description	The config ethernet_oam ports command is used to start or stop the remote peer to enter Ethernet OAM remote loopback mode. To start the remote peer to enter remote loopback mode, the port must be in active mode and the OAM connection established. If the local client is already in remote loopback mode, then the command cannot be applied.
Parameters	<i>[all <portlist 1-10>]</i> – Specifies a range of ports or all ports to be

	configured. <i>remote_loopback [start stop]</i> – If start is specified, a request is sent to the remote peer to change to remote loopback mode. If stop is specified, a request is sent to the remote peer to change to normal operation mode.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To start remote loopback on port 1 of unit 1:

```
DGS-1100-10/ME:5> config ethernet_oam ports 1 remote_loopback start
Command: config ethernet_oam ports 1 remote_loopback start

Success!
DGS-1100-10/ME:5>
```

config ethernet_oam ports (received remote loopback)	
Purpose	Used to configure the method to process the received Ethernet OAM remote loopback command.
Syntax	config ethernet_oam ports [all <portlist 1-10>] received_remote_loopback [process ignore]
Description	The config ethernet_oam ports command is used to configure the client to process or to ignore a received Ethernet OAM remote loopback command. In remote loopback mode, user traffic is not forwarded on the port. If ignore is specified for received_remote_loopback, the specified port will ignore all requests to transition to remote loopback mode and prevent the switch from entering remote loopback mode, and so it will continue to process user traffic regardless.
Parameters	<i>[all <portlist 1-10>]</i> – Specifies a range of ports or all ports to be configured. <i>received_remote_loopback [process ignore]</i> – Specifies whether to process or ignore the received Ethernet OAM remote loopback command. The default method is “ignore”.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure the method of processing the received remote loopback command as “process” on port 1:

```
DGS-1100-10/ME:5> config ethernet_oam ports 1 received_remote_loopback process
Command: config ethernet_oam ports 1 received_remote_loopback process

Success!
DGS-1100-10/ME:5>
```

show ethernet_oam ports (status)

Purpose	Used to display primary controls and status information for Ethernet OAM per port.
Syntax	show ethernet_oam ports [all <portlist 1-10>] status
Description	<p>The show ethernet_oam ports command is used to show primary controls and status information for Ethernet OAM on specified ports. The information includes:</p> <p>(1) OAM administration status: enabled or disabled</p> <p>(2) OAM operation status. It maybe the below value:</p> <p><input type="checkbox"/> Disable: OAM is disabled on this port</p> <p><input type="checkbox"/> LinkFault: The link has detected a fault and is transmitting OAMPDUs with a link fault indication.</p> <p><input type="checkbox"/> PassiveWait: The port is passive and is waiting to see if the peer device is OAM capable.</p> <p>ActiveSendLocal: The port is active and is sending local information</p> <p><input type="checkbox"/> SendLocalAndRemote: The local port has discovered the peer but has not yet accepted or rejected the configuration of the peer.</p> <p><input type="checkbox"/> SendLocalAndRemoteOk: The local device agrees the OAM peer entity.</p> <p><input type="checkbox"/> PeeringLocallyRejected: The local OAM entity rejects the remote peer OAM entity.</p> <p><input type="checkbox"/> PeeringRemotelyRejected: The remote OAM entity rejects the local device.</p> <p><input type="checkbox"/> Operational: The local OAM entity learns that both it and the remote OAM entity have accepted the peering.</p> <p><input type="checkbox"/> NonOperHalfDuplex: Since Ethernet OAM functions are not designed to work completely over half-duplex port. This value indicates Ethernet OAM is enabled but the port is in half-duplex operation.</p> <p>(3) OAM mode: passive or active</p> <p>(4) Maximum OAMPDU size: The largest OAMPDU that the OAM entity supports. OAM entities exchange maximum OAMPDU sizes and negotiate to use the smaller of the two maximum OAMPDU sizes between the peers.</p> <p>(5) OAM configuration revision: The configuration revision of the OAM entity as reflected in the latest OAMPDU sent by the OAM entity. The config revision is used by OAM entities to indicate that configuration changes have occurred, which might require the peer OAM entity to re-evaluate whether OAM peering is allowed.</p> <p>(6) OAM Functions Supported: The OAM functions supported on this port. These functions include:</p> <p><input type="checkbox"/> Unidirectional: It indicates that the OAM entity supports the transmission of OAMPDUs on links that are operating in unidirectional mode (traffic flowing in one direction only).</p> <p><input type="checkbox"/> Loopback: It indicates that the OAM entity can initiate and respond to loopback commands.</p> <p><input type="checkbox"/> Link Monitoring: It indicates that the OAM entity can send and receive Event Notification OAMPDUs.</p> <p><input type="checkbox"/> Variable: It indicates that the OAM entity can send and receive variable requests to monitor the attribute value as described in the IEEE 802.3 Clause 30 MIB.</p> <p>(7) Loopback Status: The current status of the loopback function of the port:</p> <p><input type="checkbox"/> No Loopback – The local and remote ports are not in loopback</p>

	mode.
	<input type="checkbox"/> Initiating Loopback – The local port has sent the start remote loopback request to the peer and is waiting for response.
	<input type="checkbox"/> Remote Loopback – This indicates that both the local and remote ports entered the loopback mode. Any non-OAM packet received in the local port will be dropped.
	<input type="checkbox"/> Local Loopback – This indicates that both the local and remote ports entered the loopback mode. The local port is doing the loopback. Any non-OAM packets received on the port will be sent back to the same port.
	<input type="checkbox"/> Terminate Loopback - The port is stopping loopback on the port.
Parameters	<i>[all <portlist 1-10>]</i> – Specifies a range of ports or all ports to display status.
Restrictions	None.

Example usage:

To show OAM control and status information on port 3:

```
DGS-1100-10/ME:5> show ethernet_oam ports 3 status
Command: show ethernet_oam ports 3 status

Port 3
Local Client
-----
OAM                : Disabled
Mode               : Passive
Max OAMPDU        : 1518
Remote Loopback   : Support
Unidirection      : Not Supported
Link Monitoring    : Support
Variable Request  : Support
PDU Revision      : 0
Operation Status  : Disabled
Loopback Status   : No Loopback

Remote Client
-----
Mode               : Unknown
MAC Address       : 00:00:00:00:00:00
Vendor (OUI)     : 00:00:00
```

show ethernet_oam ports (configuration)

Purpose	Used to display Ethernet OAM configuration per port.
Syntax	show ethernet_oam ports [all <portlist 1-10>] configuration
Description	The show ethernet_oam ports command is used to view Ethernet OAM configurations for ports.
Parameters	<i>[all <portlist 1-10>]</i> – Specifies a range of ports or all ports to display status.
Restrictions	None.

Example usage:

To show Ethernet OAM configuration on port 3:

```
DGS-1100-10/ME:5> show ethernet_oam ports 3 configuration
Command: show ethernet_oam ports 3 configuration

Port 3
-----
OAM                : Disabled
Mode               : Passive
Critical Event     : Enabled
Remote Loopback OAMPDU : Not Processed

Symbol Error
Notify State       : Enabled
Window            : 1000
Threshold         : 23

Frame Error
Notify State       : Enabled
Window            : 1000
Threshold         : 1

Frame Period Error
Notify State       : Enabled
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a ALL
```

show ethernet_oam ports (statistics)

Purpose	Used to display Ethernet OAM statistics for ports.
Syntax	show ethernet_oam ports [all <portlist 1-10>] statistics
Description	The show ethernet_oam ports command is used to display Ethernet OAM ports statistics information.
Parameters	<i>[all <portlist 1-10>]</i> – Specifies a range of ports or all ports to display status.

Restrictions	None.
--------------	-------

Example usage:

To show Ethernet OAM statistics on port 2:

```
DGS-1100-10/ME:5> show ethernet_oam ports 2 statistics
```

```
Command: show ethernet_oam ports 2 statistics
```

```
Port 2
```

```
-----
Information OAMPDU Tx           : 0
Information OAMPDU Rx           : 0
Unique Event Notification OAMPDU Tx : 0
Unique Event Notification OAMPDU Rx : 0
Duplicate Event Notification OAMPDU Tx: 0
Duplicate Event Notification OAMPDU Rx: 0
Loopback Control OAMPDU Tx      : 0
Loopback Control OAMPDU Rx      : 0
Variable Request OAMPDU Tx      : 0
Variable Request OAMPDU Rx      : 0
Variable Response OAMPDU Tx     : 0
Variable Response OAMPDU Rx     : 0
Organization Specific OAMPDU Tx : 0
Organization Specific OAMPDU Rx : 0
Unsupported OAMPDU Tx           : 0
Unsupported OAMPDU Rx           : 0
Frames Lost Due To OAM          : 0
```

```
DGS-1100-10/ME:5>
```

show ethernet_oam ports (event log)

Purpose	Used to display Ethernet OAM event log.
Syntax	show ethernet_oam ports [<i>all</i> <i><portlist 1-10></i>] event_log { <i>index <value_list></i> }
Description	The show ethernet_oam ports command is used to view ports Ethernet OAM event log information. The Switch can buffer 1000 event logs. The event log is different from sys-log. It provides more detailed information than sys-log. Each OAM event will be recorded in both OAM event log and syslog. Specify an index to show a range of events.
Parameters	<i>[all <portlist 1-10>]</i> – Specifies a range of ports or all ports to display status. <i>index <value_list></i> – Specifies an index range to display.
Restrictions	None.

Example usage:

To show Ethernet OAM event log on port 1:

```
DGS-1100-10/ME:5> show ethernet_oam ports 1 event_log index 2
Command: show ethernet_oam ports 1 event_log index 2

Port 1
-----
Event Listing:
Index Type          Location Time Stamp      Value  Window
  Threshold Accumulated errors
-----
DGS-1100-10/ME:5>
```

clear ethernet_oam ports

Purpose	Used to clear Ethernet OAM port statistics or event log.
Syntax	clear ethernet_oam ports [all <portlist 1-10>] [event_log statistics]
Description	The clear ethernet_oam ports command is used to clear Ethernet OAM ports statistics or event log information.
Parameters	<i>[all <portlist>]</i> – Specifies a range of ports or all ports to clear OAM statistics or event log. <i>[event_log statistics]></i> – Specifies an index range to display.
Restrictions	None.

Example usage:

To clear port 1 OAM statistics:

```
DGS-1100-10/ME:5> clear ethernet_oam ports 1 statistics
Command: clear ethernet_oam ports 1 statistics

Success!
DGS-1100-10/ME:5>
```

SAFEGUARD COMMANDS

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

Command	Parameter
config safeguard_engine	state [enable disable]
show safeguard_engine	

Each command is listed in detail, as follows:

config safeguard_engine	
Purpose	To define the safeguard engine on the switch.
Syntax	config safeguard_engine state [enable disable]
Description	To define the safeguard_engine on the switch.
Parameters	<i>state [enable disable]</i> – enable and disable Safeguard engine on the switch.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To enable the safeguard engine on the switch:

```
DGS-1100-10/ME:5>config safeguard_engine state enable
Command: config safeguard_engine state enable

Success!
DGS-1100-10/ME:5>
```

show safeguard_engine	
Purpose	To show the safeguard engine status on the switch.
Syntax	show safeguard_engine
Description	To show the safeguard engine on the switch.
Parameters	None.
Restrictions	None.

Example usage:

To show the safeguard engine status on the switch:

```
DGS-1100-10/ME:5> show safeguard_engine
Command: show safeguard_engine

Safeguard Engine State      : Enable

DGS-1100-10/ME:5>
```