D-Link

D-Link™ DGS-2000 Ver.A1

Managed Access Switch

CLI Reference Guide

V1.0

Information in this document is subject to change without notice.

© 2020 D-Link Computer Corporation. All rights reserved.

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

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

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

FCC Warning

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

CE Mark Warning

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

Warnung!

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

Precaución!

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

Attention!

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

Attenzione!

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

VCCI Warning

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

Table of Contents

INTRODUCTION **1**

USING THE COMMAND LINE INTERFACE **2**

COMMAND SYNTAX **6**

BASIC SWITCH COMMANDS **8**

enable clipaging 9
disable clipaging 10
enable password encryption 10
disable password encryption 10
config terminal length 11
config terminal width 11
show terminal 12
create account 12
config account 13
show account 14
reset account 14
reset password 15
delete account 15
show switch 16
show firmware information 16
enable web 17
disable web 18
enable telnet 18
disable telnet 18
show session 19
show config 19
enable jumbo_frame 20
disable jumbo_frame 21
show jumbo_frame 21
save 21
reboot 22
reset 22
logout 23
ping 23
ping6 24
config time_range 24
show time_range 25
enable ssh 26
disable ssh 26
enable telnet 27
disable telnet 27
telnet 27
traceroute 28
show cpu port 29

reset cpu port 29
MODIFY BANNER AND PROMPT COMMANDS 31
config command_prompt 31
config greeting_message 32
show greeting_message 33
SWITCH PORT COMMANDS 34
config ports 34
show ports 35
enable auto learning 36
disable auto learning 36
config duld ports 37
show duld ports 38
SPANNING TREE COMMANDS 39
enable loopdetect 39
enable stp 40
disable stp 40
config stp 40
config stp ports 41
config stp version 43
config stp fbpdu 43
config stp priority 44
show stp 44
show stp ports 45
create stp instance_id 45
delete stp instance_id 46
config stp instance_id 46
show stp instance 47
config stp mst_config_id 48
config stp mst_ports 48
show stp mst_config_id 49
config stp nni_bpdu_addr 50
LOOPBACK DETECTION COMMANDS 51
enable loopdetect 51
disable loopdetect 51
config loopdetect mode 52
config loopdetect ports 52
config loopdetect 53
config loopdetect vlan 53
show loopdetect 54
PPPOE CIRCUIT ID INSERTION COMMANDS 55
config pppoe circuit_id_insertion state 55
config pppoe circuit_id_insertion ports 56
show pppoe circuit_id_insertion 56
show pppoe circuit_id_insertion ports 57
NETWORK MANAGEMENT (SNMP) COMMANDS 58

enable snmp 59
disable snmp 60
show snmp global state 60
create snmp user 60
delete snmp user 61
show snmp user 61
create snmp view 62
delete snmp view 63
show snmp view 63
create snmp community 64
create snmp community_masking 64
delete snmp community 65
delete snmp all_community 65
show snmp community 66
create snmp group 67
delete snmp group 68
show snmp groups 68
create snmp host 69
create snmp v6host 70
delete snmp host 71
show snmp host 72
config snmp engineID 72
show snmp engineID 73
config snmp traps 73
show snmp traps 74
config snmp system_location 75
config snmp system_name 75
config snmp system_contact 75
enable community_encryption 76
disable community_encryption 76
show community_encryption 77
DOWNLOAD/UPLOAD COMMANDS 78
download 78
upload 79
DHCP AUTO COMMANDS 81
enable autoconfig 81
disable autoconfig 82
config autoconfig timeout 82
show autoconfig 82
enable autoimage 83
disable autoimage 84
show autoimage 84
DHCP RELAY COMMANDS 85
enable dhcp_relay 86
disable dhcp_relay 86
config dhcp_relay 86
config dhcp_relay hops 87

config dhcp_relay time 87
config dhcp_relay vlan 88
config dhcp_relay port 88
config dhcp_relay option_82 89
show dhcp_relay 90
enable dhcp_local_relay 90
disable dhcp_local_relay 91
config dhcp_local_relay vlan 91
config dhcp_local_relay port 92
show dhcp_local_relay 92
enable dhcpv6_relay 93
disable dhcp6_relay 93
config dhcpv6_relay 93
config dhcpv6_relay hop_count 94
config dhcpv6_relay option_37 94
show dhcpv6_relay 95
NETWORK MONITORING COMMANDS 96
show packet ports 97
show statistics ports 98
show error ports 98
show utilization 99
clear counters 100
clear log 100
show log 100
save log 101
config log_save_timing 101
show log_save_timing 102
enable command logging 102
disable command logging 103
show command logging 103
show log_software_module 103
enable syslog 104
disable syslog 104
create syslog host 105
config syslog host 107
delete syslog host 109
show syslog host 109
cable diagnostic port 110
FORWARDING DATABASE COMMANDS 111
create fdb 111
delete fdb 112
config fdb aging_time 112
show fdb 113
clear fdb 114
create multicast_fdb 114
config multicast_fdb 115
delete multicast_fdb 115

show multicast_fdb 116
config multicast filter 116
show multicast filter port_mode 117
enable flood_fdb 117
disable flood_fdb 117
config flood_fdb 118
show flood_fdb 118
clear flood_fdb 119
create auto_fdb 119
delete auto_fdb 120
show auto_fdb 120
BROADCAST STORM CONTROL COMMANDS 121
config traffic control 121
config traffic control 122
config traffic control auto_recover_time 123
show traffic control 123
QOS COMMANDS 125
config bandwidth_control 125
show bandwidth_control 126
config qos mode 127
show qos mode 127
config scheduling_mechanism 127
show scheduling_mechanism 128
config 802.1p default_priority 128
show 802.1p default_priority 129
show 802.1p user_priority 129
show scheduling 130
config dscp_mapping 131
show dscp_mapping 131
RMON COMMANDS 132
enable rmon 132
disable rmon 133
create rmon alarm 133
delete rmon alarm 134
create rmon collection stats 134
delete rmon collection stats 135
create rmon collection history 135
delete rmon collection history 136
create rmon event 136
delete rmon event 137
show rmon 137
PORT MIRRORING COMMANDS 139
enable mirror 139
disable mirror 139
create mirror id 140
config mirror 140

show mirror 141
VLAN COMMANDS 142
create vlan 142
delete vlan 143
config vlan 143
show vlan 144
enable asymmetric_vlan 144
disable asymmetric_vlan 145
show asymmetric_vlan 145
config port_vlan 146
show port_vlan pvid 146
enable pvid auto_assign 147
disable pvid auto_assign 147
show pvid auto_assign 147
Q-IN-Q COMMANDS 149
enable qinq 149
disable qinq 150
show qinq 150
config qinq ports 151
config qinq inner_tpid 151
show qinq inner_tpid 152
create vlan_translation 152
show vlan_translation 152
delete vlan_translation ports 153
INTERFACE AND IP COMMANDS 154
create ipif 154
config ipif 155
show ipif 156
enable ipif 156
disable ipif 156
delete ipif 157
create iproute 157
delete iproute 158
show iproute 158
create ipv6route 159
delete ipv6route 160
show ipv6route 160
IPV6 NEIGHBOR DISCOVERY COMMANDS 162
create ipv6 neighbor_cache ipif 162
delete ipv6 neighbor_cache 163
show ipv6 neighbor_cache 163
config ipv6 nd ns ipif 164
show ipv6 nd ipif 164
enable ipif_ipv6_link_local_auto 164
disable ipif_ipv6_link_local_auto 165
MAC NOTIFICATION COMMANDS 166

enable mac_notification 166
disable mac_notification 166
config mac_notification 167
config mac_notification ports 167
show mac_notification 168
show mac_notification ports 168
IGMP SNOOPING COMMANDS 170
enable igmp_snooping 171
disable igmp_snooping 171
config igmp_snooping 172
config igmp_snooping querier 173
create igmp_snooping static_group 174
config igmp_snooping static_group 174
delete igmp_snooping static_group 175
show igmp_snooping static_group 175
config igmp_snooping data_driven_learning 176
config igmp_snooping data_driven_learning max_learning_entry 177
clear igmp_snooping data_driven_group 177
config router_ports 178
config router_ports_forbidden 178
show router_ports 179
config igmp access_authentication ports 180
show igmp access_authentication ports 180
show igmp_snooping 181
show igmp_snooping group 182
show igmp_snooping forwarding 182
show igmp_snooping host 183
show igmp_snooping statistic counter 183
clear igmp_snooping statistic counter 184
config igmp_snooping rate_limit 185
config igmp_snooping v3_src_filter 185
show igmp_snooping v3_src_filter 186
MLD SNOOPING COMMANDS 187
enable mld_snooping 188
disable mld_snooping 188
config mld_snooping 188
config mld_snooping querier 189
config mld_snooping data_driven_learning 190
config mld_snooping data_driven_learning max_learned_entry 191
clear mld_snooping data_driven_group 192
config mld_snooping mrouter_ports 192
config mld_snooping mrouter_ports_forbidden 193
show mld_snooping mrouter_ports 193
show mld_snooping 194
show mld_snooping group 195
show mld_snooping forwarding 195
show mld_snooping host 196

show mld_snooping statistics counter 196
clear mld_snooping statistics counter 197
config mld_snooping v3_src_filter 197
show mld_snooping v3_src_filter 198
MULTICAST VLAN COMMANDS 199
enable igmp_snooping multicast_vlan 200
disable igmp_snooping multicast_vlan 200
create igmp_snooping multicast_vlan 200
config igmp_snooping multicast_vlan 201
delete igmp_snooping multicast_vlan 202
show igmp_snooping multicast_vlan 202
config igmp_snooping multicast_vlan_group 203
show igmp_snooping multicast_vlan_group 203
enable mld_snooping multicast_vlan 204
disable mld_snooping multicast_vlan 204
create mld_snooping multicast_vlan 205
config mld_snooping multicast_vlan 205
delete mld_snooping multicast_vlan 206
show mld_snooping multicast_vlan 206
config mld_snooping multicast_vlan_group 207
show mld_snooping multicast_vlan_group 208
LIMITED IP MULTICAST ADDRESS COMMANDS 209
create mcast_filter_profile 209
config mcast_filter_profile 210
config mcast_filter_profile ipv6 210
delete mcast_filter_profile 211
show mcast_filter_profile 211
config limited_multicast_addr ports 212
show limited_multicast_addr ports 213
config max_mcast_group ports 213
show max_mcast_group ports 214
802.1X COMMANDS 215
enable 802.1x 216
disable 802.1x 216
show 802.1x 217
show 802.1x auth_state 217
show 802.1x auth_configuration 218
config 802.1x auth_parameter ports 219
config 802.1x init 220
config 802.1x auth_protocol 221
config 802.1x reauth 221
config radius add 222
config radius delete 223
config radius 223
show radius 224
config 802.1x fwd_pdu system 224
show 802.1x fwd_pdu system status 225

config 802.1x auth_mode 225
create 802.1x guest_vlan 226
delete 802.1x guest_vlan 226
config 802.1x guest_vlan ports 227
show 802.1x guest_vlan 227
create 802.1x user 228
show 802.1x user 228
delete 802.1x user 229
config 802.1x capability ports 229
PORT SECURITY COMMANDS 231
config port_security 231
show port_security 232
delete port_security _entry 233
clear port_security _entry 233
TIME AND SNTP COMMANDS 234
enable sntp 234
disable sntp 235
config sntp 235
show sntp 235
config time 236
config time_zone operator 236
config dst 237
show time 238
ARP COMMANDS 239
create arpentry 239
config arpentry 239
delete arpentry 240
show arpentry 240
clear arptable 241
config arp_aging time 241
show arpentry aging_time 242
COMMAND HISTORY LIST COMMANDS 243
? 243
config command_history 245
show command_history 245
ACCESS CONTROL LIST COMMANDS 246
create access_profile ethernet 248
config access_profile 249
create access_profile ip 250
config access_profile 252
create access_profile ipv6 254
config access_profile profile_id 255
create access_profile packet_content_mask 257
config access_profile profile_id 258
delete access_profile 259
config access_profile profile_id 260

show access_profile 260
create cpu_access_profile ethernet 261
config cpu_access_profile profile_id 262
create cpu_access_profile ip 263
config cpu_access_profile profile_id 264
create cpu_access_profile ipv6 265
config cpu_access_profile profile_id 266
create cpu_access_profile packet_content 266
config cpu_access_profile profile_id 267
delete cpu_access_profile 269
config cpu_access_profile profile_id 269
show cpu_access_profile 269
ACCESS AUTHENTICATION CONTROL COMMANDS 271
create authen_login method_list_name 272
config authen_login 272
delete authen_login method_list_name 274
show authen_login 274
show authen_policy 275
create authen_enable method_list_name 275
config authen_enable 276
delete authen_enable method_list_name 277
show authen_enable 278
enable authen_policy 278
disable authen_policy 279
config authen application 279
show authen application 280
config authen parameter 281
show authen parameter 281
create authen server_host 281
config authen server_host 283
delete authen server_host 284
show authen server_host 284
create authen server_group 285
config authen server_group 286
delete authen server_group 287
show authen server_group 287
enable admin 288
config admin local_enable 288
POWER SAVING COMMANDS 290
config power_saving mode 290
config power_saving 290
show power_saving 291
ENERGY EFFICIENT ETHERNET COMMANDS 292
config EEE port 292
show EEE_mode port 292
LLDP COMMANDS 294

enable lldp 295
disable lldp 295
config lldp message_tx_interval 295
config lldp message_tx_hold_multiplier 296
config lldp reinit_delay 296
config lldp tx_delay 297
config lldp notification_interval 297
show lldp 298
show lldp ports 298
show lldp local_ports 299
show lldp remote_ports 300
config lldp ports 300
show lldp mgt_addr 305
show lldp statistics 306
show lldp power_pse_tlv 306
TRAFFIC SEGMENTATION COMMANDS 308
config traffic_segmentation 308
show traffic_segmentation 308
ETHERNET OAM COMMANDS 310
config ethernet_oam ports (mode) 311
config ethernet_oam ports (state) 312
config ethernet_oam ports (remote loopback) 312
config ethernet_oam ports (received remote loopback) 313
config ethernet_oam ports (link monitor error symbol) 314
config ethernet_oam ports (link monitor error frame) 315
config ethernet_oam ports (link monitor error frame seconds) 316
config ethernet_oam ports (link monitor error frame period) 317
show ethernet_oam ports (status) 318
show ethernet_oam ports (configuration) 319
show ethernet_oam ports (statistics) 320
show ethernet_oam ports (event log) 321
clear ethernet_oam ports 322
SAFEGUARD COMMANDS 323
config safeguard_engine 323
show safeguard_engine 323
LINK AGGREGATION COMMANDS 325
create link_aggregation 325
delete link_aggregation 326
config link_aggregation group_id 326
config lacp port_priority 327
config lacp_ports 328
show lacp 328
VOICE VLAN COMMANDS 330
enable voice_vlan 330
disable voice_vlan 331
config voice_vlan aging_time 331

config voice_vlan priority 332
config voice_vlan oui 332
config voice_vlan ports 333
config voice_vlan log state 334
show voice_vlan 335
AUTO SURVEILLANCE VLAN COMMANDS 337
enable surveillance_vlan 337
disable surveillance_vlan 338
config surveillance_vlan aging_time 338
config surveillance_vlan priority 339
config surveillance_vlan oui 339
config surveillance_vlan onvif_discover_port 340
config surveillance_vlan onvif_ipc 340
config surveillance_vlan onvif_nvr 341
config surveillance_vlan ports 341
config surveillance_vlan log state 342
show surveillance_vlan 342
D-LINK DISCOVER PROTOCOL COMMANDS 344
enable ddp 344
disable ddp 344
config ddp report state 345
config ddp report_timer 345
config ddp ports 346
show ddp 346
DIGITAL DIAGNOSTIC MONITORING COMMANDS 348
config ddm ports 348
config ddm power_unit 349
show ddm ports 349
IPV4/IPV6 ROUTING COMMANDS 351
create iproute 351
delete iproute 352
show iproute 352
create ipv6route 353
delete ipv6route 353
show ipv6route 354
IP-MAC-PORT BINDING COMMANDS 355
create address_binding ip_mac 355
config address_binding ip_mac ports 356
config address_binding auto_scan 357
config address_binding auto_scan ipv6address 357
delete address_binding 358
show address_binding 358
show address_binding auto_scan list 359
enable address_binding dhcp_snoop 360
disable address_binding dhcp_snoop 360
config address_binding dhcp_snoop 360

show address_binding dhcp_snoop 361
DOS PREVENTION COMMANDS 363
config dos_prevention dos_type 363
show dos_prevention 364
TRUST HOST COMMANDS 366
enable trusted_host 366
disable trusted_host 366
create trusted_host 367
show trusted_host 368
delete trusted_host 368
POE COMMANDS 370
config poe ports 370
config poe system 371
show poe ports 372
show poe system 372
DEBUG COMMANDS 374
debug config semaphore 374
show tech support 375
clear tech support 378
DEVICE SPECIFICATIONS 379
Technical Specifications 379
Supported Transceivers 382

1

INTRODUCTION

DGS-2000 Rev.A1 series inculdes DGS-2000-10, DGS-2000-10P, DGS-2000-10MP, DGS-2000-20, DGS-2000-26, DGS-2000-28, DGS-2000-28P, DGS-2000-28MP, DGS-2000-52, and DGS-2000-52MP. This series offer variable combaination of port quantity and PoE capability.

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

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

No flow controThis 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-2000-28MP:5# config ipif System ipaddress 10.90.90.91/8
Command: config ipif System ipaddress 10.90.90.91/8


Success.

DGS-2000-28MP: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.

2

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.

The login messag contains the information of firmware verion and model name:

```
DGS-2000-28MP Gigabit Ethernet Switch
Command Line Interface

Firmware: Build 1.00.008
Copyright(C) 2019 D-Link Corporation . All rights reserved.

DGS-2000-28MP:5#
```

Figure 2–1 Initial Console Screen after Logging In

Commands are entered at the command prompt, DGS-2000-28MP: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-2000-28MP:5# ?
Command: ?


USEREXEC commands :
?
cable diagnostic port
clear
clear address_binding dhcp_snoop binding_entry ports
clear arptable
clear counters
clear ethernet_oam ports
clear fdb
clear flood_fdb
clear igmp_snooping data_driven_group
clear igmp_snooping statistics counter
clear log
clear mld_snooping statistics counter
clear port_security_entry port
clear tech support
compute dlink-SHA1
```

```
config 802.1p default_priority
config 802.1x auth_mode
config 802.1x auth_parameter portscompute dlink-SHA1
config 802.1x auth_mode
config 802.1x auth_parameter ports
```

Figure 2–2 The ? Command

CLI engine offers mechanism to automatic listed the possible parameters if command does not completed entered by use:

```
DGS-2000-28MP:5# config vlan

Command: config vlan

Next possible completions :
vlanid          <vlan_name 20>

DGS-2000-28MP:5# show firmware ?

Command: show firmware

Next possible completions :
Information

DGS-2000-28MP: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-2000-28MP:5# config vlan

Command: config vlan

Next possible completions :
vlanid          <vlan_name 20>

DGS-2000-28MP:5# config vlan
```

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:

```
DGS-2000-28MP:5# DLINK

Available commands :
  ?              cable          clear          compute
  config         create         delete         disable
  download       enable         logout         ping
  ping6          reboot         reset          save
  show           telnet         traceroute     upload


DGS-2000-28MP: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-2000-28MP:5# show

Command: show

Next possible completions :
  802.1p              802.1x              access_profile      account
  acct_client         address_binding     arpentry            asymmetric_vlan
  auth_client         authen              authen_enable       authen_login
  authen_policy       auto_fdb            autoconfig          autoimage
  bandwidth_control   command             command_history
  community_encryption                    config              configuration
  cos                 cpu                 cpu_access_profile  ddm
  ddp                 dhcp_local_relay    dhcp_relay          dhcpv6_relay
  dos_prevention      dscp_mapping        duld                EEE_mode
  error               ethernet_oam        fdb                 firmware
  flood_fdb           greeting_message    igmp                igmp_snooping
  ipif                iproute             ipv6                ipv6route
  jumbo_frame         lacp                limited_multicast_addr
  link_aggregation    lldp                log                 log_save_timing
  log_software_module logintimeout        loopdetect          mac_notification
  max_mcast_group     mcast_filter_profile                    mirror
  mld_snooping        multicast           multicast_fdb       packet
  poe                 port_security       port_vlan           ports
  power_saving        pppoe               pvid                qinq
  qos                 radius              rmon                router_ports
  safeguard_engine    scheduling          scheduling_mechanism
```

```
session                 snmp                    sntp                    statistics
stp                     surveillance_vlan       switch                  syslog
tech                    terminal                time                    time_range
traffic                 traffic_segmentation                            trusted_host
utilization             vlan                    vlan_translation        voice_vlan

DGS-2000-28MP:5#
```

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.

3

COMMAND SYNTAX

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

4

BASIC SWITCH COMMANDS

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

Command	Parameter
enable clipaging	
disable clipaging	
enable password encryption	
disable password encryption	
config terminal length	{<integer (10-512)> | default}
config terminal width	{<integer (40-255)> | default}
show terminal	
create account	[admin | operator | user] <username 15>
config account	<username 15> {encrypt {plain_text <password 15> | sha_1 <password 35>}}
show account	
reset account	
reset password	{<username 15>}
delete account	<username 15>
show switch	
show firmware information	
enable web	{<tcp_port_number 1-65535>}
disable web	
enable telnet	{<tcp_port_number 1-65535>}
disable telnet	
show session	
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	[systme {force_agree}]

Command	Parameter
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>}
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]
show time_range	
enable ssh	
disable ssh	
enable telnet	
disable telnet	
telnet	<ipaddr>
traceroute	<ip_addr> {min-ttl <short 1-99> | max-ttl <short 1-99> | port <value 30000-64900> | timeout <sec 1-60> | probe <value 1-9>}
traceroute6	<ipv6_addr> {min-ttl <short 1-99> | max-ttl <short 1-99> | port <value 30000-64900> | timeout <sec 1-60> | probe <value 1-9>}
show cpu port	
reset cpu port	

Each command is listed in detail, as follows:

enable clipaging	
Purpose	Used to enable automatic paging mechanism when information could not be fit within a page.
Syntax	**enable clipaging**
Description	Clipaging is an automatic mechanism to paging printout in command line session.
Parameters	None.
Restrictions	Only Administrator level users can issue this command.

Example usage:

To enable clipaging on the Switch:

```
DGS-2000-28MP:5# enable clipaging
Command: enable clipaging

Success.
DGS-2000-28MP:5#
```

disable clipaging

Purpose	Used to disable automatic paging mechanism when information could not be fit within a page.
Syntax	**disable clipaging**
Description	Clipaging is an automatic mechanism to paging printout in command line session.
Parameters	None.
Restrictions	Only Administrator level users can issue this command.

Example usage:

To enable clipaging on the Switch:

```
DGS-2000-28MP:5# disable clipaging
Command: disable clipaging

Success.
DGS-2000-28MP:5#
```

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-2000-28MP:5# enable password encryption
Command: enable password encryption


Success.

DGS-2000-28MP: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-2000-28MP:5#  disable password encryption
Command: disable password encryption

Success !
DGS-2000-28MP:5#
```

config terminal length

Purpose	Used to specify the terminal output parameters.
Syntax	**config terminal length {<integer (10-512)> | default}**
Description	This command is used to adjust the Command line interface output parameters in order to fulfill different tool.
Parameters	*<interger (10-512)>* - Configurable range 10-512.
Restrictions	Only Administrator level users can issue this command.

Example usage:

To adjust the terminal length:

```
DGS-2000-28MP:5# config terminal length 30
Command: config terminal length 30

DGS-2000-28MP:5#
```

config terminal width

Purpose	Used to specify the terminal output parameters.
Syntax	**config terminal length {<integer (40-255)> | default}**
Description	This command is used to adjust the Command line interface output parameters in order to fulfill different tool.
Parameters	*<interger (40-255)>* - Configurable range 40-255.
Restrictions	Only Administrator level users can issue this command.

Example usage:

To adjust the terminal width:

```
DGS-2000-28MP:5# config terminal width 50
Command: config terminal width 50

DGS-2000-28MP:5#
```

show terminal

Purpose	Used to display the terminal output parameters.
Syntax	**show terminal**
Description	This command is used to display the configured parameters of terminal.
Parameters	None
Restrictions	None

Example usage:

To display the terminal configurations:

```
DGS-2000-28MP:5# show terminal
Command: show terminal

Terminal Settings:
 Length: 30 lines
 width: 50 columns
 Default Length: 25 lines
 Default Width: 80 columns
 Baud Rate: 115200 bps

DGS-2000-28MP: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	*admin* − Name of the administrator account. *oper* − Specify an operator level account. *user* − Specify a user account with read-only permissions. <*username 1-15*> − The account username may be between 1 and 15 characters. *password* <password_string> {encrypted} - the account password can be included, and (optionally) can be encrypted.
Restrictions	Only Administrator level users can issue this command.

Usernames can be between 1 and 15 characters. Passwords can be between 0 and 15 characters.

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-2000-28MP: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-2000-28MP:5#
```

config account

Purpose	To change the password for an existing user account.
Syntax	**config account <username 15> {encrypt {plain_text <password 15> | sha_1 <password 35>}}**
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. *encrypt* – Capbility for option <plain text> or <sha 1> encryption *sha_1* – Encryption method (password string can be hashed via command “compute dlink-sSHA1 <string15>)
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the user password of ‘dlink’ account:

```
DGS-2000-28MP:5# compute dlink-SHA1 test
Command: compute dlink-SHA1 test

Result = *@&qUqP5cyxm6YcTAhz05Hph5gvu9P+CdlY

DGS-2000-28MP:5# config account dlink encrypt sha_1 *@&qUqP5cyxm6Y
cTAhz05Hph5gvu9P+CdlY
Command: config account dlink encrypt sha_1 ******

DGS-2000-28MP:5# show config current_config include "account"
```

```
Command: show config current_config include account

#------------------------------------------------------------------------
#            DGS-2000-28MP Gigabit Ethernet Switch Configuration
#
#                        Firmware: Build 1.00.009
#       Copyright(C) 2019 D-Link Corporation. All rights reserved.
#------------------------------------------------------------------------
create account admin "dlink"
*@&qUqP5cyxm6YcTAhz05Hph5gvu9P+CdlY
*@&qUqP5cyxm6YcTAhz05Hph5gvu9P+CdlY
```

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 the created account information

```
DGS-2000-28MP:5# show account
Command: show account

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

Total Entries     : 1

DGS-2000-28MP:5#
```

reset account

Purpose	To erase entire account information
Syntax	**reset account**
Description	The **reset account** command is used to erase ALL accounts information.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To reset all accounts created:

```
DGS-2000-28MP:5# reset account
```

```
Command: reset account

Are you sure to proceed with clean account?(y/n)y

Success.

DGS-2000-28MP:5#
```

reset password

Purpose	To erase the password configured in user accounts
Syntax	**reset password {<username 15>}**
Description	The **reset passowrd** command is used to erase ALL or particular password information configured in user accounts.
Parameters	*<username 15>* - Specify the user account the password would be reset. Without this parameter, ALL account password would be reset.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To reset password in ALL accounts:

```
DGS-2000-28MP:5# reset password
Command: reset password

Success.

DGS-2000-28MP: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-2000-28MP:5# delete account dlink
Command: delete account dlink

Success.

DGS-2000-28MP:
```

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-2000-28MP:5# show switch
Command: show switch

 Device Type                 : DGS-2000-28MP
 MAC Address                 : F4-8C-EB-E9-EE-00
 IP Address                  : 10.90.90.91
 VLAN Name                   : default
 Subnet Mask                 : 255.0.0.0
 Default Gateway             : 0.0.0.0
 System Boot Version         : 1.00.001
 System Firmware Version     : 1.00.005
 System Hardware Version     : A1
 System Serial Number        : TM1C1JA000043
 System Name                 :
 System Location             :
 System Up Time              : 0 days, 4 hrs, 13 min, 22 secs
 System Contac               :
 System Time                 : 01:44:25 05 01 2019
 IGMP Snooping               : Disabled
 802.1X Status               : Disabled
 Telnet                      : Enabled  <TCP  23>
 SSH                         : Enabled  <TCP  22>
 Web                         : Enabled  <TCP  80>
 RMON                        : Disabled
 Syslog Global State         : Disabled
 CLI Paging                  : Enabled

DGS-2000-28MP:5#
```

show firmware information

Purpose	Used to display the firmware section information.
Syntax	**show firmware information**
Description	The **show firmware information** command is used to display the

	firmware section information.
Parameters	None.
Restrictions	None.

Example usage:

```
DGS-2000-28MP:5# show firmware information
Command: show firmware information


 Image ID    Version       Size(B)     Update Time
 ----------  ------------  ----------  ------------
 *1c         1.00.008      10968120    1/1/2019 00:04:06
  2          1.00.008      10968120    1/1/2019 00:32:11

 c : Current boot up firmware
 * : Boot up firmware

DGS-2000-28MP: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 or configure the TCP port number:

```
DGS-2000-28MP:5# enable web
Command: enable web


Success.

DGS-2000-28MP:5# enable web 9527
Command: enable web 9527


Success.

DGS-2000-28MP: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. Please be noted disabling HTTP access method may cause lost management if this is the LAST management method available.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To disable HTTP-capbility of switch:

```
DGS-2000-28MP:5# disable web
Command: disable web

Success.

DGS-2000-28MP: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-2000-28MP:5# enable telnet
Command: enable telnet

Success.

DGS-2000-28MP:5#
```

disable telnet

Purpose	To disable telnet.
Syntax	**disable telnet**
Description	The **disable telnet** command disables telnet. Please be noted disabling TELNET access method may cause lost management if this is the LAST management method available.

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

Example usage:

To disable telnet:

```
DGS-2000-28MP:5# disable telnet
Command: enable telnet
```

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 logged in user information:

```
DGS-2000-28MP:5# show session
Command: show session

ID   Login Time           Live Time   From                  Level   Name
--   -------------------- ----------- --------------------- -----   ---------------
1    3/24/2020 08:22:12   00:10:33    console               5       anonymous

Total Entries       : 1

DGS-2000-28MP: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	config_in_nvram config_id <value 1-2> − Display the system configuration from NV-RAM. current_config − Display system configuration from the DRAM

	database, i.e. the current system setting. [begin | exclude | include] − Display the configuration which is begined, excluded or included. <string 80> − Display the configuration which begin or exclude the specified string. The maximum string is 80.
Restrictions	None.

Example usage:

To display current config in switch:

```
DGS-2000-28MP:5# show config current_config
Command: show config current_config

#------------------------------------------------------------------
#            DGS-2000-28MP Gigabit Ethernet Switch Configuration
#
#                        Firmware: Build 1.00.009
#        Copyright(C) 2019 D-Link Corporation. All rights reserved.
#------------------------------------------------------------------
command-start

# Port
config ports 1-28 speed auto
config ports 25-28 medium_type fiber speed auto
config ports 1-28 state enable
config ports 25-28 medium_type fiber state enable
config ports 1-28 flow_control disable
config ports 25-28 medium_type fiber flow_control disable
config ports 1-28 learning enable
config ports 25-28 medium_type fiber learning enable
config ports 1-28 mdix auto
config ports 1 capability_advertised 10_half 10_full 100_half 100_full 1000_full
config ports 2 capability_advertised 10_half 10_full 100_half 100_full 1000_full
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. DGS-2000 Series supports jumbo frame to 10,000 bytes.
Parameters	None.
Restrictions	Only Administrator or operate-level users can issue this command.

Example usage:

To enable jumbo frames:

```
DGS-2000-28MP:5# enable jumbo_frame
Command: enable jumbo_frame
```

```
Success.

DGS-2000-28MP: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.

Example usage:

To disable jumbo_frames:

```
DGS-2000-28MP:5# disable jumbo_frame
Command: disable jumbo_frame

Success.

DGS-2000-28MP: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 capability:

```
DGS-2000-28MP:5# show jumbo_frame
Command: show jumbo_frame

Jumbo Frame is  Enabled
DGS-2000-28MP: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	*config* – Used to save the current configuration to a file. *log* – 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 current configurations into non-volatile RAM:

```
DGS-2000-28MP:5# save config
Command: save config


Success.

DGS-2000-28MP: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-2000-28MP:5# reboot
Command: reboot

Are you sure you want to proceed with the system reboot?(y/n)y
```

reset

Purpose	To reset the Switch to the factory default settings.
Syntax	**reset [system} {force_agree}]**
Description	The **reset** command restores the Switch's configuration to the default settings in veriable ways: 1. IP address, log and user account remains 2. Entire configuration restored to factory default
Parameters	*system* − 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. *{force_agree}* - When force_agree is specified, the reset command will be executed immediately without further confirmation. 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.
Restrictions	Only administrator-level users can issue this command.

Example usage:

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

```
DGS-2000-28MP:5# reset system
Command: reset system

Are you sure you want to proceed with the system reset, save and reboot?(y/n)
```

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 CLI session:

```
DGS-2000-28MP:5# logout
Command: 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	*<ipaddr>* - The IP address of the host. *times <value 0-255>* - The number of individual ICMP echo messages to be sent. The maximum value is 255. The default is 4. *timeout <sec 1-99>* - The time-out period while waiting for a response from the remote device. A value of 1 to 99 seconds can be specified. The default is 1 second. *size <value 1-60000>* - Specify the size of the test packet. A value of 0 to 2080 can be specified.
Restrictions	None.

Example usage:

To ping the IP address 10.90.90.97 three times:

```
DGS-2000-28MP:5# ping 10.90.90.123 times 3 size 100 timeout 3
Command: ping 10.90.90.123 times 3 size 100 timeout 3

Reply Received From :10.90.90.123, TimeTaken : 40 ms
Reply Received From :10.90.90.123, TimeTaken : 20 ms
Reply Received From :10.90.90.123, TimeTaken : 40 ms

--- 10.90.90.123 Ping Statistics ---
3 Packets Transmitted, 3 Packets Received, 0% Packets Loss
DGS-2000-28MP: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	*<ipv6addr>* - The IPv6 address of the host. *size <value 1-6000>* - Specify the size of the test packet. A value of 1 to 6000 can be specified. *timeout <sec 1-99>* - The time-out period while waiting for a response from the remote device. A value of 1 to 99 seconds can be specified. The default is 1 second. *times <value 1-255>* - The number of individual ICMP echo messages to be sent. The maximum value is 255. The default is 4.
Restrictions	None.

Example usage:

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

```
DGS-2000-28MP:5#ping6 3000::1 times 4
Command: ping6 3000::1 times 4

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


--- 3000::1 Ping Statistics ---
4 Packets Transmitted, 4 Packets Received, 0% Packets Loss
DGS-2000-28MP: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 2014-2029> month <start_mth 1-12> date <start_date 1-31> to_day year <end_year 2014-2029> 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	*<range_name 20>* – Specifies the time range name. The range of characters is 1 - 20. *start_time <start_time 32>* – defines the time on which the time range will start to be active. *end_time <end_time 32 >*– defines the time on which the time range will stop to be active. *weekdays <daylist 32>* – defines the days of the week on which the time range will be active. *<start_year 2014-2029 >* – Specifies the time range start year. *<start_mth 1-12>* – Specifies the time range start month. *<start_date 1-31>* – Specifies the time range start date. *<end_year 2014-2029 >* – Specifies the time range end year. *<end _mth 1-12>* – Specifies the time range end month. *<end _date 1-31>* – Specifies the time range end date. *delete* – Delete the time range settings.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure the time range on the Switch:

```
DGS-2000-28MP:5# config time_range test hours start_time 00:33 end_time 15:30 weekdays mon,tue,wed,thu,fri,sat,sun
Command: config time_range test hours start_time 00:33 end_time 15:30 weekdays mon,tue,wed,thu,fri,sat,sun


Success.
```

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-2000-28MP:5# show time_range
Command: show time_range


Time Range Information
-------------------------------------------
  Range Name                          : test
  Weekdays                            : mon,tue,wed,thu,fri,sat,sun
  Start Time                          : 00:33
  End Time                            : 15:30
  From Day                            :
  To Day                              :

DGS-2000-28MP:5#
```

enable ssh

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

Example usage:

To enable SSH:

```
DGS-2000-28MP:5# enable ssh
Command: enable ssh

Success.

The SSH server is enabled.

DGS-2000-28MP:5#
```

disable ssh

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

Example usage:

To disable SSH:

```
DGS-2000-28MP:5# disable ssh
Command: disable ssh

Success.

The SSH server is disable.

DGS-2000-28MP:5#
```

enable telnet

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

Example usage:

To enable telnet:

```
DGS-2000-28MP:5# enable telnet
Command: enable telnet


Success.
DGS-2000-28MP: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-2000-28MP:5# disable telnet
Command: disable telnet

Success.

DGS-2000-28MP:5#
```

telnet

Purpose	To telnet another device.

Syntax	**telnet <ipaddr> {-l <string>}**
Description	The **telnet** command is used to telnet another device.
Parameters	None.
Restrictions	Only Administrator or operate-level users can issue this command.

Example usage:

To telnet another device which IP is 10.90.90.91:

```
DGS-2000-28MP:5# telnet 10.90.90.91
Command: telnet 10.90.90.91
```

traceroute

Purpose	The traceroute User EXEC mode command discovers routes that packets actually take when traveling to their destination.
Syntax	**traceroute [<ip_addr> | ipv6 <ipv6addr>] {min-ttl <short 1-99> | max-ttl <short 1-99> | port <value 30000-64900> | timeout <sec 1-60> | probe <value 1-9>}**
Description	The **traceroute** command discovers routes that packets actually take when traveling to their destination.
Parameters	<*ip_addr*>| *ipv6* <*ipv6addr*> - Specifies the IP address of the destination host. *min-ttl* - Specify the minimum time to live value of the trace route request. <*short 1-99*> - Specify the minimum time to live value of the trace route request. *max-ttl* - Specify the maximum time to live value of the trace route request. <*short 1-99*> - Specify the maximum time to live value of the trace route request. *port* - Specify the port number. <*value 30000-64900*> - - Specify the port number. The value range is from 30000 to 64900. The default is 33435. *timeout* - Specify the timeout period while waiting for a response from the destination. <sec 1-60> - Specify the timeout period while waiting for a response from the remote device. *probe* - Specify the number of probes. <*value 1-9*> - Specify the number of probes. The range is from 1 to 9. If unspecified, the default value is 1.
Restrictions	Only Administrator or operate-level users can issue this command.

Example usage:

To trace route IP 10.90.90.92 with max-ttl is 10:

```
DGS-2000-28MP:5# traceroute 8.8.8.8
Command: traceroute 8.8.8.8

 10  ms      192.168.0.1
 10  ms      168.95.98.254
 20  ms      168.95.22.118
```

```
10   ms      220.128.12.122
20   ms      72.14.202.34
*          Timeout
10   ms      8.8.8.8

Trace Complete
DGS-2000-28MP:5#
```

show cpu port

Purpose	To display the CPU port information.
Syntax	**show cpu port**
Description	The **show cpu port** command displays the CPU port information.
Parameters	None.
Restrictions	Only Administrator users can issue this command.

Example usage:

To display the CPU port information:

```
DGS-2000-28MP:5# show cpu port
Command: show cpu port

Type                       Total      Diff
-------------------------- ---------- -----------
ARP                        0
DHCP                       0
DHCPv6                     0
GVRP                       0
ICMP                       0
ICMPv6                     0
IGMP                       0
LACP                       0
LLDP                       0
PPPoE                      0
Reserved Multicast         0
STP                        0
TELNET                     0
UDP                        0


DGS-2000-28MP:5#
```

reset cpu port

Purpose	To reset the CPU port information.
Syntax	**reset cpu port**
Description	The **reset cpu port** command resets the CPU port information.

Parameters	None.
Restrictions	Only Administrator users can issue this command.

Example usage:

To reset the CPU port information:

```
DGS-2000-28MP:5# reset cpu port
Command: reset cpu port

Success.

DGS-2000-28MP:5#
```

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	*<string 32>* – The command prompt can be changed by entering a new name of no more that 32 characters. *default* – The command prompt will reset to factory default command prompt. Default = the name of the Switch model, for example "DGS-2000-28MP". *username* – The command prompt will be changed to the login username.
Restrictions	Only Administrator-level users can issue this command. Other restrictions include: 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.

Example usage:

Change the command prompt to username:

```
DGS-2000-28MP:5# config command_prompt username
Command: config command_prompt username


Success.

dlink: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	*default* – 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: 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
Restrictions	Only Administrator-level users can issue this command. Other restrictions include: 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. 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.

Example usage:

```
DGS-2000-28MP:5# config greeting_message
Command: config greeting_message

Greeting Messages Editor
============================================================
DGS-2000-28MP
DGS-2000-28MP
DGS-2000-28MP
DGS-2000-28MP
============================================================


Array Up    : Cursor up          Ctrl+X    : Erase all
Array Down  : Cursor down        Ctrl+L    : Relaod original data
Array Left  : Cursor left        Ctrl+C    : Quit without save
Array Right : Cursor right       Ctrl+W    : Save and quit
Ctrl+D      : Erase current line
```

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-2000-28MP:5# show greeting_message
Command: show greeting_message


DGS-2000-28MP
DGS-2000-28MP
DGS-2000-28MP
DGS-2000-28MP


DGS-2000-28MP:5#
```

6

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>] {medium_type [copper | fiber] | mdix [normal | crossover | auto] | description <desc 32> | description <desc32> | flow_control [enable | disable] | learning [enable | disable] | state [enable | disable] | speed [auto | 1000_full | 100_full | 100_half | 10_full | 10_half] | capability_advertised [10_half | 10_full | 100_half | 100_full |1000_full]}
show ports	[<portlist> | all] [media type | description | err_disabled | auto_negotiation | linkup_time | capability_advertisement]
enable auto learning	
disable auto learning	
config duld ports	[all | <portlist>] {state [enable | disable] | mode [shutdown | normal | discovery_time <sec 5-65535)>}
show duld ports	{all | <portlist>}

Each command is listed in detail, as follows:

config ports	
Purpose	To configure the Switch's Ethernet port settings.
Syntax	**config ports [all | <portlist>] {medium_type [copper | fiber] | mdix [normal | crossover | auto] | description <desc 32> | description <desc32> | flow_control [enable | disable] | learning [enable | disable] | state [enable | disable] | speed [auto | 1000_full | 100_full | 100_half | 10_full | 10_half] | capability_advertised [10_half | 10_full | 100_half | 100_full |1000_full]}**
Description	The **config ports** command configures the Switch's Ethernet port settings. Only the ports listed in the <portlist> are affected.
Parameters	*<portlist>* − A port or range of ports to be configured. *all* − Configures all ports on the Switch. *medium_type [copper | fiber]* − If configuring the Combo ports, this defines the type of medium being configured. *mdix [normal | crossover | auto]* − Specifies the implementation of Medium Dependant Interface Crossover. The MDIX setting can be auto, normal or cross. 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. *description <desc 32>* − Enter and alphanumeric string of no more that 32 characters to describe a selected port interface.

	clear_description – Clear the description for the specified ports. *flow_control [enable]* – Enables flow control for the specified ports. *flow_control [disable]* – Disables flow control for the specified ports. *learning [enable* | *disable]* c Enables or disables the MAC address learning on the specified range of ports. *state [enable* | *disable]* − Enables or disables the specified range of ports. *speed* – Sets the speed of a port or range of ports, with the addition of one of the following: • *auto* − Enables auto-negotiation for the specified range of ports. • *[10* | *100* | *1000]* − Configures the speed in Mbps for the specified range of ports. • *[half* | *full]* − Configures the specified range of ports as either full or half-duplex. *capability_advertised* – Specified the link speed capabilities that device advertised to link partner.
Restrictions	Only Administrator or Operator 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-2000-28MP: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-2000-28MP:5#
```

show ports

Purpose	To display the current configuration of a range of ports.
Syntax	**show ports [<portlist> | all] [media type | description | err_disabled | auto_negotiation | linkup_time | capability_advertisement]**
Description	The **show ports** command displays the current configuration of a port or range of ports.
Parameters	<*portlist*> − A port or range of ports whose settings are to be displayed. *all* – Specifies all ports to be displayed. *media type* – Display the media type used to estibalished connection *description* – Display the port description *error_disable* – Display the port error disable information *auto_negotiation* – Display the auto negotiation result of the port specified *linkup_time* – Display the time linked up of the port specified.

	capability_advertisement – Display the link speed capability advertised of the port specified.
Restrictions	None.

Example usage:

To display the configuration of port 1-3 on the Switch:

```
DGS-2000-28MP:5# show ports 1-3
Command: show ports 1-3

Port   State/      Settings              Connection            Address
       MDI         Speed/Duplex/FlowCtrl Speed/Duplex/FlowCtrl Learning
-----  --------    --------------------  --------------------  --------
1      Enabled     Auto/Disabled         Link Down             Enabled
       Auto
2      Enabled     Auto/Disabled         1G/Full/Disabled      Enabled
       Auto
3      Enabled     Auto/Disabled         1G/Full/Disabled      Enabled
       Auto

DGS-2000-28MP:5#
```

enable auto learning

Purpose	The global switch for MAC addresses learning mechanism.
Syntax	**enable auto learning**
Description	MAC address learning mechanism helps to learn the MAC addresses of hosts. In other words, the packet can be forwarded to its demand particular destination. In stead of learning switch in port's configuration, this command controls learning mechanism globally.
Parameters	None
Restrictions	Only Administrator level users can issue this command

Example usage:

To turn on auto learning mechanism.

```
DGS-2000-28MP:5# enable auto learning
Command: enable auto learning

Success.

DGS-2000-28MP:5#
```

disable auto learning

Purpose	The global switch for MAC addresses learning mechanism.
Syntax	**disable auto learning**

Description	MAC address learning mechanism helps to learn the MAC addresses of hosts. In other words, the packet can be forwarded to its demand particular destination. In stead of learning switch in port's configuration, this command controls learning mechanism globally.
Parameters	None
Restrictions	Only Administrator level users can issue this command

Example usage:

To turn off auto learning mechanism.

```
DGS-2000-28MP:5# disable auto learning
Command: disable auto learning


Success.

DGS-2000-28MP:5#
```

config duld ports

Purpose	To configure DULD (D-Link Unidirectional Link Detection) feature.
Syntax	**config duld ports {state [enable | disable] | mode [shutdown | normal | discovery_time <sec 5-65535)>}**
Description	D-Link Unidirectional Link Detection provides discovery mechanism based on IEEE 802.3ah to discovery its neighbor. If the discovery can complete in configured discovery time, it concludes the link is bidirectional. Otherwise, it starts detecting task to detect the unidirectional link status.
Parameters	*{all | <portlist>}* − Specifies all ports or range of ports to be configured. *state [enable | disable]* – To configure the state of DULD feature of specified port. *mode* – Specify the action when unidirectional link detected *shutdown* – shutdown the port when unidirection link detected *normal* – Only log an event when a unidirectional link is detected *discovery_time* – Specify the time for neighbor discovery. If the discovery is timeout, the unidirectional link detection will start.
Restrictions	Only Administrator level users can issue this command

Example usage:

To configure DULD feature in ports 1-5.

```
DGS-2000-28MP:5# config duld ports 1-5 state enable mode shutdown
Command: config duld ports 1-5 state enable mode shutdown


Success.
```

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	*{all | <portlist>}* − 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-2000-28MP:5# show duld ports 1-5
Command: show duld ports 1-5

Port  Admin State  Oper Status  Mode      Link Status    Discovery Time
----  -----------  -----------  --------- -------------  --------------
1     Enabled      Disabled     ShutDown  Unknown        5
2     Enabled      Disabled     ShutDown  Unknown        5
3     Enabled      Disabled     ShutDown  Unknown        5
4     Enabled      Disabled     ShutDown  Unknown        5
5     Enabled      Disabled     ShutDown  Unknown        5
DGS-2000-28MP:5#
```

7

SPANNING TREE COMMANDS

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

Command	Parameter
enable stp	
disable stp	
config stp	{maxage <value 6-40> | hellotime <value 1-10> | forwarddelay <value 4-30>| txholdcount <value 1-10> | maxhops <value 6-40>}
config stp ports	<portlist> {externalcost [auto | <value 1-200000000>] | edge [auto | true | false] | hellotime <value 1-2> | p2p [true | false | auto] | state [enable | disable] | fbpdu [enable | disable] | migrate [yes | no] | priority <value 0-240> | restricted_role [true | false] | restricted_tcn [true | false] }
config stp version	[mstp | rstp | stp]
config stp fbpdu	[enable | disable]
config stp priority	<value 0-61440> instance_id <value 0-15>
show stp	
show stp ports	{<portlist>}
create stp instance_id	<value 1-63>
delete stp instance_id	<value 1-63>
config stp instance_id	<value 1-63> [add_vlan | remove_vlan] <vidlist>
show stp instance	<value 1-63>}
config stp mst_config_id	[revision_level <int 0-65535> | name <string 32>]
config stp mst_ports	<portlist> instance_id <value 0-15> {internalCost [auto | value 1-200000000] | priority <value 0-240>}
show stp mst_config_id	

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-2000-28MP:5# enable loopdetect
Command: enable loopdetect


Success.
```

enable stp	
Purpose	To globally enable STP on the Switch.
Syntax	**enable stp**
Description	The **enable stp** command is used to set the Spanning Tree Protocol to be globally enabled on the Switch.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To enable STP, globally, on the Switch:

```
DGS-2000-28MP:5# enable stp
Command: enable stp

Success.
DGS-2000-28MP:5#
```

disable stp	
Purpose	To globally disable STP on the Switch.
Syntax	**disable stp**
Description	The **disable stp** command is used to set the Spanning Tree Protocol to be globally disabled on the Switch.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To disable STP on the Switch:

```
DGS-2000-28MP:5# disable stp
Command: disable stp

Success.
DGS-2000-28MP:5#
```

config stp	
Purpose	To setup STP, RSTP and MSTP on the Switch.
Syntax	**config stp {maxage <value 6-40> | hellotime <value 1-10> | forwarddelay <value 4-30>| txholdcount <value 1-10> |**

	maxhops <value 6-40>}
Description	The **config stp** command configures the Spanning Tree Protocol (STP) for the entire switch. All commands here are implemented for the STP version that is currently set on the Switch.
Parameters	*maxage* <*value 6-40*> − This value may be set to ensure that old information does not endlessly circulate through redundant paths in the network, preventing the effective propagation of the new information. Set by the Root Bridge, this value aids in determining that the Switch has spanning tree configuration values consistent with other devices on the bridged LAN. If the value ages out and a BPDU has still not been received from the Root Bridge, the Switch starts sending its own BPDU to all other switches for permission to become the Root Bridge. If your switch has the lowest priority, it becomes the Root Bridge. The user may choose a time between 6 and 40 seconds. The default value is 20. *hellotime* <*value 1-10*> − The user may set the time interval between transmission of configuration messages by the root device in STP, or by the DGSignated router, thus stating that the Switch is still functioning. The value may be between 1 and 10 seconds. The default value is 2 seconds. *forwarddelay* <*value 4-30*> − The amount of time (in seconds) that the root device will wait before changing from Blocking to Listening , and from Listening to Learning states. The value may be between 4 and 30 seconds. The default is 15 seconds. *txholdcount* <*value 1-10*> − The maximum number of BPDU Hello packets transmitted per interval. Default value = 3. *maxhops* <*value 6-40*> - The maximum number of BPDU hops packets transmitted per interval. Default value = 20.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure STP with maxage 18 and hellotime 2:

```
DGS-2000-28MP:5# config stp maxage 18 hellotime 2
Command: config stp maxage 18 hellotime 2

Success.
DGS-2000-28MP:5#
```

config stp ports

Purpose	To setup STP on the port level.
Syntax	**config stp ports <portlist> {externalcost [auto | <value 1-200000000>] | edge [auto | true | false] | hellotime <value 1-2> | p2p [true | false | auto] | state [enable | disable] | fbpdu [enable | disable] | migrate [yes | no] | priority <value 0-240> | restricted_role [true | false] | restricted_tcn [true | false] }**
Description	The **config stp ports** command configures STP for a group of ports.
Parameters	<*portlist*> – A port or range of ports to be configured. The port list is specified by listing switch number and the beginning port number on that switch, separated by a colon. Then the highest port number of the range is specified. The beginning and end of the port list range are separated by a dash. *externalCost* − Defines a metric that indicates the relative cost of

forwarding packets to the specified port list. Port cost can be set automatically or as a metric value. The default value is auto.

- *auto* – Automatically sets the speed for forwarding packets to the specified port(s) in the list for optimal efficiency. Default port cost:10Mbps port = 2000000. 100Mbps port = 200000. Gigabit port = 20000. Port-channel = 20000.
- <*value 1-200000000*> - Defines a value between 1 and 200000000 to determine the external cost. The lower the number, the greater the probability the port will be chosen to forward packets.

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

hellotime <*value 1-2*> – The time interval between transmission of configuration messages by the DGSignated port, to other devices on the bridged LAN, thus stating that the Switch is still functioning. The user may choose a time between 1 and 2 seconds. The default is 2 seconds.

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

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

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

migrate [yes | *no]* − Setting this parameter as "yes" will set the ports to send out BPDU packets to other bridges, requesting information on their STP setting if the Switch is configured for RSTP, the port will be capable to migrate from 802.1D STP to 802.1w RSTP. If the Switch is configured for MSTP, the port is capable of migrating from 802.1D STP to 802.1s MSTP. RSTP and MSTP can coexist with standard STP, however the benefits of RSTP and MSTP are not realized on a port where and 802.1D network connects to and 802.1w or 802.1s enabled network. Migration should be set as yes on ports connected to network stations or segments that are capable of being upgraded to 802.1w RSTP or 802.1s MSTP on all or some portion of the segment.

priority <*value 0-240*> − Specifies the priority. The range is from 0 to 240.

restricted_role [true | *false]* − To decide if this is to be selected as the Root Port. The default value is false.

restricted_tcn [true | *false]* − To decide if this port is to propagate

	topology change. The default value is false.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure STP with path cost 19 and state enable for ports 1-3:

```
DGS-2000-28MP:5# config stp ports 1-3 externalcost 19 state enable
Command: config stp ports 1-3 externalcost 19 state enable

Success.
DGS-2000-28MP:5#
```

config stp version

Purpose	To globally set the version of STP on the Switch.
Syntax	**config stp version [mstp | rstp | stp]**
Description	The **config stp version** command sets the version of the spanning tree to be implemented on the Switch.
Parameters	*mstp* – Sets the Multiple Spanning Tree Protocol (MSTP) globally on the Switch. *rstp* – Sets the Rapid Spanning Tree Protocol (RSTP) globally on the Switch. *stp* – Sets the Spanning Tree Protocol (STP) globally on the Switch.
Restrictions	Only administrator-level users can issue this command.

Example usage:

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

```
DGS-2000-28MP:5# config stp version mstp
Command: config stp version mstp

Success.
DGS-2000-28MP:5#
```

config stp fbpdu

Purpose	To globally set the fbpdu of STP on the Switch.
Syntax	**config stp fbpdu [enable | disable]**
Description	The **config stp fbpdu** command allows the forwarding of STP BPDU packets from other network devices when STP is disabled on the Switch.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To set the Switch globally for the Spanning Tree Protocol (STP) fbpdu enable:

```
DGS-2000-28MP:5# config stp fbpdu enable
Command: config stp fbpdu enable

Success.
```

```
DGS-2000-28MP:5#
```

config stp priority

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

Example usage:

To set the priority value for instance_id 2 as 4096:

```
DGS-2000-28MP:5# config stp priority 4096 instance_id 2
Command: config stp priority 4096 instance_id 2

Success.
DGS-2000-28MP:5#
```

show stp

Purpose	To display the Switch's current STP configuration.
Syntax	**show stp**
Description	The **show stp** command displays the Switch's current STP configuration.
Parameters	None.
Restrictions	None.

Example usage:

To display the status of STP on the Switch:

```
DGS-2000-28MP:5# show stp
Command: show stp


STP Bridge Global Settings
-----------------------------------------
STP Status          : Enabled
STP Version         : RSTP
Bridge Priority     : 32768
```

```
Max Age                 : 18
Hello Time              : 2
Forward Delay           : 15
TX Hold Count           : 6
Forward BPDU            : Enabled
Root Cost               : 0
Root Maximum Age        : 18
Root Forward Delay      : 15
Root Port               : 0
Root Bridge             : 80:00:9C:D6:43:60:4F:A4

DGS-2000-28MP:5#
```

show stp ports

Purpose	To display the Switch's current instance_id configuration.
Syntax	**show stp ports {<portlist>}**
Description	The **show stp ports** command displays the STP Instance Settings and STP Instance Operational Status currently implemented on the Switch.
Parameters	*<portlist>* – A port or range of ports to be configured. The port list is specified by listing switch number and the beginning port number on that switch, separated by a colon. Then the highest port number of the range is specified. The beginning and end of the port list range are separated by a dash.
Restrictions	None.

Example usage:

To show stp port 1 on switch one:

```
DGS-2000-28MP:5# show stp ports 1
Command: show stp ports 1

MSTP      Port Information
-----------------------------------------------------------------
Port Index:1 ,  Port STP:Enabled ,     P2P:Auto ,
External PathCost : 19 ,       Edge Port:Auto ,
Port RestrictedRole:False ,    Port RestrictedTCN:False
Port Priority:128 ,    Port Forward BPDU:Enabled ,
MSTI DGSignated Bridge              Internal PathCost  Prio  Status     Role
-------  -------------------------  -----------------  ----  ----------  ----------
0        80:00:00:B2:FD:DA:EE:EB  200000             128   Disabled  Disabled

DGS-2000-28MP:5#
```

create stp instance_id

Purpose	To create instance ID on the Switch.
Syntax	**create stp instance_id <value 1-63>**

Description	The **create stp instance_id** command creates an instance ID of STP on the Switch.
Parameters	<*value 1-63*> - The value of the instance ID to be created.
Restrictions	Only administrator-level users can issue this command.

To create instance id 1:

```
DGS-2000-28MP:5# create stp instance_id 1
Command: create stp instance_id 1

Warning: There is no VLAN mapping to this instance_id!

Success.
DGS-2000-28MP:5#
```

delete stp instance_id

Purpose	To delete instance ID on the Switch.
Syntax	**delete stp instance_id <value 1-63>**
Description	The **delete stp instance_id** command removes the instance ID of STP on the Switch.
Parameters	<*value 1-63*> - The value of the instance ID to be removed.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To remove instance id 2:

```
DGS-2000-28MP:5# delete stp instance_id 1
Command: delete stp instance_id 1

Success.
DGS-2000-28MP:5#
```

config stp instance_id

Purpose	To configure instance ID on the Switch.
Syntax	**config stp instance_id <value 1-63> [add_vlan | remove_vlan] <vidlist>**
Description	The **config stp instance_id** command is used to map VIDs (VLAN IDs) to previously configured STP instances on the Switch by creating an *instance_id*. A STP instance may have multiple members with the same MSTP configuration. There is no limit to the number of STP regions in a network but each region only supports a maximum of 16 spanning tree instances (one unchangeable default entry). VIDs can belong to only one spanning tree instance at a time.
Parameters	<*value 1-63*> − Enter a number between 1 and 15 to define the *instance_id*. The Switch supports 63 STP instances with one unchangeable default instance ID set as *0*. *add_vlan* – Along with the *vid_range* <*vidlist*> parameter, this command will add VIDs to the previously configured STP *instance_id.* *remove_vlan* − Along with the *vid_range* <*vidlist*> parameter, this

	command will remove VIDs to the previously configured STP *instance_id.* *<vidlist>* − Specify the VID range from configured VLANs set on the Switch. Supported VIDs on the Switch range from ID number 1 to 4094.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure instance ID 2 to add VID 10:

```
DGS-2000-28MP:5# config stp instance_id 2 add_vlan 10
Command : config stp instance_id 2 add_vlan 10

Success.
DGS-2000-28MP:5#
```

show stp instance

Purpose	To display the Switch's STP instance configuration
Syntax	**show stp instance {<value 1-63>}**
Description	The **show stp instance** command displays the Switch's current STP Instance Settings and the STP Instance Operational Status.
Parameters	*<value 1-63>* - The value of the previously configured instance_id on the Switch. The value may be between 1 and 63.
Restrictions	None.

Example usage:

To display the STP instance configuration on the Switch:

```
DGS-2000-28MP:5# show stp instance
Command: show stp instance


 ## CIST
Designated Root Bridge   00:00:00:00:00:00    Priority 0
                         We are the Root for CST
                         Port 0       , path cost 0
Regional Root Bridge     00:00:00:00:00:00    Priority  0
                        Path cost 0
Designated Bridge       00:00:00:00:00:00    Priority  0
Configured Forward delay 15, Max age 20, Max hops 20
Operational Forward delay 15, Max age 20
Topology Changes Count : 0
Last Topology Change     : 0

Interface Role       Sts        Cost    Prio.Nbr Type
------------ ------  ------     ------  ----------  -------

DGS-2000-28MP:5#
```

config stp mst_config_id

Purpose	To update the MSTP configuration identification.
Syntax	**config stp mst_config_id [revision_level <int 0-65535> | name <string 32>]**
Description	The **config stp mst_config_id** command uniquely identifies the MSTP configuration currently configured on the Switch. Information entered here is attached to BDPU packets as an identifier for the MSTP region to which it belongs. Switches having the same revision_level, name and identical vlans mapped for STP instance_ids are considered to be part of the same MSTP region.
Parameters	*revision_level <int 0-65535>*– The MSTP configuration revision number. The value may be between 0 and 65535. This value, along with the name and identical vlans mapped for STP instance_ids identifies the MSTP region configured on the Switch. The default setting is 0. *name <string 32>* - A string of up to 32 alphanumeric characters to uniquely identify the MSTP region on the Switch. This name, along with the revision_level value and identical vlans mapped for STP instance_ids identifies the MSTP region configured on the Switch. If no name is entered, the default name is the MAC address of the device.
Restrictions	Only administrator-level users can issue this command.

Example usage:

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

```
DGS-2000-28MP:5# config stp mst_config_id name Trinity revision_level 10
Command: config stp mst_config_id name Trinity revision_level 10

Success.
DGS-2000-28MP:5#
```

config stp mst_ports

Purpose	To update the port configuration for a MSTP instance.
Syntax	**config stp mst_ports <portlist> instance_id <value 0-15> {internalCost [auto | value 1-200000000] | priority <value 0-240>}**
Description	The **config stp mst_ports** command updates the port configuration for a STP instance_id. If a loop occurs, the MSTP function uses the port cost to select an interface to put into the forwarding state (if the switch isn't Root). If the switch is Root, then higher priority value for interfaces will influence on selected ports to be forwarding first at connected network devices. In instances where the priority value is identical, the MSTP function implements the lowest port number into the forwarding state and other interfaces are blocked. Remember that lower priority values mean higher priorities for forwarding packets.
Parameters	*<portlist>* – A port or range of ports to be configured. The port list is specified by listing switch number and the beginning port number on that switch, separated by a colon. Then the highest port number of the range is specified. The beginning and end of the port list range are separated by a dash. *instance_id <value 0-15>* - The value may be between 0 and 15. An

	entry of 0 denotes the CIST (Common and Internal Spanning Tree. *internalCost* – The relative cost of forwarding packets to specified ports when an interface is selected within an STP instance. The default setting is auto. There are two options: • *auto* – Specifies setting the quickest route automatically and optimally for an interface. The default value is derived from the media speed of the interface. • *value 1-200000000* – Specifies setting the quickest route when a loop occurs. The value may be in the range of 1-200000000. A lower internalCost represents a quicker transmission. *priority <value 0-240>* - The priority for the port interface The value may be between 0 and 240. A lower number denotes a higher priority. A higher priority designates the interface to forward packets first.
Restrictions	Only administrator-level users can issue this command.

Example usage:

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

```
DGS-2000-28MP:5# config stp mst_ports 1-5 instance_id 2 internalCost auto priority 16
Command: config stp mst_ports 1-5 instance_id 2 internalCost auto priority 16

Success.

DGS-2000-28MP:5#
```

show stp mst_config_id

Purpose	To display the MSTP configuration identification.
Syntax	**show stp mst_config_id**
Description	The **show stp mst_config_id** command displays the Switch's current MSTP configuration identification.
Parameters	None.
Restrictions	None.

Example usage:

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

```
DGS-2000-28MP:5# show stp mst_config_id
Command: show stp mst_config_id

Name          [00:23:22:03:14:25]
Revision      0
Instance      Vlans mapped
--------      ------------------------------------------------------------
0             1-1024,1025-2048,2049-3072,3073-4094
-------------------------------------------------------------------------------
```

```
DGS-2000-28MP:5#
```

config stp nni_bpdu_addr

Purpose	To determine the BPDU protocol address for STP in service provide site.
Syntax	**config stp nni_bpdu_addr [dot1d|dot1ad]**
Description	To determine the BPDU protocol address for STP in service provide site. It can use 802.1d STP address, 802.1ad service provider STP address.
Parameters	*dot1d* - Specify to use an 802.1d STP address. *dot1ad* - Specify to use an 802.1ad service provider STP address.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure the BPDU destination address:

```
DGS-2000-28MP:5# config stp nni_bpdu_addr dot1ad
Command: config stp nni_bpdu_addr dot1ad


Success.

DGS-2000-28MP:5#
```

8

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 > | all] state [enable | disable]
config loopdetect	interval_time <value 1-32767> lbd_recover_time [0 | <value 60-1000000>]
config loopdetect vlan	{all | <vidlist 1-4094>} state {disable | enable}
show loopdetect	{ports [<portlist > | 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-2000-28MP:5# enable loopdetect
Command: enable loopdetect


Success.
```

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-2000-28MP:5# disable loopdetect
Command: disable loopdetect


Success.
```

config loopdetect mode

Purpose	To configure the loop back detection mode to be 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	*portbase* – The port would be physical shutdown if loop detected by LBD *vlanbase* – The port would stay on physical LINKED but the particular VLAN traffic would be dropped (The VLAN that loop detected)
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

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

```
DGS-2000-28MP:5# config loopdetect mode vlanbase
Command: config loopdetect mode vlanbase


Success.
```

config loopdetect ports

Purpose	To configures the loop back detection to be enabled or disabled for the specific ports on the Switch.
Syntax	**config loopdetect ports [<portlist > | all] state [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	*<portlist >* − A port or range of ports to be configured. *all* − All ports settings are to be configured. *[enabled | disabled]* − Specifies the 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 all ports

```
DGS-2000-28MP:5# config loopdetect ports all state disable
Command: config loopdetect ports all state disable
```

```
Success.
```

config loopdetect

Purpose	To configure the loop back detection interval time and recover time on the Switch.
Syntax	**config loopdetect ports interval_time <value 1-32767> lbd_recover_time [0 | <value 60-1000000>]**
Description	The **config loopdetect** command is used to configure detection interval and recovery time.
Parameters	*interval_time <value 1-32767>* − Specifies the interval time of loop back detection. The range is between 1 and 32767 seconds. *lbd_recover_time [0 | <value 60-10000>]* − Specifies the recover time of loop back detection on the switch. "Value 0" represents recovery mechanism turned off. 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-2000-28MP:5# config loopdetect lbd_recover_time 0
Command: config loopdetect lbd_recover_time 0

Success.
```

config loopdetect vlan

Purpose	To configure the specific VLAN group for loopdetect VLAN mode.
Syntax	**config loopdetect vlan {all | <vidlist 1-4094>} state {disable | enable}**
Description	The **config loopdetect vlan** command is used to control the state of particular VLAN group.
Parameters	*vlan {all | <vidlist 1-4094>}* − Specifies the VLAN group for all or particular VID. *state {disable | enable}* – Used to control the state for specified VLAN.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

Turn on loopdect on VID 33:

```
DGS-2000-28MP:5# config loopdetect vlan 33 state enable
Command: config loopdetect vlan 33 state enable

Success.
```

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

Example usage:

To display the loop back detection information on the Switch:

```
DGS-2000-28MP:5# show loopdetect
Command: show loopdetect

    Loopdetect Global Settings
    --------------------------
Loopdetect Status        : Enabled
Loopdetect Mode          : Vlan-Base
VLAN List                : 33
Loopdetect Interval      : 2
Recover Time             : 0
DGS-2000-28MP:5#
```

9

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 as the alternative of the 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 >] { 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	When PPPoE circuit identifier insertion is enabled, the system will insert the circuit ID tag to the received PPPoE discover and request packet if the tag is absent, and remove the circuit ID tag from the received PPPoE offer and session confirmation packet. The inserted circuit ID contains the following information: MAC address Device ID Port number By default, the Switch IP address is used as the device ID to encode the circuit ID option.
Parameters	*[enable* | *disable]* – Enables or disable 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-2000-28MP:5# config pppoe circuit_id_insertion state enable
Command: config pppoe circuit_id_insertion state enable
```

```
Success.
```

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 >] [circuit_id [mac | ip | udf <string 32>] | state [enable | disable]]**
Description	When the port's state and the global state are enabled, the system will insert the Circuit ID TAG to the PPPoE discovery initiation and request (PADI and PADR) packets received.
Parameters	*[all | <portlist >]* – Specifies a list of ports or all ports to be configured. The default settings are enabled for ID insertion per port, but disabled globally. *circuit_id* – Configures the device ID used for encoding of the circuit ID option. *mac* – Specifies that the Switch MAC address be used to encode the circuit ID option. *ip* – Specifies that the Switch IP address be used to encode the circuit ID option. *udf* – A user defined string to be used to encode the circuit ID option. The maximum length is 32. The default encoding for the device ID option is the Switch IP address. *state* – Specify to enable or disable PPPoE circuit ID insertion for the ports listed.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To enable port 1 PPPoE circuit ID insertion function and use MAC of switch:

```
DGS-2000-28MP:5# config pppoe circuit_id_insertion ports 1 circuit_id mac
Command: config pppoe circuit_id_insertion ports 1 circuit_id mac


Success.

DGS-2000-28MP:5# config pppoe circuit_id_insertion ports 1 state enable
Command: config pppoe circuit_id_insertion ports 1 state enable


Success.
```

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-2000-28MP:5# show pppoe circuit_id_insertion
Command: show pppoe circuit_id_insertion

Status : Enabled
```

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 >}**
Description	The **show pppoe circuit_id_insertion ports** command allows the user to view the configuration of PPPoE ID insertion for each port.
Parameters	*{all | <portlist >}* - Specifies which ports to display. If no ports are specified, all ports configuration will be listed.
Restrictions	None.

Example usage:

To view the PPPoE circuit ID configuration for ports 1 to 3:

```
DGS-2000-28MP:5# show pppoe circuit_id_insertion ports 1-3
Command: show pppoe circuit_id_insertion ports 1-3

Port  State      Circuit ID
----- ---------- --------------------------------------------
1     Enabled    Switch MAC
2     Disabled   Switch IP
3     Disabled   Switch IP
```

10

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
enable snmp	
disable snmp	
show snmp global state	
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 16> <oid_mask 16 view_type [included | excluded]
delete snmp view	<view_name 32> [all | <oid 16>]
show snmp view	{<view_name 32>}
create snmp community	<community_string 32> <username 32>
create snmp community_masking	<community_string(100)> <username(20)>
delete snmp community	<community_string 32>
delete snmp all_community	
show snmp community	{<community_string 32>}
create snmp group	<groupname 32> [v1 | v2c | v3 [noauth_nopriv | auth_nopriv | auth_priv]] {read_view <view_name 32> | write_view <view_name 32> | notify_view <view_name 32>}

Command	Parameter
delete snmp group	<groupname 32> [v1 | v2c | v3] [auth_nopriv | auth_priv | noauth_priv]
show snmp groups	
create snmp host	<ipaddr> [v1 <username 32> | v2c <username 32> | v3 [noauth_nopriv | auth_nopriv | auth_priv] <username 32>]
create snmp v6host	<ip6_addr> [v1 <username 32> | v2c <username 32> | v3 [noauth_nopriv | auth_nopriv | auth_priv] <username 32>]
delete snmp host	[host <Host_IP_address> | v6host <Host_IPv6_address>]
show snmp v6host	[host {<ipaddr>} | v6host {<ipv6_addr>}]
config snmp engineID	<snmp_engineID 64>
show snmp engineID	
config snmp traps	{ address_binding | stp_new_root | stp_topo_change | authenticate | coldstart | warmstart | linkchange { ports [<portlist> | all] } | firmware_upgrade | port_security_violation | lbd | duplicate_ip_detected | traffic_control { type [storm_cleared | storm_occurred | both]} | dos_prevention | poe_onoff | poe_error | poe_over_budget | flood_fdb | all } state [enable | disable]
show snmp traps	
config snmp system_location	<string 32>
config snmp system_name	<string 32>
config snmp system_contact	<string 32>
enable community_encryption	
disable community_encryption	
show community_encryption	

Each command is listed in detail, as follows:

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-2000-28MP:5# enable snmp
Command: enable snmp
```

```
Success.
DGS-2000-28MP:5#
```

disable snmp

Purpose	To disable SNMP support.
Syntax	**disable snmp**
Description	The **disable snmp** command enables 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-2000-28MP:5# disable snmp
Command: disable snmp

Success.
DGS-2000-28MP: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 SNMP global state on the Switch:

```
DGS-2000-28MP:5# show snmp global state
Command: show snmp global state

SNMP Global State : Enable

DGS-2000-28MP:5#
```

create snmp user

Purpose	To create a new SNMP user and add the 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 the user to an existing SNMP group.
Parameters	*<username 32>* − The new SNMP username, up to 32 alphanumeric

	characters. *<groupname 32>* − The SNMP groupname the new SNMP user is associated with, up to 32 alphanumeric characters. *auth* - The user may also choose the type of authentication algorithms used to authenticate the snmp user. The choices are: • *MD5* − Specifies that the HMAC-MD5-96 authentication level to be used. md5 may be utilized by entering one of the following: • *<auth password 32>* - A string of between 1 and 32 alphanumeric characters used to authorize the agent to receive packets for the host. • *SHA* − Specifies that the HMAC-SHA-96 authentication level will be used. • *<priv_password 32>* - A string of between 1 and 32 alphanumeric characters used to authorize the agent to receive packets for the host. • *DES* − 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-2000-28MP:5# create snmp user dlink SW22 v3 MD5 1234 DES jklj22
Command: create snmp user dlink SW22 v3 MD5 1234 DES jklj22

Success.
DGS-2000-28MP: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	*<username 32>* − 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-2000-28MP:5# delete snmp user dlink v3
Command: delete snmp user dlink v3

Success.
DGS-2000-28MP: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-2000-28MP: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-2000-28MP: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 16> <oid_mask 16 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	*<view_name 32>* − A string of up to 30 alphanumeric characters that identifies the SNMP view to be created. *<oid 16>* − The object ID that identifies an object tree (MIB tree) to be included or excluded from access by an SNMP manager. *<oid_mask 16>* − The object ID mask that identifies an object tree (MIB tree) to be included or excluded from access by an SNMP manager. *included* − Includes this object in the list of objects that an SNMP manager can access. *excluded* − Excludes this object from the list of objects that an SNMP manager can access.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To create an SNMP view:

```
DGS-2000-28MP: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-2000-28MP: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 16>]**
Description	The **delete snmp view** command removes an SNMP view previously created on the Switch.
Parameters	*<view_name 32>* − A string of up to 32 alphanumeric characters that identifies the SNMP view to be deleted. *[all | <oid 32>]* − The object ID that identifies an object tree (MIB tree) that is deleted from the Switch.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To delete all configured SNMP view from the Switch:

```
DGS-2000-28MP:5#  delete snmp view dlink all
Command: delete snmp view dlink all

Success.
DGS-2000-28MP: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-2000-28MP: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-2000-28MP: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	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: 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	<*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. <*username 32*> − A string of up to 32 alphanumeric characters that 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-2000-28MP:5# create snmp community dlinkgroup dlink
Command: create snmp community dlinkgroup dlink

Success.

DGS-2000-28MP:5#
```

create snmp community_masking

Purpose	To create SNMP community with encrypted string
Syntax	**create snmp community_masking <community_string(100)> <username(20)>**
Description	The **create snmp community_masking** command is used to create SNMP community with encrypted string.
Parameters	<*community_string 100*> − A string of up to 100 encrypted for community string.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To create the SNMP community string ‘test’:

```
DGS-2000-28MP:5# create snmp community_masking "@^3AD3BEBA355EDACF" "username"
Command: create snmp community_masking @^3AD3BEBA355EDACF username


Success.

DGS-2000-28MP:5# show snmp community
Command: show snmp community

SNMP Community Table
(Maximum Entries : 10)
Community Name                  User Name
---------------                 ----------
******                          ReadOnly
******                          ReadWrite
test                            username

Total Entries       : 3

DGS-2000-28MP:
```

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	<*community_string 32*> − A string of up to 32 alphanumeric characters that is used to identify 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-2000-28MP:5# delete snmp community dlinkgroup
Command: delete snmp community dlinkgroup

Success.
DGS-2000-28MP:5#
```

delete snmp all_community

Purpose	To remove all SNMP communities string from the Switch.
Syntax	**delete snmp all_community**

Description	The **delete snmp all_community** command removes all SNMP communities (which includes default communities).
Parameters	<*community_string 32*> − A string of up to 32 alphanumeric characters that is used to identify 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 all the SNMP community:

```
DGS-2000-28MP:5# delete snmp all_community
Command: delete snmp all_community


Success.

DGS-2000-28MP:5# show snmp community
Command: show snmp community

SNMP Community Table
(Maximum Entries : 10)
Community Name                  User Name
---------------                 ----------

Total Entries      : 0
```

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	<*community_string 32*> − 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-2000-28MP: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-2000-28MP: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]] {read_view <view_name 32> | write_view <view_name 32> | notify_view <view_name 32>}**
Description	The **create snmp group** command creates a new SNMP group, or a table that maps SNMP users to SNMP views.
Parameters	*<groupname 32>* − A name of up to 30 alphanumeric characters that identifies the SNMP group the new SNMP user is to be associated with. *v1* – Specifies that SNMP version 1 is to be used. The Simple Network Management Protocol (SNMP), version 1, is a network management protocol that provides a means to monitor and control network devices. *v2c* – Specifies that SNMP version 2c is to be used. The SNMP v2c supports both centralized and distributed network management strategies. It includes improvements in the Structure of Management Information (SMI) and adds some security features. *v3* – Specifies that the SNMP version 3 is to be used. SNMP v3 provides secure access to devices through a combination of authentication and encrypting packets over the network. SNMP v3 adds: • Message integrity − Ensures that packets have not been tampered with during transit. • Authentication − Determines if an SNMP message is from a valid source. • Encryption − Scrambles the contents of messages to prevent it from being viewed by an unauthorized source. *noauth_nopriv* − Specifies that there is no authorization and no encryption of packets sent between the Switch and a remote SNMP manager. *auth_nopriv* − Specifies that authorization is required, but there is no encryption of packets sent between the Switch and a remote SNMP manager. *auth_priv* − Specifies that authorization is required, and that packets sent between the Switch and a remote SNMP manger are encrypted. *read_view* – Specifies that the SNMP group being created can request SNMP messages. • *<view_name 32>* − A string of up to 32 objects that a remote SNMP manager is allowed to access on the Switch. *write_view* – Specifies that the SNMP group being created has write privileges. • *<view_name 32* identifies the group of MIB objects that a

	remote SNMP manager is allowed to access on the Switch. *notify_view* − Specifies that the SNMP group being created can receive SNMP trap messages generated by the Switch's SNMP agent. • <*view_name 32*> − 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-2000-28MP: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-2000-28MP:5#
```

delete snmp group

Purpose	To remove an SNMP group from the Switch.
Syntax	**delete snmp group <groupname 32> [v1 | v2c | v3] [auth_nopriv | auth_priv | noauth_priv]**
Description	The **delete snmp group** command removes an SNMP group from the Switch.
Parameters	<*groupname 32*> − 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-2000-28MP:5#  delete snmp group sg1 v2c
Command: delete snmp group sg1 v2c

Success.
DGS-2000-28MP: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-2000-28MP: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-2000-28MP: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	*<ipaddr>* − The IP address of the remote management station to serve as the SNMP host for the Switch. *v1* – Specifies that SNMP version 1 is to be used. The Simple Network Management Protocol (SNMP), version 1, is a network management protocol that provides a means to monitor and control network devices. *v2c* – Specifies that SNMP version 2c is to be used. The SNMP v2c supports both centralized and distributed network management strategies. It includes improvements in the Structure of Management Information (SMI) and adds some security features. *v3* – Specifies that the SNMP version 3 is to be used. SNMP v3 provides secure access to devices through a combination of authentication and encrypting packets over the network. SNMP v3 adds: • Message integrity − ensures that packets have not been tampered with during transit. • Authentication − determines if an SNMP message is from a valid source.

	• Encryption − scrambles the contents of messages to prevent it being viewed by an unauthorized source. *<username 32>* − 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. *noauth_nopriv* − Specifies that there is no authorization and no encryption of packets sent between the Switch and a remote SNMP manager. *auth_nopriv* − Specifies that authorization is required, but there is no encryption of packets sent between the Switch and a remote SNMP manager. *auth_priv* − Specifies that authorization is required, and that packets sent between the Switch and a remote SNMP manger are encrypted.
Restrictions	Only Administrator and oper-level users can issue this command

Example usage:

To create an SNMP host to receive SNMP messages:

```
DGS-2000-28MP: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-2000-28MP: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	*<ipv6_addr>* − The IPv6 address of the remote management station to serve as the SNMP host for the Switch. *v1* – Specifies that SNMP version 1 is to be used. The Simple Network Management Protocol (SNMP), version 1, is a network management protocol that provides a means to monitor and control network devices. *v2c* – Specifies that SNMP version 2c is to be used. The SNMP v2c supports both centralized and distributed network management strategies. It includes improvements in the Structure of Management Information (SMI) and adds some security features. *v3* – Specifies that the SNMP version 3 is to be used. SNMP v3 provides secure access to devices through a combination of authentication and encrypting packets over the network. SNMP v3 adds: • Message integrity − ensures that packets have not been tampered with during transit. • Authentication − determines if an SNMP message is from a valid source.

	• Encryption − scrambles the contents of messages to prevent it being viewed by an unauthorized source. *<username 32>* − 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. *noauth_nopriv* − Specifies that there is no authorization and no encryption of packets sent between the Switch and a remote SNMP manager. *auth_nopriv* − Specifies that authorization is required, but there is no encryption of packets sent between the Switch and a remote SNMP manager. *auth_priv* − Specifies that authorization is required, and that packets sent between the Switch and a remote SNMP manger are encrypted.
Restrictions	Only Administrator and oper-level users can issue this command

Example usage:

To create an SNMP host to receive SNMP messages:

```
DGS-2000-28MP:5# create snmp v6host 3000::1 v3 noauth_nopriv dlink
Command: create snmp v6host 3000::1 v3 noauth_nopriv dlink

Success.
DGS-2000-28MP:5#
```

delete snmp host

Purpose	To remove a recipient of SNMP traps generated by the Switch's SNMP agent.
Syntax	**delete snmp host [host <Host_IP_address> | v6host <Host_IPv6_address>]**
Description	The **delete snmp host** command deletes a recipient of SNMP traps generated by the Switch's SNMP agent.
Parameters	*host <Host_IP_address>* − The IP address of a remote SNMP manager that receives SNMP traps generated by the Switch's SNMP agent. *v6host <Host_IPv6_address>* - 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-2000-28MP:5# delete snmp host 10.90.90.22
Command: delete snmp host 10.90.90.22

Success.
DGS-2000-28MP:5#
```

show snmp host

Purpose	To display the recipient of SNMP traps generated by the Switch's SNMP agent.
Syntax	**show snmp host [host {<ipaddr>} | v6host {<ipv6_addr>}]**
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	*host <Host_IP_address>* − The IP address of a remote SNMP manager that receives SNMP traps generated by the Switch's SNMP agent. *v6host <Host_IPv6_address>* - 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 SNMP hosts on the Switch:

```
DGS-2000-28MP: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-2000-28MP: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	*<snmp_engineID 64>* − A string, of between 10 and 64 alphanumeric characters, to be used to identify the SNMP engine on the Switch.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To give the SNMP agent on the Switch:

```
DGS-2000-28MP:5# config snmp engineID 12345678900
Command: config snmp engineID 12345678900
```

```
Success.
DGS-2000-28MP:5#
```

show snmp engineID

Purpose	To display SNMP community strings configured on the Switch.
Syntax	**show snmp engineID**
Description	The **show snmp engineID** command displays SNMP engine ID configured on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display the currently SNMP engine ID:

```
DGS-2000-28MP:5# show snmp engineID
Command: show snmp engineID

Default SNMP Engine ID      : 800000ab03ecade062afa0
SNMP Engine ID              : 1213123123123123123123
```

config snmp traps

Purpose	To configure SNMP traps for individual features.
Syntax	**config snmp traps { address_binding | stp_new_root | stp_topo_change | authenticate | coldstart | warmstart | linkchange { ports [<portlist> | all] } | firmware_upgrade | port_security_violation | lbd | duplicate_ip_detected | traffic_control { type [storm_cleared | storm_occurred | both]} | dos_prevention | poe_onoff | poe_error | poe_over_budget | flood_fdb | all } state [enable | disable]**
Description	The **config snmp traps** command controls capability for sending traps when specific event occurred.
Parameters	*address_binding* – Address binding related events *stp_new_root* – Spanning Tree New root elected event *stp_topo_change* – Spanning Tree topology change event *authenticate* – 802.1x authentication related event *coldstart* – System coldstart event *warmstart* – System warmstart event *linkchange {ports <portlist> | all}* – System physical port link-change event. Port can specified via “ports” parameter. *firmware_upgrade* – Firmware upgrade related events *port_security_violation* – Port security related event *lbd* – Loopback detection related event *duplicate_ip_detected* – Duplicated IP detected event *traffic_control {type [storm_cleared | storm_occurred | both]}* – Traffic control related event. Storm type can be specified via “type” parameter *dos_prevention* – DoS prevention related events

	poe_onoff – PoE on/off event *poe_error* – PoE error event p*oe_over_budget* – PoE over max budget event *flood_fdb* – Flood fdb event *all* – all events listed *state [enable* | *disable]* – Specify the state individual feature
Restrictions	Only Administrator or operator-level users can issue this command

Example usage:

To enable the SNMP trap for address binding feature:

```
DGS-2000-28MP:5# config snmp traps address_binding state enable
Command: config snmp traps address_binding state enable

Success.

DGS-2000-28MP: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 display the current SNMP trap configuration:

```
DGS-2000-28MP:5#  show snmp traps
Command: show snmp traps

 SNMP Authentication Traps       : Enabled
 Coldstart Traps                 : Enabled
 Warmstart Traps                 : Enabled
 Linkchange Traps                : Enabled on ports 1-28
 STP New Root Traps              : Enabled
 STP Topology Change Traps       : Enabled
 Firmware Upgrade State Traps    : Enabled
 Port Security violation Traps   : Enabled
 Loopback detection Traps        : Enabled
 Traffic control Traps           :Storm Occurred and Storm Cleared
 DoS Prevention violation Traps  : Enabled
 Duplicate IP Detected Traps     : Enabled
 address_binding Traps           : Enabled
```

```
flood_fdb Traps                 : Enabled
PoE Power On/Off Traps          : Enabled
PoE Power Error Traps           : Enabled
over max power budget Traps     : Enabled

DGS-2000-28MP:5#
```

config snmp system_location

Purpose	To enter a description of the location of the Switch.
Syntax	**config snmp sysem_location <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-2000-28MP:5# config snmp system_location HQ5F
Command: config snmp system_location HQ5F

Success.
DGS-2000-28MP:5#
```

config snmp system_name

Purpose	To define the name for the Switch.
Syntax	**config snmp system_name <string 32>**
Description	The **config snmp system_name** 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:

```
DGS-2000-28MP:5# config snmp system_name DLINK_switch
Command: config snmp system_name DLINK_switch

Success.
DGS-2000-28MP:5#
```

config snmp system_contact

Purpose	To define the name for the Switch.

Syntax	**config snmp system_contact <string 32>**
Description	The **config snmp system_contact** command is used to configure the contact information presented in swtch information.
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 contact name:

```
DGS-2000-28MP:5# config snmp system_contact DLINK_support
Command: config snmp system_contact DLINK_support

Success.
DGS-2000-28MP:5#
```

enable community_encryption

Purpose	To enable encryption mechanism of SNMP community string.
Syntax	**enable community_encryption**
Description	The **enable community_encryption** command enables the mechanism to encryption SNMP community string which provides higher security level for user.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command

Example usage:

To enable encryption of SNMP community string:

```
DGS-2000-28MP:5# enable community_encryption
Command: enable community_encryption

Success.
```

disable community_encryption

Purpose	To disable encryption mechanism of SNMP community string.
Syntax	**disable community_encryption**
Description	The **disable community_encryption** command disables the mechanism of encryption SNMP community string.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command

Example usage:

To disable encryption of SNMP community string:

```
DGS-2000-28MP:5# disable community_encryption
Command: disable community_encryption
```

Success.

show community_encryption	
Purpose	To display cureent encryption mechanism state of SNMP community string.
Syntax	**show community_encryption**
Description	The **show community_encryption** command disables the mechanism of encryption SNMP community string.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command

Example usage:

To display current state of SNMP community encryption:

```
DGS-2000-28MP:5# show community_encryption
Command: show community_encryption


SNMP Community Encryption State : Disabled


DGS-2000-28MP:5#
```

11

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	[cfg_fromTFTP [<ipaddr> | <ipv6_addr>] <path_filename 64>] | [firmware_fromTFTP [<ipaddr> | <ipv6_addr>] < path_filename 64>]
upload	[[firmware_toTFTP [<ipaddr> | <ipv6_addr>] <path_filename 64>] | [cfg_toTFTP [<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 [cfg_fromTFTP [<ipaddr> | <ipv6_addr>] <path_filename 64>] | [firmware_fromTFTP [<ipaddr> | <ipv6_addr>] < path_filename 64>] | [log_fromTFTP [<ipaddr> | <ipv6_addr>] <path_filename 64>] | [log_toTFTP [<ipaddr> | <ipv6_addr>] <path_filename 64>]**
Description	The **download** command downloads a firmware, boot, log or switch configuration file from a TFTP server.
Parameters	*cfg_fromTFTP* − Downloads a switch configuration file from a TFTP server. <*ipaddr*> − The IPv4 address of the TFTP server. <*ipv6_addr*> − The IPv6 address of the TFTP server. <*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. *startup* − Indicates the Configuration file is to be downloaded to the startup config. *firmware_fromTFTP* − Downloads and installs firmware on the Switch from a TFTP server. < *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.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To download a firmware file:

DGS-2000-28MP:5# download firmware_fromTFTP 10.90.90.123 DGS-2000-SERIES-1-00-008-ALL.hex

Command: download firmware_fromTFTP 10.90.90.123 DGS-2000-SERIES-1-00-008-ALL.hex

```
Connecting to Server.....    Done
Transfer firmware.....       Done
Upgrade processing.....      Done
Firmware upgrade successfully!


Success.

DGS-2000-28MP:5#
```

To download a configuration file:

```
DGS-2000-28MP:5# download cfg_fromTFTP 10.90.90.123 test.cfg
Command: download cfg_fromTFTP 10.90.90.123 test.cfg

Connecting to server.....    Done
Transfer configuration.....  Done. Do not power off!!
Config restore successfully!

Success.
```

upload

Purpose	To upload the current switch settings to a TFTP server.
Syntax	**upload [[firmware_toTFTP [<ipaddr> | <ipv6_addr>] <path_filename 64>] | [cfg_toTFTP [<ipaddr> | <ipv6_addr>] <path_filename 64>**
Description	The **upload** command uploads the Switch's current settings to a TFTP server.
Parameters	*firmware_toTFTP* − Specifies that the Switch's current firmware are to be uploaded to the TFTP server. <*ipaddr*> − The IPv4 address of the TFTP server. The TFTP server must be on the same IP subnet as the Switch. <*ipv6_addr*> − The IPv6 address of the TFTP server. The TFTP server must be on the same IP subnet as the Switch. <*path_filename 64*> − The location of the Switch configuration file on the TFTP server. *cfg_fromTFTP* − Uploads a switch configuration file from a TFTP server.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To upload a configuration file:

```
DGS-2000-28MP:5# upload cfg_toTFTP 10.90.90.123 test.cfg
Command: upload cfg_toTFTP 10.90.90.123 test.cfg

Connecting to server.....    Done
Transfer configuration.....    Done. Do not power off!!
Config backup successfully!

Success.
```

12

DHCP AUTO COMMANDS

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

Command	Parameter
enable autoconfig	
disable autoconfig	
config autoconfig	timeout <interger 1-65535>
show autoconfig	
enable autoimage	
disable autoimage	
show autoimage	

Each command is listed in detail, as follows:

enable autoconfig	
Purpose	Used to activate the auto configuration function for the Switch.
Syntax	**enable autoconfig**
Description	DHCP auto config is feature that helps to restrive the config file user specified after device reboot automatically. Furthermore, the DHCP server must be properly configured in order to disturibe the correct information. 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	When autoconfig is enabled, switch turned into DHCP client mode AUTOMATICALLY after device reboot. Please be aware the DHCP server MUST capable to transmit the following options: DHCP option6 (Domain Name Server.), option 66 (TFTP server name), option 67 (Bootfile name), and option 150 (TFTP Server Address) with the correct contents which guide the swtich to contact the TFTP server and obtain the config file. If the switch failed to complete the autoconfig process, the origin config will be used after process timed out.

Example usage:

To enable auto configuration on the Switch:

```
DGS-2000-28MP:5# enable autoconfig
Command: enable autoconfig


Success.
```

```
DGS-2000-28MP:5#
```

disable autoconfig

Purpose	Use this to deactivate DHCP auto configuration function.
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-2000-28MP:5# disable autoconfig
Command: disable autoconfig

Success.

DGS-2000-28MP:5#
```

config autoconfig timeout

Purpose	Used to configure the timeout period.
Syntax	**config autoconfig timeout <integer 1-65535>**
Description	The **config autoconfig** command is used to configure the time out range from 1~65535 seconds.
Parameters	<*1-65535*> - Specify the timeout range from 1~65535 seconds
Restrictions	None.

Example usage:

To display the autoconfig status:

```
DGS-2000-28MP:5# config autoconfig timeout 300
Command: config autoconfig timeout 300

Success.

DGS-2000-28MP: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-2000-28MP:5# show autoconfig
Command: show autoconfig

Autoconfig State: Disabled
Timeout        : 300 sec


Success.
DGS-2000-28MP:5#
```

enable autoimage

Purpose	Used to activate the auto image 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	When autoconfig is enabled, switch turned into DHCP client mode AUTOMATICALLY after device reboot. Please be aware the DHCP server MUST capable to transmit the following options: DHCP option6 (Domain Name Server.), option 125 (Vendor-Specific Information), and option 150 (TFTP Server Address) with the correct contents which guide the swtich to contact the TFTP server and obtain the config file. The detail information about DHCP option 125: Dlink enterprise id (171) : 0x00 0x00 0x00 0xAB (Fixed) Suboption Length : 0x08 (Variable) Suboption code:0x01 (Fixed) File length: 0x06 (Variable) fw.hex : 0x66 0x77 0x2E 0x68 0x65 0x78 (Variable)

Example usage:

To enable auto configuration on the Switch:

```
DGS-2000-28MP:5# enable autoconfig
Command: enable autoconfig


Success.
DGS-2000-28MP:5#
```

disable autoimage

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-2000-28MP:5# disable autoconfig
Command: disable autoconfig


Success.

DGS-2000-28MP:5#
```

show autoimage

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-2000-28MP:5# show autoconfig
Command: show autoconfig

Autoconfig State: Disabled
Timeout        : 300 sec


Success.
DGS-2000-28MP:5#
```

13

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 | delete] ipif System <ipaddr>
config dhcp_relay hops	<value 1-16>
config dhcp_relay time	<sec 0-65535>
config dhcp_relay vlan	[<vlan_name 20> | vlanid <vidlist>] state [enable | disabel]
config dhcp_relay port	<portlist> state [enable | disable]
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]
config dhcp_local_relay port	<portlist> state [enable | disable]
show dhcp_local_relay	
enable dhcpv6_relay	
disable dhcpv6_relay	
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>]]
show dhcpv6_relay	{ipif system}

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 operate-level users can issue this command.

Example usage:

To enable DHCP Relay on the Switch:

```
DGS-2000-28MP:5# enable dhcp_relay
Command: enable dhcp_relay

Success.
DGS-2000-28MP: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 operate-level users can issue this command.

Example usage:

To disable DHCP Relay on the Switch:

```
DGS-2000-28MP:5# disable dhcp_relay
Command: disable dhcp_relay

Success.
DGS-2000-28MP:5#
```

config dhcp_relay

Purpose	To define or remove the DHCP server location.
Syntax	**config dhcp_relay [add | delete] ipif System <ipaddr>**
Description	The DHCP server must be specified for DHCP relay process.
Parameters	<*ipaddr*> − The IP address of the DHCP server. Up to 4 servers can be defined.
Restrictions	Only Administrator or operate-level users can issue this command.

Example usage:

To add a DHCP server as a DHCP Relay server:

```
DGS-2000-28MP:5# config dhcp_relay add ipif System 10.6.150.49
Command: config dhcp_relay add ipif System 10.6.150.49
```

```
Success.
DGS-2000-28MP:5#
```

config dhcp_relay hops

Purpose	To identify the number of hops allowed for DHCP relay.
Syntax	**config dhcp_relay hops <value 1-16>**
Description	The **config dhcp_relay hops** command configures the DHCP/BOOTP relay feature. Along with DHCP process, the DHCP relay agent increments the hop count before forwarding DHCP packets to the server.
Parameters	<*value 1-16*> − Specifies the maximum number of relay agent hops that the DHCP packets can cross.
Restrictions	Only Administrator or operate-level users can issue this command.

Example usage:

To configure the DHCP relay on the Switch:

```
DGS-2000-28MP:5# config dhcp_relay hops 12
Command: config dhcp_relay hops 12

Success.
DGS-2000-28MP:5#
```

config dhcp_relay time

Purpose	To identify the DHCP relay time.
Syntax	**config dhcp_relay hops <value 1-16>**
Description	The **config dhcp_relay hops** command configures the DHCP/BOOTP relay feature. The time record in DHCP packet and started the counting when client intiate the very first DHCP packet DHCP discover and DHCP request). DHCP packet would be dropped once the value is greater thatn the time value configured. Value 0 means the switch will not examine this field of the DHCP packets.
Parameters	<*value 1-16*> − Specifies the maximum number of relay agent hops that the DHCP packets can cross.
Restrictions	Only Administrator or operate-level users can issue this command.

Example usage:

To configure the DHCP relay on the Switch:

```
DGS-2000-28MP:5# config dhcp_relay time 15
Command: config dhcp_relay time 15

Success.
DGS-2000-28MP:5#
```

config dhcp_relay vlan

Purpose	To configure the DHCP relay feature in VLAN basis.
Syntax	**config dhcp_relay vlan [<vlan_name 20> | vlanid <vidlist>] state [enable | disabel]**
Description	The **config dhcp_relay vlan** command specfies the DHCP relay state for individual VLAN group. This feature helps user to bind the VLAN group which aquires the DHCP relay feature. BOTH VLAN group and port MUST be state enabled in order to process the DHCP relay.
Parameters	*<vlan_name 20>* − Specifies the VLAN group via VLAN name string. *vlanid <vidlist>* − Specifies the VLAN group via VLAN ID. *state [enable | disable]* – The state switch for VLAN group specified.
Restrictions	Only Administrator or operate-level users can issue this command.

Example usage:

To configure the DHCP relay on the Switch:

```
DGS-2000-28MP:5# config dhcp_relay vlan default state enable
Command: config dhcp_relay vlan default state enable


Success.

DGS-2000-28MP:5#
```

config dhcp_relay port

Purpose	To configure the DHCP relay feature in port basis.
Syntax	**config dhcp_relay port <portlist> state [enable | disable]**
Description	The **config dhcp_relay port** command specfies the DHCP relay state for specific port. This feature helps user to bind the port which aquires the DHCP relay feature. BOTH VLAN group and port MUST be state enabled in order to process the DHCP relay.
Parameters	*<portlist>* − Specifies a port or a range of ports. *state [enable | disable]* – The state switch for port(s) specified.
Restrictions	Only Administrator or operate-level users can issue this command.

Example usage:

To configure the DHCP relay on the Switch:

```
DGS-2000-28MP:5# config dhcp_relay port 1-3 state enable
Command: config dhcp_relay port 1-3 state enable


Success.

DGS-2000-28MP:5#
```

config dhcp_relay option_82

Purpose	To configure the check, policy and state of DHCP relay agent information option 82 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	*check:* used to configure the check of DHCP relay agent information option 82 of the Switch. *enable* – 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. *disable* – When the field is toggled to disable, the relay agent will not check the validity of the packet's option 82 field. policy: used to configure the re-forwarding policy of DHCP relay agent information option 82 of the Switch. *replace* − The option 82 field will be replaced if the option 82 field already exists in the packet received from the DHCP client. *drop* − The packet will be dropped if the option 82 field already exists in the packet received from the DHCP client. *keep* − The option 82 field will be retained if the option 82 field already exists in the packet received from the DHCP client. state: used to configure the state of DHCP relay agent information option 82 of the Switch. *enable* − 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 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. *disable* − 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.
Restrictions	Only Administrator or operate-level users can issue this command.

Example usage:

To disable the DHCP relay option 82 on the Switch:

```
DGS-2000-28MP:5# config dhcp_relay option_82 state disable
Command: config dhcp_relay option_82 state disable

Success.
DGS-2000-28MP: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-2000-28MP: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 VID List                                : 1
 DHCP Relay PortList                                : 1-3
 DHCP Relay Agent Information Option82 State        : Enabled
 DHCP Relay Agent Information Option82 Check        : Disabled
 DHCP Relay Agent Information Option82 Policy       : replace
 DHCP Relay Agent Information Option82 Remote ID    : F4-8C-EB-E9-EE-00

 Interface    Server 1        Server 2        Server 3        Server 4
 ---------    ---------------  ---------------  ---------------  ---------------
 System       10.1.1.1


DGS-2000-28MP: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-2000-28MP:5# enable dhcp_local_relay
Command: enable dhcp_local_relay

Success
DGS-2000-28MP: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-2000-28MP:5# disable dhcp_local_relay
Command: disable dhcp_local_relay

Success.
DGS-2000-28MP:5#
```

config dhcp_local_relay vlan

Purpose	To configure the DHCP local relay feature in VLAN basis.
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	*<vlan_name 20>* – the VLAN name identifier *vlanid <vidlist>* – The VLAN tag identifier *state [enable | disable]* – enable or disable of 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-2000-28MP:5# config dhcp_local_relay vlan vlanid 10 state disable
```

```
Command: config dhcp_local_relay vlan vlanid 10 state disable


Success.
DGS-2000-28MP:5#
```

config dhcp_local_relay port

Purpose	To configure the DHCP local relay feature in port basis.
Syntax	**config dhcp_local_relay port <portlist> state [enable | disable]**
Description	Port must be added into DHCP local relay list in order to execute the DHCP local relay.
Parameters	*<portlist>* − Specifies a port or a range of ports. *state [enable | disable]* – The state switch for port(s) specified.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To enable port 1-3 for VLAN of DHCP Local Relay:

```
DGS-2000-28MP:5# config dhcp_local_relay port 1-3 state enable
Command: config dhcp_local_relay port 1-3 state enable


Success.

DGS-2000-28MP: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-2000-28MP:5#  show dhcp_local_relay
Command: show dhcp_local_relay

DHCP Local Relay Status        : Disabled
DHCP Local Relay VID List      : 1
DGS-2000-28MP: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-2000-28MP:5# enable dhcpc6_relay
Command: enable dhcpc6_relay

Success.
DGS-2000-28MP:5#
```

disable dhcp6_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-2000-28MP:5# disable dhcpv6_relay
Command: disable dhcpv6_relay

Success.
DGS-2000-28MP:5#
```

config dhcpv6_relay

Purpose	Used to add or delete a destination IP address to or from the switch's DHCPv6 relay table.
Syntax	**config dhcpv6_relay [add | delete] ipif System <ipv6_addr>**
Description	The **config dhcpv6_relay** command can add or delete an IPv6 destination address to forward (relay) DHCPv6 packets.
Parameters	*add* − Add an IPv6 destination to the DHCPv6 relay table. *delete* − Remove an IPv6 destination to the DHCPv6 relay table. *ipif system* − The name of the IP interface in which DHCPv6 relay is to be enabled. <*ipv6_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-2000-28MP:5# config dhcpv6_relay add ipif System 3000::1
Command: config dhcpv6_relay add ipif System 3000::1

Success.
DGS-2000-28MP: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-2000-28MP:5# config dhcpv6_relay hop_count 3
Command: config dhcpv6_relay hop_count 3

Success.
DGS-2000-28MP: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	*state [enable | disable]* - 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-2000-28MP:5# config dhcpv6_relay hop_count 3
Command: config dhcpv6_relay hop_count 3

Success.
DGS-2000-28MP: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 of all interfaces, or if an IP interface name is specified, the DHCPv6 relay configuration for that IP interface.
Parameters	None.
Restrictions	None.

Example usage:

To display DHCPv6 Relay settings:

```
DGS-2000-28MP:5# show dhcpv6_relay
Command: show dhcpv6_relay

 DHCPv6 Relay Status                 : Disabled
 DHCPv6 Relay Hops Count Limit       : 4
 DHCPv6 Relay Option37 State         : Disabled
 DHCPv6 Relay Option37 Check         : Disabled
 DHCPv6 Relay Option37 Remote ID     : EC-AD-E0-62-AF-A0
 ------------------------------------------------

Interface       Server Address
--------------- ---------------

DGS-2000-28MP:5#
```

14

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 >
show statistics ports	<portlist>
show error ports	<portlist >
show utilization	[ports {<portlist>} | cpu | mem]
clear counters ports	<porlist >
clear log	
show log	{[index <value 1-500> - <value 1-500>] | severity [debug | informational | warning] | module <string 32>}
save log	
config log_save_timing	[log_trigger | on_demand | time_interval <min 1-65535>]
show log_save_timing	
enable command logging	
disable command logging	
show command logging	
show log_software_module	
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 > | all]

Each command is listed in detail, as follows:

show packet ports	
Purpose	To display statistics about the packets sent and received in frames per second by the Switch.
Syntax	**show packet ports <portlist >**
Description	The **show packet ports** command displays statistics about packets sent and received by ports specified in the port list. The results are separated into three tables, labeled A, B, and C in the window below. Table A is relevant to the size of the packets, Table B is relevant to the type of packets and Table C is relevant to the type of frame associated with these packets.
Parameters	*<portlist* > − A port or range of ports whose statistics are to be displayed.
Restrictions	None.

Example usage:

To display the packets analysis for port 5:

DGS-2000-28MP:5# show packet ports 5
Command: show packet ports

Port Number : 5

Frame Size	Frame Counts	Frame/sec	Frame Type	Total	Total/sec
64	2161	5	RX Bytes	8088	128
65-127	249	0	RX Frames	2435	2
128-255	18	0			
256-511	7	0	TX Bytes	3314	1071
512-1023	0	0	TX Frames	3550	3
1024-1518	0	0			
Unicast RX	2000	0			
Multicast RX	35	0			
Broadcast RX	5	0			
Unicast TX	892	0			
Multicast TX	584	0			
Broadcast TX	193	0			

Unicast RX	2158	2
Multicast RX	5	0

```
DGS-2000-28MP:5#
```

show statistics ports

Purpose	To display the packet type statistics for a port or a range of ports.
Syntax	**show statistics ports <portlist >**
Description	The **show statistics ports** command displays the packet statistics in packet type basis.
Parameters	<*portlist* > − A port or range of ports whose error statistics are to be displayed.
Restrictions	None.

Example usage:

To display the statistics of port 5:

```
DGS-2000-28MP:5# show statistics ports 2
Command: show statistics ports 2

 Port Number : 2
 ------------------------
                        TX                      RX
 OutOctets              519669      InOctets    14856095
 OutUcastPkts           7665        InUcastPkts 7665
 OutNUcastPkts          454         InNUcastPkts 8070
 OutErrors              0           InDiscards  8070
 LateCollisions         0           InErrors    0
 ExcessiveCollisions    0           FCSErrors   0
                                    FrameTooLongs 0

DGS-2000-28MP:5#
```

show error ports

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

Example usage:

To display the errors of port 1:

```
DGS-2000-28MP:5# show errors ports 2
Command: show error ports 1
```

```
Port Number : 2
-----------------------

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

DGS-2000-28MP:5#
```

show utilization

Purpose	To display real-time port utilization statistics.
Syntax	**show utilization [ports {<portlist >} | 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 percentage..
Parameters	*ports{* – Entering this parameter will display the current port utilization of the Switch. *<portlist >* – Specifies a range of ports to be displayed. *cpu* – Entering this parameter will display the current CPU utilization of the Switch. *dram* – Entering this parameter will display the current memory utilization of the Switch.
Restrictions	None.

To display the port utilization statistics:

```
DGS-2000-28MP:5# show utilization ports 5
Command: show utilization ports 5

 Port        TX Pkts/sec      RX Pkts/sec      Util
 -----       -------------    -------------    -----
 5           1                0                0
```

To display the cpu utilization statistics:

```
DGS-2000-28MP:5# show utilization cpu
Command: show utilization cpu

CPU Utilization:
-------------------------------------------------------------------------------
```

```
Five Seconds: 1  %
One  Minute : 1  %
Five Minute : 2  %
```

clear counters

Purpose	To clear the Switch's statistics counters.
Syntax	**clear counters ports <porlist >**
Description	The **clear counters** command is used to clear all the counters (includes error counters, packet counters).
Parameters	*<portlist >* – 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-2000-28MP:5#  clear counters ports 2-5
Command: clear counters ports 2-5

Success.
DGS-2000-28MP:5#
```

clear log

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

Example usage:

To clear the log information:

```
DGS-2000-28MP:5# clear log
Command: clear log

Success.
DGS-2000-28MP:5#
```

show log

Purpose	To display the Switch history log.
Syntax	**show log {[index <value 1-500> - <value 1-500>] | severity [debug | informational | warning] | module <string 32>}}**
Description	The **show log** command displays log entries. Furthermore, logs can be filtered via demand.
Parameters	*index <value 1-500>* − The number of entries in the history log to display. *severity [debug | informational | warning]* − Specifies the severity

	type to be displayed. *module* <*string 32*> - Logs can be filtered via different software modules: CLI, LinkStatus, SYSTEM, IP Change, WEB, 802.1x, EOAM
Restrictions	None.

Example usage:

To display the log entries:

```
DGS-2000-28MP:5# show log
Command: show log

Index  Time                 Log Text                                  Log Severity
-------- ----------------- ------------------------------------------ ----------------
3      Jan  2 05:59:30      [LinkStatus]:Port 5 link down             Information
2      Jan  2 05:58:48      [LinkStatus]:Port 5 link up,              Information
                            1Gbps FULL duplex
1      Jan  1 06:40:04      [SYSTEM]:System started up                Critical
```

save log

Purpose	To save the Switch history log.
Syntax	**save log**
Description	The **save log** command saves logs in non-volatile memory.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To save the Switch history log:

```
DGS-2000-28MP:5#  save log
Command: save log

Success.
DGS-2000-28MP:5#
```

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	*log_trigger* – Users who choose this method will have logs saved to the Switch every time a log event occurs on the Switch. *on_demand* – 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. *time_interval <min 1-65535>*– 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.
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-2000-28MP:5# config log_save_timing time_interval 30
Command: config log_save_timing time_interval 30

Success.
DGS-2000-28MP:5#
```

show log_save_timing

Purpose	To check the current log saving mechanism.
Syntax	**show log_save_timing**
Description	The **show log_save_timing** command is used to check the current status of log saving mechanism.
Parameters	None.
Restrictions	None.

Example usage:

To check log saving mechanism:

```
DGS-2000-28MP:5# show log_save_timing
Command: show log_save_timing

Saving log method   : on_demand

DGS-2000-28MP:5#
```

enable command logging

Purpose	To trun on the mechanism to log the command executed.
Syntax	**enable command logging**
Description	"**commad logging**" is feature that logs the command executed. It provides the complete actions executed in the device. Also, it helps in device management and issue debugging.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To turn on command logging on the Switch:

```
DGS-2000-28MP:5# enable command logging
Command: enable command logging
```

```
Success.

DGS-2000-28MP:5#
```

disable command logging

Purpose	To trun off the mechanism to log the command executed.
Syntax	**disable command logging**
Description	"**commad logging**" is feature that logs the command executed. It provides the complete actions executed in the device. Also, it helps in device management and issue debugging.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To turn off command logging on the Switch:

```
DGS-2000-28MP:5# disable command logging
Command: disable command logging


Success.

DGS-2000-28MP:5#
```

show command logging

Purpose	To check current status of command logging mechanism.
Syntax	**show command logging**
Description	"**commad logging**" is feature that logs the command executed. It provides the complete actions executed in the device. Also, it helps in device management and issue debugging.
Parameters	None.
Restrictions	None

Example usage:

To check command logging on the Switch:

```
DGS-2000-28MP:5# show command logging
Command: show command logging

Command Logging State : Enabled

DGS-2000-28MP:5#
```

show log_software_module

Purpose	To check modules that supported in logging mechanism.

Syntax	**show log_software_module**
Description	"**show log_software_module**" shows the modules currently supported in logging mechanism..
Parameters	None.
Restrictions	None

Example usage:

To check modules for logging mechanism:

```
DGS-2000-28MP:5# show log_software_module
Command: show log_software_module

CLI    LinkStatus     SYSTEM  IP Change      WEB     802.1x  EOAM

DGS-2000-28MP: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-2000-28MP:5# enable syslog
Command: enable syslog

Success.
DGS-2000-28MP: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-2000-28MP:5# disable syslog
Command: disable syslog

Success.
```

DGS-2000-28MP: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	*all* − Specifies that the command is to be applied to all hosts. *<index 1-4>* − The syslog host index id. There are four available indices, numbered 1 to 4. *ipaddress [<ipaddr>* | *<ipv6addr>]* − The IPv4 or IPv6 address of the remote host to which syslog messages are to be sent. *severity* − The message severity level indicator. These are described in the table below (Bold font indicates that the corresponding severity level is currently supported on the Switch):

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

Example usage:

To create syslog host:

```
DGS-2000-28MP: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-2000-28MP:5#

config syslog host

Purpose	To configure the syslog protocol to send system log data to a remote host.
Syntax	**config syslog host [all | <index 1-4>] {severity [informational | warning | debug] | facility [local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7] | state [enable | disable] | 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	*all* − Specifies that the command applies to all hosts. *<index 1-4>* − Specifies that the command applies to an index of hosts. There are four available indices, numbered 1 to 4. *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-2000-28MP:5#  config syslog host 1 severity debug
Command: config syslog host 1 severity debug

Success.
DGS-2000-28MP: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	*<index 1-4>* − The syslog host index id. There are four available indices, numbered 1 to 4. *all* − Specifies that the command applies to all hosts.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To delete a previously configured syslog host:

```
DGS-2000-28MP:5# delete syslog host all
Command: delete syslog host all

Success.
DGS-2000-28MP: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	*<index 1-4>* − The syslog host index id. There are four available indices, numbered 1 to 4.
Restrictions	None.

Example usage:

To show Syslog host information:

```
DGS-2000-28MP:5# show syslog host
Command: show syslog host
```

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

Total Entries       : 1

DGS-2000-28MP: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 > | 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	*<portlist >* – A port or range of ports to be configured. *all* − 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-2000-28MP:5# cable diagnostic port 3
Command: cable diagnostic port 3

Port  Type  Link Status   Test Result  Fault Distance (meters)  Length(M)
----- ----- ------------ ------------ ------------------------ ----------
2     GE    Link Up      Pair1:OK     Pair1:N/A                <50
                         Pair2:OK     Pair2:N/A
                         Pair3:OK     Pair3:N/A
                         Pair4:OK     Pair4:N/A


DGS-2000-28MP:5#
```

15

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 <vlan_name (20)> <macaddr> port <port>
delete fdb	<vlan_name 20> <macaddr>
config fdb aging_time	<sec 10-1000000>
show fdb	{port <port > | vlan <vlan_name 32> | vlanid <vidlist (1-4094) | mac_address <macaddr> | static | aging_time}
clear fdb	[vlan <vlan_name 20> | port <port> | all]
create multicast_fdb	<vlanid 1-4094><macaddr>
config multicast_fdb	< vlanid 1-4094> <macaddr> [add | delete] <portlist >
delete multicast_fdb	<vlanid 1-4094> <macaddr>
show multicast_fdb	{vlan <vlan_name 20> | mac_address <macaddr>}
config multicast filter	<portlist> [filter | forward]
show multicast filter port_mode	
enable flood_fdb	
disable flood_fdb	
show flood_fdb	
config flood_fdb	log [enable | disable]
clear flood_fdb	
create auto_fdb	
delete auto_fdb	
show auto_fdb	

Each command is listed in detail, as follows:

create fdb	
Purpose	To create a static entry in the unicast MAC address forwarding table (database)
Syntax	**create fdb vlan <vlanid 1-4094> <macaddr> port <port >**
Description	The **create fdb** command creates a static entry in MAC address forwarding database.

Parameters	<*vlan_name*> − The specific VLAN group name of the MAC address entry. <*macaddr*> − The MAC address to be added to the forwarding table. *port* <*port* > − The port number corresponding to the MAC destination address. The Switch will always forward traffic to the specified device through this port.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To create a static FDB entry:

```
DGS-2000-28MP:5# create fdb vlan default 00-00-00-00-00-02 port 3
Command: create fdb vlan default 00:00:00:00:00:02 port 3

Success.

DGS-2000-28MP:5
```

delete fdb

Purpose	To remove a static entry in the unicast MAC address forwarding table (database)
Syntax	**delete fdb <vlan_name 20> <macaddr>**
Description	The **delete fdb** command removes a static entry in MAC address forwarding database.
Parameters	<*vlan_name*> − The specific VLAN group name of the MAC address entry. <*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 remove MAC address from FDB:

```
DGS-2000-28MP:5# delete fdb default 00-00-00-00-00-02
Command: delete fdb default 00:00:00:00:00:02

Success.

DGS-2000-28MP: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-2000-28MP:5# config fdb aging_time 300
Command: config fdb aging_time 300

Success.
DGS-2000-28MP:5#
```

show fdb

Purpose	To display the current MAC address forwarding database.
Syntax	**show fdb {port <port > | vlan <vlan_name 32> | vlanid <vidlist (1-4094) | mac_address <macaddr> | static | aging_time}**
Description	The **show fdb** command displays the current contents of the Switch's forwarding database.
Parameters	*<port >* − The port number corresponding to the MAC destination address. The Switch always forwards traffic to the specified device through this port. *vlan <vlan_name 32>* − Specify the VLAN group via name string. *vlan <vidlist 1-4094>* − Specify the VLAN group via VID. *<macaddr>* − The MAC address entry in the forwarding table. *static* − Specifies that static MAC address entries are to be displayed. *aging_time* − Displays the aging time for the MAC address forwarding database.
Restrictions	None.

Example usage:

To display unicast MAC address table:

```
DGS-2000-28MP: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-2000-28MP:5#
```

To display the aging time:

```
DGS-2000-28MP:5# show fdb aging_time
Command: show fdb aging_time

Unicast MAC Address Aging Time = 300 sec

DGS-2000-28MP:5#
```

clear fdb

Purpose	To clear the dynamic learned MAC address(es) entry from forwarding database.
Syntax	**clear fdb [vlan <vlan_name 20> | port <port> | all]**
Description	The **clear fdb** command clears the dynamic MAC address entry. The action can be executed on VLNA group or port basis.
Parameters	*vlan* <*vlan_name 32*> − Specify the VLAN group via name string. <*port* > − The port number corresponding to the MAC destination address. The Switch always forwards traffic to the specified device through this port. all – Referring to entire MAC address table
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To clear the MAC address entries in default VLAN

```
DGS-2000-28MP:5# clear fdb vlan default
Command: clear fdb vlan default

Success.

DGS-2000-28MP: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-2000-28MP:5# create multicast_fdb 1 00-00-00-01-02-03
Command: create multicast_fdb 1 00-00-00-01-02-03

Success.
DGS-2000-28MP: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 >**
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. *add* − Specifies that the MAC address is to be added to the forwarding table. Delete will remove the MAC address from the forwarding table. *delete* − Specifies that the MAC address is to be removed from the forwarding table. <*portlist* > − 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-2000-28MP:5# config multicast_fdb 1 00-00-00-01-02-03
Command: config multicast_fdb 1 00-00-00-01-02-03

Success.
DGS-2000-28MP:5#
```

delete multicast_fdb

Purpose	To delete an multicast entry in the Switch's forwarding database.
Syntax	**delete multicast_fdb <vlanid 1-4094> <macaddr>**
Description	The **delete multicast_fdb** command deletes a multicast entry in the Switch's MAC address forwarding database.
Parameters	<*vlanid 1-4094*> − Specify the VLAN group via VID. <*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 the static multicast FDB entry:

```
DGS-2000-28MP:5# delete multicast_fdb 1 01-22-33-44-55-
66
Command: delete multicast_fdb 1 01:22:33:44:55:66


Success.
DGS-2000-28MP: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	*vlan* <*vlan_name 20*> − The name of the VLAN on which the MAC address resides. *mac_address* <*macaddr*> − The MAC address that will be added to the forwarding table.
Restrictions	None.

Example usage:

To display multicast MAC address table:

```
DGS-2000-28MP:5#  show multicast_fdb
Command: show multicast_fdb


Total Entries: 0


DGS-2000-28MP:5#
```

config multicast filter

Purpose	To configure multicast filtering.
Syntax	**config multicast filter <portlist> [filter | forward]**
Description	The **config multicast filter** command enables filtering of multicast addresses in port basis
Parameters	<*portlist* > - A port or range of ports to be configured. *forward_unregistered_groups* - Forwards unregistered multicast packets. *filter_unregistered_groups* - Filter unregistered multicast packets.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure multicast filtering

```
DGS-2000-28MP:5# config multicast filter 2 filter
Command: config multicast filter 2 filter
```

```
Success.

DGS-2000-28MP:5#
```

show multicast filter port_mode

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

Example usage:

To show multicast filtering settings:

```
DGS-2000-28MP:5# show multicast filter port_mode
Command: show multicast filter port_mode

Multicast Filter Mode For Unregistered Group:
        Forwarding List: 1,3-28
        Filtering  List: 2

DGS-2000-28MP:5#
```

enable flood_fdb

Purpose	To enable the Switch's forwarding database on the Switch.
Syntax	**enable flood_fdb**
Description	The **enable flood_fdb** command enables dynamically learned entries from the Switch's forwarding database.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To enable FDB dynamic entries:

```
DGS-2000-28MP:5# enable flood_fdb
Command: enable flood_fdb


Success.
DGS-2000-28MP:5#
```

disable flood_fdb

Purpose	To disable the Switch's forwarding database on the Switch.

Syntax	**disable flood_fdb**
Description	The **disable flood_fdb** command disables dynamically learned entries from the Switch's forwarding database.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To disable FDB dynamic entries:

```
DGS-2000-28MP:5# disable flood_fdb
Command: disable flood_fdb


Success.
DGS-2000-28MP:5#
```

config flood_fdb

Purpose	To configure the Switch's forwarding database on the Switch.
Syntax	**config flood_fdb [log | trap] [enable | disable]**
Description	The **config flood_fdb** command configures dynamically learned entries from the Switch's forwarding database.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure FDB dynamic entries:

```
DGS-2000-28MP:5# config flood_fdb trap disable log enable
Command: config flood_fdb trap disable log enable


Success.
DGS-2000-28MP:5#
```

show flood_fdb

Purpose	To display the Switch's forwarding database on the Switch.
Syntax	**show flood_fdb**
Description	The **show flood_fdb** command displays dynamically learned entries from the Switch's forwarding database.
Parameters	None.
Restrictions	None.

Example usage:

To display FDB dynamic entries:

```
DGS-2000-28MP:5# show flood_fdb
Command: show flood_fdb

```

```
Flooding FDB State : Enabled
Log State          : Disabled
Trap State         : Disabled

Value  VLAN ID    MAC Address       Time stamp
-------- ------------  ------------------      ------------------
DGS-2000-28MP:5#
```

clear flood_fdb

Purpose	To clear the Switch's forwarding database of all dynamically learned MAC addresses.
Syntax	**clear flood_fdb**
Description	The **clear flood_fdb** command clears dynamically learned entries from the Switch's forwarding database.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To clear all FDB dynamic entries:

```
DGS-2000-28MP:5# clear flood_fdb
Command: clear flood_fdb

Success.
DGS-2000-28MP:5#
```

create auto_fdb

Purpose	To create a static entry in the auto forwarding table (database).
Syntax	**create auto_fdb <ipaddr>**
Description	The **create auto_fdb** command creates a static entry in MAC address forwarding table (database).
Parameters	*<ipaddr>* − The IP address to be deleted from the auto forwarding table.
Restrictions	None.

Example usage:

To create auto forwarding table:

```
DGS-2000-28MP:5# create auto_fdb 192.168.33.1
Command: create auto_fdb 192.168.33.1


Success.

DGS-2000-28MP:5#
```

delete auto_fdb	
Purpose	To delete a static entry in the auto forwarding table (database).
Syntax	**delete auto_fdb <ipaddr>**
Description	The **delete auto_fdb** command removes a static entry in the multicast MAC address forwarding table (database).
Parameters	<*ipaddr*> − The IP address to be deleted from the auto forwarding table.
Restrictions	None.

Example usage:

To delete auto forwarding table:

```
DGS-2000-28MP:5# delete auto_fdb 172.21.47.13
Command: delete auto_fdb 172.21.47.13

Success.
DGS-2000-28MP:5#
```

show auto_fdb	
Purpose	To display the auto forwarding table.
Syntax	**show auto_fdb <ipaddr>**
Description	The **show auto_fdb** command shows auto FDB table.
Parameters	<*ipaddr*> − The IP address to be deleted from the auto forwarding table.
Restrictions	None.

Example usage:

To delete auto forwarding table:

```
DGS-2000-28MP:5# show auto_fdb
Command: show auto_fdb

IP Address      VLAN ID    MAC Address         Port       Time Stamp
--------------- ---------- ------------------- ---------- ----------
10.90.90.222
192.168.33.1

DGS-2000-28MP:5#
```

16

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> | all] {broadcast [enable | disable] | multicast [enable | disable] | unicast [enable | disable] | action drop | threshold <value (64-N)> | time_interval <time_interval (5-30)> | countdown [0 | <minutes (5-30)>] }
config traffic control	[<portlist> | all] {broadcast [enable | disable] | multicast [enable | disable] | unicast [enable | disable] | action shutdown | threshold <value (0-255000)> | time_interval <time_interval (5-30)> | countdown [0 | <minutes (5-30)>] }
config traffic control auto_recover_time	[0 | <minutes (1-65535)>]
show traffic control	{<portlist >}

Each command is listed in detail, as follows:

config traffic control

Purpose	To configure broadcast / multicast / unknown unicast traffic control for “drop” action.
Syntax	**config traffic control [<portlist> | all] {broadcast [enable | disable] | multicast [enable | disable] | unicast [enable | disable] | action drop | threshold <value (64-N)> | time_interval <time_interval (5-30)> | countdown [0 | <minutes (5-30)>] }**
Description	The **config traffic control** command helps limit the traffic via variable reaction. The type of traffic can be specified via command: unicast, broadcast and multicast. Drop mode: When particular type traffic exceeds the threshold configured, the device starts to responding by dropping the packets (the parameter “countdown” does NOT apply in drop mode) Shutdown mode: When particular type traffic exceeds the threshold configured, the countdown timer starts to countdown then shutdown action would be executed.
Parameters	*<portlist >* - A port or range of ports to be configured. *all* − Specifies all ports on the Switch are to be configured. *broadcast [enable* | *disable]* – Control of broadcast traffic *multicast [enable* | *disable]* – Cotrol of multicast traffic *unicast [enable* | *disable]* – Control of unicast traffic *action drop* – The specific traffic flow that exceeds the threshold would be dropped.. *threshold <value 64-1024000>* − 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 *time_interval (5-30)* – Sampling time interval for particular type of traffic. Measure unit in seconds.
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-2000-28MP:5# config traffic control all broadcast enable multicast enable
unicast enable time_interval 5 action drop countdown 0 threshold 64000
Command: config traffic control all broadcast enable multicast enable unicast en
able time_interval 5 action drop countdown 0 threshold 64000


Success.

DGS-2000-28MP:5#
```

config traffic control

Purpose	To configure broadcast / multicast / unknown unicast traffic control for “drop” action.
Syntax	**config traffic control [<portlist> | all] {broadcast [enable | disable] | multicast [enable | disable] | unicast [enable | disable] | action shutdown | threshold <value (0-255000)> | time_interval <time_interval (5-30)> | countdown [0 | <minutes (5-30)>] }**
Description	The **config traffic control** command helps limit the traffic via variable reaction. The type of traffic can be specified via command: unicast, broadcast and multicast. Drop mode: When particular type traffic exceeds the threshold configured, the device starts to responding by dropping the packets (the parameter “countdown” does NOT apply in drop mode) Shutdown mode: When particular type traffic exceeds the threshold configured, the countdown timer starts to countdown then shutdown action would be executed.
Parameters	*<portlist >* - A port or range of ports to be configured. *all* − Specifies all ports on the Switch are to be configured. *broadcast [enable* | *disable]* – Control of broadcast traffic *multicast [enable* | *disable]* – Cotrol of multicast traffic *unicast [enable* | *disable]* – Control of unicast traffic *action drop* – The specific traffic flow that exceeds the threshold would be dropped.. *threshold <value 0-255000>* − 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 *time_interval (5-30)* – Sampling time interval for particular type of traffic. Measure unit in seconds. *countdown [0 | <minutes (5-30)>]* - The timer starts when traffic exceeds the threshold. Value “0” represents immediate responds.
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-2000-28MP:5# config traffic control 4-5 broadcast enable unicast disable threshold 4000 action shutdown
Command: config traffic control 4-5 broadcast enable unicast disable threshold 4
000 action shutdown



Success.

DGS-2000-28MP:5#
```

config traffic control auto_recover_time

Purpose	To identify the time to recovery from shutdown mode.
Syntax	**config traffic control auto_recover_time [0 | <minutes (1-65535)>]**
Description	The **config traffic control auto_recover_time** command is used to specify the recover time when storm occurred. This time applies to "shutdown" mode only..
Parameters	*[0 | <minutes (1-65535)>]* – Measurment unit in minute. Value "0" represents auto recoevery mechanism DISABLED.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To display traffic control setting:

```
DGS-2000-28MP:5# config traffic control auto_recover_time 3
Command: config traffic control auto_recover_time 3



Success.

DGS-2000-28MP:5#
```

show traffic control

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

Example usage:

To display traffic control setting:

```
DGS-2000-28MP: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-2000-28MP:5#
```

17

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 > | all] {rx_rate [no_limit | <value 16-1000000>] | tx_rate [no_limit | <value 16-1000000>]}
show bandwidth_control	{[<portlist > | all]}
config qos mode	[802.1p | dscp | portbased]
show qos mode	
config scheduling_mechanism	[strict | wrr]
show scheduling_mechanism	
config 802.1p default_priority	[<portlist> | all] priority <value 0-7>
show 802.1p default_priority	{[<portlist> | all]}
show 802.1p user_priority	
show scheduling_mechanism	
show scheduling	
config dscp_mapping	dscp_value <value_list 0-63> class <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 > | 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	*<portlist* > - A port or range of ports to be configured. *all* - Specifies that the **config bandwidth_control** command applies to all ports on the Switch. *rx_rate* - Enables ingress rate limiting

	• *no_limit* – Indicates no limit is defined. • <*value 16–1000000*>] – Indicates a range between 16-1000000 kbps. *tx_rate* – Enables egress rate limiting. • *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-2000-28MP: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-2000-28MP:5#
```

show bandwidth_control

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

Example usage:

T o display the bandwidth control configuration:

```
DGS-2000-28MP: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-2000-28MP: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	*[802.1p* | *dscp* | *portbased]* – 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-2000-28MP:5#  config qos mode portbased
Command: config qos mode portbased

Success.
DGS-2000-28MP: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-2000-28MP:5#  show qos mode
Command: show qos mode

Qos mode  :  portbased
DGS-2000-28MP:5#
```

config scheduling_mechanism

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

	order − from the highest priority hardware queue (class 3) to the lowest priority hardware queue (class 0). Each queue will transmit all of the packets in its buffer before allowing the next lower priority queue to transmit its packets. A lower priority hardware queue will be pre-empted from emptying its queue if a packet is received on a higher priority hardware queue. The packet received on the higher priority hardware queue transmits its packet before allowing the lower priority hardware queue to resume clearing its queue.
Parameters	*strict* – Specifies that the highest class of service is the first to be processed. That is, the highest class of service should finish emptying before the others begin. *wrr* – Specifies that the priority classes of service are to empty packets in a weighted roundrobin (WRR) order.
Restrictions	Only administrator or operator level users can issue this command.

Example usage:

To configure the traffic scheduling mechanism for each COS queue:

```
DGS-2000-28MP:5# config scheduling_mechanism strict
Command: config scheduling_mechanism strict

Success.
DGS-2000-28MP: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-2000-28MP:5#  show scheduling_mechanism
Command: show scheduling_mechanism

Queue Mechanism       : strict
DGS-2000-28MP:5#
```

config 802.1p default_priority

Purpose	To assign an 802.1p priority tag to an incoming untagged packet that has no 802.1p priority tag.
Syntax	**config 802.1p default_priority [<portlist> | all] <priority 0-7>**
Description	The **config 802.1p default_priority** command specifies the 802.1p priority value an untagged, incoming packet is assigned before being forwarded to its destination.

Parameters	<*portlist*> − A port or range of ports to be configured. *all* − Specifies that the config 802.1p default_priority command applies to all ports on the Switch. <*priority 0-7*> − The 802.1p priority value that an untagged, incoming packet is granted before being forwarded to its destination.
Restrictions	Only administrator or operator level users can issue this command.

Example usage:

To configure 802.1p default priority on the Switch:

```
DGS-2000-28MP:5# config 802.1p default_priority all 4
Command: config 802.1p default_priority all 4

Success.
DGS-2000-28MP:5#
```

show 802.1p default_priority

Purpose	To display the currently configured 802.1p priority value that is assigned to an incoming, untagged packet before being forwarded to its destination.
Syntax	**show 802.1p default_priority {<portlist>}**
Description	The **show 802.1p default_priority** command displays the currently configured 802.1p priority value that is assigned to an incoming, untagged packet before being forwarded to its destination.
Parameters	<*portlist*> − A port or range of ports to be displayed.
Restrictions	None.

Example usage:

To display the current port 1-5 802.1p default priority configuration on the Switch:

```
DGS-2000-28MP:5# show 802.1p default_priority 1-5
Command: show 802.1p default_priority 1-5

Port  Default Priority  Effective Priority
----- ----------------- -------------------
1     0                 4
2     0                 4
3     0                 4
4     0                 4
5     0                 4

DGS-2000-28MP:5#
```

show 802.1p user_priority

Purpose	To display the current mapping between an incoming packet's 802.1p priority value and one of the Switch's eight hardware priority classes of service.
Syntax	**show 802.1p user_priority**

Description	The **show 802.1p user_priority** command displays the current mapping of an incoming packet's 802.1p priority value to one of the Switch's four hardware priority queues.
Parameters	None.
Restrictions	None.

Example usage:

To show 802.1p user priority:

```
DGS-2000-28MP:5# show 802.1p user_priority
Command: show 802.1p user_priority


802.1p Priority   Queue
---------------   ------
0                 2
1                 0
2                 1
3                 3
4                 4
5                 5
6                 6
7                 7

DGS-2000-28MP:5#
```

show scheduling

Purpose	To display the currently configured traffic scheduling on the Switch.
Syntax	**show scheduling**
Description	The **show scheduling** command displays the current configuration for the maximum number of packets (*max_packet*) value assigned to the four priority classes of service on the Switch. The Switch empties the four hardware queues in order, from the highest priority (class 3) to the lowest priority (class 0).
Parameters	None.
Restrictions	None.

Example usage:

To display the current scheduling configuration:

```
DGS-2000-28MP:5# show scheduling
Command: show scheduling


Queue  Weight
-----  ------
0      1
1      2
2      3
```

```
3    4
4    5
5    6
6    7
7    8

DGS-2000-28MP:5#
```

config dscp_mapping

Purpose	To enable setting the DSCP User Priority
Syntax	**config dscp_mapping dscp_value <value_list 0-63> class <value 0-7>**
Description	The **config dscp_mapping** command enables mapping the DSCP value (the priority) to a specific queue (the class_id).
Parameters	*<value_list 0-63>* –The selected value of priority. The value may be between 0 and 63. *queue <value 0-7>* – 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-2000-28MP:5#  config dscp_mapping dscp_value 10 class 0
Command: config dscp_mapping dscp_value 10 class 0

Success.
DGS-2000-28MP: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	*dscp_value <value_list 0-63>* - The selected value of priority will be dispalyed. The value may be between 0 and 63.
Restrictions	None.

Example usage:

To display the DSCP mapping with value 10:

```
DGS-2000-28MP:5#  show dscp_mapping dscp_value 10
Command: show dscp_mapping dscp_value 10

DSCP  Priority
-------  ------------
10       0
DGS-2000-28MP:5#
```

18

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-2000-28MP:5# enable rmon
Command: enable rmon
```

```
Success.
DGS-2000-28MP: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-2000-28MP:5# disable rmon
Command: disable rmon

Success.
DGS-2000-28MP: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	*<alarm_index>* − Specifies the alarm number. *<OID_variable 255>* − Specifies the MIB variable value. *<interval 1-2147482647>* − Specifies the alarm interval time in seconds. *[absolute | delta]* − Specifies the sampling method for the selected variable and comparing the value against the thresholds. The possible values are absolute and delta: • *absolute* –Compares the values directly with the thresholds at the end of the sampling interval. • *delta* –Subtracts the last sampled value from the current value. The difference in the values is compared to the threshold. *rising-threshold <value 0-2147483647>* − Specifies the rising counter value that triggers the rising threshold alarm. *<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-2000-28MP: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-2000-28MP: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	*<alarm_index 1-65535>* − 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-2000-28MP:5# delete rmon alarm 100
Command: delete rmon alarm 100

Success.
DGS-2000-28MP:5#
```

create rmon collection stats

Purpose	To allow user 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 user to configure the rmon stats settings on the Switch.
Parameters	*<stats_index 1-65535>* − Specifies the stats number. *port <ifindex>* − Specifies the port from which the RMON information was taken. *owner <owner_string 32>* − Specifies the device or user that defined

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

Example usage:

To create a RMON collection stats on the Switch:

```
DGS-2000-28MP:5#  create rmon collection stats 100 port 1 owner dlink
Command: create rmon collection stats 100 port 1 owner dlink

Success.
DGS-2000-28MP: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	*<stats_index 1-65535>* − 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-2000-28MP:5# delete rmon collection stats 2
Command: delete rmon collection stats 2

Success.
DGS-2000-28MP:5#
```

create rmon collection history

Purpose	To allow 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	*<hist_index 1-65535>* − Indicates the history control entry number. *port <ifindex>* − Specifies the port from which the RMON information was taken. *buckets <buckets_req 1-50>* − Specifies the number of buckets that the device saves. *interval <interval 1-3600>* − Specifies in seconds the time period that samplings are taken from the ports. The field range is *1-3600*. The default is *1800* seconds (equal to 30 minutes). *owner <owner_string 127>* − 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-2000-28MP:5# create rmon collection history 120 port 1 buckets 10
Command: create rmon collection history 120 port 1 buckets 10

Success.
DGS-2000-28MP: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	*<hist_index 1-65535>* − 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-2000-28MP:5# delete rmon collection history 2
Command: delete rmon collection history 2

Success.
DGS-2000-28MP:5#
```

create rmon event

Purpose	To provide user to configure the settings of 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 allows user to provides user to configure the settings of rmon event on the Switch.
Parameters	*<event_index 1-65535>* − Specifies the event number. *description <desc_string 128>* − Specifies the user-defined event description. *log* − Indicates that the event is a log entry. *owner <owner_string 32>* − Specifies the time that the event occurred. *trap <community_string 32>* − Specifies the community to which the event belongs.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To create a RMON collection history on the Switch:

```
DGS-2000-28MP:5# create rmon event 125 description linkrmon owner dlink
Command: create rmon event 125 description linkrmon owner dlink

Success.
DGS-2000-28MP: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	*<event_index 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-2000-28MP:5# delete rmon event 2
Command: delete rmon event 2

Success.
DGS-2000-28MP: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	*statistics <stats_index 1-65535>* − Specify the index of RMON statistics to be displayed. *alarms* – Specify the RMON alarm to be displayed. *events* − Specify the RMON events to be displayed. *history <hist_index 1-65535>* − Specify the RMON history to be displayed. *overview* – Display the RMON overview.
Restrictions	None.

Example usage:

To display the RMON feature on the Switch:

```
DGS-2000-28MP: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-2000-28MP:5#
```

19

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	group_id <value 1-4>
config mirror	group_id <value 1-4> [target_port <port> | [add | delete] source ports <portlist> [rx |x | both] | state [enable | disable]]
delete mirror	group_id <value 1-4>
show mirror	{group_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, 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 enable the mirroring feature:

```
DGS-2000-28MP:5# enable mirror
Command: enable mirror

Success.
DGS-2000-28MP: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-2000-28MP:5# disable mirror
Command: disable mirror

Success.
DGS-2000-28MP:5#
```

create mirror id

Purpose	Used to create a port mirroring ID.
Syntax	**create mirror group_id <value 1-4>**
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	*group_id <value 1-4>* − Specifies the mirror ID to be created.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To create the mirroring ID:

```
DGS-2000-28MP:5#  create mirror id 1
Command: create mirror id 1

Success.
DGS-2000-28MP:5#
```

config mirror

Purpose	To configure a mirror port − source port pair on the Switch.
Syntax	**config mirror group_id <value 1-4> [target_port <port> | [add | delete] source ports <portlist> [rx |x | both] | state [enable | disable]]**
Description	The **config mirror target** 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	*group_id <value 1-4>* − Specifies the mirror ID. *target <short >* − Specifies the port that mirrors traffic forwarding. *[add | delete]* − Specifies to add or delete the target port. *source ports <portlist >* – Specifies the port or ports being mirrored.

	This cannot include the target port. *rx* – Allows mirroring of packets received by (flowing into) the source port. *tx* – Allows mirroring of packets sent to (flowing out of) the source port. *both* – Allows mirroring of all the packets received or sent by the source port. *state [enable* | *disable]* – Allows to control the state for each mirror group.
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-2000-28MP:5# config mirror group_id 1 target_port 2
Command: config mirror group_id 1 target_port 2


Success.
DGS-2000-28MP:5# config mirror group_id 1 add source ports 3 both
Command: config mirror group_id 1 add source ports 3 both


Success.

DGS-2000-28MP:5#
```

show mirror

Purpose	To show the current port mirroring configuration on the Switch.
Syntax	**show mirror {group_id <value 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:

```
Command: show mirror group_id 1

Port Mirror is Enabled

ID   Target Port  Ingress port   Egress port    Both         State
---  -----------  ------------   ------------   ------------ --------
1    2            3-24           3-24           3-24         Disabled
DGS-2000-28MP:5#
```

20

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> | vlanid <vidlist 2-4094>]
delete vlan	[<vlan_name 20> | vlanid <vidlist 2-4094>]
config vlan vlanid	<vlanid 1-4094> [[add [tagged | untagged] | delete] <portlist> | name <vlan_name 20>]
config vlan	<vlan_name (20)> {add {tagged | untagged } | delete} <portlist>
show vlan	{<vlan_name 20> | vlanid <vidlist 1-4094> | ports <portlist >}
enable asymmetric_vlan	
disable asymmetric_vlan	
show asymmetric_vlan	
config port_vlan	[<portlist> | all] pvid <vlanid 1-4094>
show port_vlan pvid	
enable pvid auto_assign	
disable pvid auto_assign	
show pvid auto_assign	

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> | vlanid <vidlist 2-4094>]**
Description	The **create vlan** command creates a VLAN on the Switch.
Parameters	*<vlan_name 20>* − The name of the VLAN to be created. *tag <vlanid 2-4094>* − The VLAN ID of the VLAN to be created. The allowed values range from 2 to 4094. *vlanid <vidlist 2-4094>* - A VID or range of VIDs can be created.
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. DGS-2000 series supports up to 256 VLAN groups. Only administrator or operator-level users can issue this command.

Example usage:

To create a VLAN v1, tag 3:

```
DGS-2000-28MP:5# create vlan v1 tag 3
Command: create vlan v1 tag 3

Success.
DGS-2000-28MP: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	*<vlan_name 20>* − The name of the VLAN to be deleted. *vlanid <vidlist 2-4092>* − 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 which VLAN ID is 2:

```
DGS-2000-28MP:5# delete vlan vlanid 2
Command: delete vlan vlanid 2

Success.
DGS-2000-28MP:5#
```

config vlan

Purpose	To add additional ports to a previously configured VLAN and to modify a VLAN name.
Syntax	**config vlan <vlanid 1-4094> [[add [tagged | untagged] | delete] <portlist> | name <vlan_name 20>]**
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	*<vlan_name 20>* − The name of the VLAN to be configure. *vlanid <int 1-4094 >* − The ID of the VLAN to which to add ports. *add* − Specifies that ports are to be added to a previously created vlan. *delete* - Specifies that ports are to be deleted from a previously created vlan. *tagged* − Specifies the additional ports as tagged. *untagged* − Specifies the additional ports as untagged. *<portlist >* − A port or range of ports to be added to or deleted from the VLAN. *name <vlan_name 20>* - Configure the name string of particular VLAN group.

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-2000-28MP:5#  config vlan vlanid 1 add tagged 1-3
Command: config vlan vlanid 1 add tagged 1-3


Success.
DGS-2000-28MP: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 >}**
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	*<vlan_name 20>* − Specify the VLAN id to be displayed. *vlanid <vidlist 1-4094>* − Specify the VLAN id to be displayed. *ports <portlist >* − Specify the ports to be displayed.
Restrictions	None.

Example usage:

To display the Switch's current VLAN settings:

```
DGS-2000-28MP:5#  show vlan
Command: show vlan

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

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

DGS-2000-28MP: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 enable 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 Asymettric VLAN on the switch:

```
DGS-2000-28MP:5# enable asymmetric_vlan
Command: enable asymmetric_vlan

Success.
DGS-2000-28MP: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-2000-28MP:5# disable asymmetric_vlan
Command: disable asymmetric_vlan

Success.
DGS-2000-28MP: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-2000-28MP:5# show asymmetric_vlan
Command: show asymmetric_vlan

Asymmetric VLAN : Enable
DGS-2000-28MP:5#
```

config port_vlan

Purpose	To assign the port VID for specific port(s).
Syntax	**config port_vlan [<portlist> | all] pvid <vlanid 1-4094>**
Description	The **config port_vlan** command configures port VID for specific port(s).
Parameters	*[<portlist > | al]l* − Specify a port, a range of ports or all ports. *pvid <vlanid 1-4094>* − Specify the VID to assign
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure the port VID for port 3:

```
DGS-2000-28MP:5# config port_vlan 3 pvid 2
Command: config port_vlan 3 pvid 2


Success.

DGS-2000-28MP: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-2000-28MP:5#  show port_vlan pvid
Command: show port_vlan pvid

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

```
11          1
12          1
13          1
14          1
DGS-2000-28MP:5#
```

enable pvid auto_assign

Purpose	To turn on PVID auto assign mechanism.
Syntax	**enable pvid auto_assign**
Description	The **pvid auto_assign** feature automatically assigns the PVID when the port(s) is assigned to VLAN group with untagged role.
Parameters	None.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To turn on PVID auto assign feature:

```
DGS-2000-28MP:5# enable pvid auto_assign
Command: enable pvid auto_assign


Success.

DGS-2000-28MP:5#
```

disable pvid auto_assign

Purpose	To turn off PVID auto assign mechanism.
Syntax	**disable pvid auto_assign**
Description	The **pvid auto_assign** feature automatically assigns the PVID when the port(s) is assigned to VLAN group with untagged role.
Parameters	None.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To turn off PVID auto assign feature:

```
DGS-2000-28MP:5# disable pvid auto_assign
Command: disable pvid auto_assign


Success.

DGS-2000-28MP:5#
```

show pvid auto_assign

Purpose	To display the current status PVID auto assign mechanism.

Syntax	**show pvid auto_assign**
Description	The **pvid auto_assign** feature automatically assigns the PVID when the port(s) is assigned to VLAN group with untagged role.
Parameters	None.
Restrictions	None.

Example usage:

To show PVID auto assign feature:

```
DGS-2000-28MP:5# show pvid auto_assign
Command: show pvid auto_assign

PVID Auto-assignment : Enabled
DGS-2000-28MP:5#
```

21

Q-IN-Q COMMANDS

The QinQ 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> | inner_tpid]}
config qinq ports	[<portlist> | all] [role [nni | uni] | outer_tpid <hex 0x1 - 0xffff> | missdrop [enable | disable]]
config qinq inner_tpid	<hex 0x1-0xffff>
show qinq inner_tpid	
create vlan_translation	ports <portlist> [add | replace] cvid <vidlist> svid <vlanid 1-4094> {priority <priority 0-7>}
show vlan_translation	{cvid <vidlist>}
delete vlan_translation	ports [<portlist> | all] {cvid [<vidlist> | all]}

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 creates a 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. GVRP and STP need to be disabled manually. If you need to run GVRP on the Switch, firstly enable GVRP manually. The default setting of Q-in-Q is disabled.
Parameters	None.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To enable Q-in-Q:

```
DGS-2000-28MP:5# enable qinq
Command: enable qinq


Success.
```

```
DGS-2000-28MP:5#
```

disable qinq

Purpose	To disable the Q-in-Q mode.
Syntax	**disable qinq**
Description	The **disable qinq** command creates a used to disable the Q-in-Q mode. All dynamically learned L2 address will be cleared. All dynamically registered VLAN entries will be cleared, GVRP will be disabled. If you need to run GVRP on the Switch, firstly enable GVRP manually. All existing SP-VLANs will run as static 1Q VLANs. The default setting of Q-in-Q is disabled.
Parameters	None.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To disable Q-in-Q:

```
DGS-2000-28MP:5# disable qinq
Command: disable qinq


Success.
DGS-2000-28MP:5#
```

show qinq

Purpose	To show global Q-in-Q and port Q-in-Q mode status.
Syntax	**show qinq {ports [<portlist> | inner_tpid]}**
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. *Inner_tpid* – Specifies the inner tpid to be showed.
Restrictions	None.

Example usage:

To show the Q-in-Q status for ports 1 to 3:

```
DGS-2000-28MP:5# show qinq ports 1-3
Command: show qinq ports 1-3

Port Role Missdrop  Outer TPID
---- ---- --------- ----------
1    NNI  Disabled  0x88A8
2    NNI  Disabled  0x88A8
3    NNI  Disabled  0x88A8
```

```
Total Entries      : 3

DGS-2000-28MP:5#
```

config qinq ports

Purpose	Used to configure Q-in-Q ports.
Syntax	**config qinq ports [<portlist> | all] [role [nni | uni] | outer_tpid <hex 0x1 - 0xffff> | missdrop [enable | disable]]**
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	*<portlist>* - A range of ports to configure. *all* – Specifies all ports to be configure. *role* - Port role in Q-in-Q mode, it can be UNI port or NNI port. *outer_tpid* - TPID in the SP-VLAN tag. *missdrop* - If specified as enabled, the VLAN translation will be performed on the port. The setting is disabled by default.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure port list 1 to 4 as NNI port, set outer TPID to 0x88a8:

```
DGS-2000-28MP:5# config qinq ports 1-3 role nni outer_tpid 0x88a8
Command: config qinq ports 1-3 role nni outer_tpid 0x88a8

Success.

DGS-2000-28MP:5#
```

config qinq inner_tpid

Purpose	Used to configure Q-in-Q inner TPID of the Switch.
Syntax	**config qinq inner_tpid <hex 0x1-0xffff>**
Description	The **config qinq inner_tpid** command is used to configure the inner TPID for port.
Parameters	<hex 0x1-0xffff> - Specifies the inner-TPID of a port.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure the inner TPID to 0x88a8:

```
DGS-2000-28MP:5# config qinq inner_tpid 0x88a8
Command: config qinq inner_tpid 0x88a8

Success.

DGS-2000-28MP:5#
```

show qinq inner_tpid

Purpose	Used to display Q-in-Q inner TPID of the Switch.
Syntax	**show qinq inner_tpid**
Description	The **show qinq inner_tpid** command is used to show the inner TPID value.
Parameters	None.
Restrictions	None.

Example usage:

To display the inner TPID:

```
DGS-2000-28MP:5# show qinq inner_tpid
Command: show qinq inner_tpid

Inner TPID: 0x88a8
DGS-2000-28MP:5#
```

create vlan_translation

Purpose	To create a VLAN translation rule that will be added as a new rule or replace a current rule.
Syntax	**create vlan_translation ports <portlist> [add | replace] cvid <vidlist> svid <vlanid 1-4094> {priority <priority 0-7>}**
Description	The **create vlan_translation cvid** command is used to create a VLAN translation rule to add to or replace the outgoing packet which is single S-tagged (the C-VID changes to S-VID and the packet's TPID changes to an outer TPID).
Parameters	*ports <portlist>* - A range of ports to be configure. *cvid* – C-VLAN ID of packets that ingress from a UNI port. *svid* – The S-VLAN ID that replaces the C-VLAN ID or is inserted in the packet. <*vlanid 1-4094*> – A VLAN ID between 1 and 4094. *priority <priority 0-7>* - Configure the priority of specified ports.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To create a VLAN translation on the Switch:

```
DGS-2000-28MP:5# create vlan_translation add cvid 2 svid 2
Command: create vlan_translation add cvid 2 svid 2



Success.
DGS-2000-28MP:5#
```

show vlan_translation

Purpose	To display the current VLAN translation rules on the Switch.
Syntax	**show vlan_translation {cvid <vidlist>}**

Description	The **show vlan_translation cvid** command display the current VLAN translation cvid on the Switch.
Parameters	<*vidlist*> − The Q-in-Q translation rules for the specified C-VID list.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To display the VLAN translation cvid on the Switch:

```
DGS-2000-28MP:5# show vlan_translation cvid 1
Command: show vlan_translation cvid 1

Port    CVID      SPVID      Action     Priority
------- --------  ----------  ----------  -------------

 Total Entries: 0

DGS-2000-28MP:5#
```

delete vlan_translation ports

Purpose	To delete VLAN translation rules.
Syntax	**delete vlan_translation ports [<portlist> | all] {cvid [<vidlist> | all]}**
Description	The **delete vlan_translation cvid** command is used to delete VLAN translation rules.
Parameters	*ports* <*portlist*> - A range of ports to be deleted. <*vidlist*> - Specifies C-VID rules in VLAN translation. *all* – Specifies all C-VID rules to be deleted.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To delete all C-VID VLAN translation rules:

```
DGS-2000-28MP:5# delete vlan_translation cvid all
Command: delete vlan_translation cvid all



Success.
DGS-2000-28MP:5#
```

22

INTERFACE AND 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
create ipif	<ipif_name (12)> <network_address> <vlan_name (20)> state {enable | disable}
config ipif system	<ipif_name (12)> {([ipaddress <network_address>] [vlan <vlan_name (20)>] [state {enable | disable}]) | dhcp | ipv6 {ipv6address <ipv6networkaddr> | state {enable | disable}} | ipv4 state {enable | disable} | dhcp_option12 { hostname <hostname (63)> | clear_hostname | state {enable | disable} } | dhcpv6_client {enable | disable}}
show ipif	[<ipif_name (12)>]
enable ipif	{<ipif_name (12)> | all}
disable ipif	{<ipif_name (12)> | all}
delete ipif	{<ipif_name (12)> | all}
create iproute default	[<network_address> | default] {metric <int 1-65535>} {primary | backup}
delete iproute	[<network_address> | default] {metric <int 1-65535>} {primary | backup}
show iproute	{[<ipaddr>|static]}
create ipv6route	[<ipv6networkaddr> | default] <ipv6addr> [metric <int 1-65535>] {primary | backup}
delete ipv6route	{<ipv6networkaddr> | default}
show ipv6route	{[< ipv6networkaddr > | static]}

Each command is listed in detail, as follows:

create ipif	
Purpose	To create an IP interface on the switch.
Syntax	**create ipif <ipif_name 12> <network_address> <vlan_name 20> state [enable | disable]**
Description	The **create ipif** command will create an IP interface.
Parameters	<*ipif_name 12*> - Specifies the IP interface name to be created. <*network_address*> - IP address and netmask of the IP interface to be created. <*vlan_name 20*> - The name of the VLAN that will be associated with the above IP interfact. *state [enable | disable]* – Specifies to enable or disable the IP interface.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To create an IP interface:

```
DGS-2000-28MP:5# create ipif ip2 10.1.2.3/255.0.0.0 default state enable
Command: create ipif ip2 10.1.2.3/255.0.0.0 default state enable

Success.
DGS-2000-28MP:5#
```

config ipif

Purpose	To configure the DHCPv6 client state for the interface.
Syntax	**config ipif <ipif_name 12> ([ipaddress <network_address>] [vlan <vlan_name 20>] [state [enable | disable]] | dhcp | ipv6 {ipv6address <ipv6networkaddr> | state {enable | disable}} | ipv4 state [enable | disable] | dhcp_option12 { hostname <hostname 63> | clear_hostname | state [enable | disable] } | dhcpv6_client [enable | disable] }**
Description	The **config ipif system** command is used to configure the DHCPv6 client state for one interface.
Parameters	*<ipif_name 12>* − 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. *dhcp* − Specifies the DHCP protocol for the assignment of an IP address to the Switch to use for the DHCP Protocol. *hostname <hostname 63>* – Specifies the host name of DHCP. *ipaddress <network_address>* − IP address and netmask of the IP interface to be created. The address and mask information may be specified by using the traditional format (for example, 10.1.2.3/255.0.0.0 or in CIDR format, 10.1.2.3/16). *gateway <ipaddr>* − IP address of gateway to be created. *state [enable | disable]* − Enables or disables the IP interface. ipv6 ipv6address <ipv6networkaddr> − 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. *dhcpv6_client [enable | disable]* − Enable or disable the DHCPv6 client state of the interface.
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-2000-28MP:5# config ipif System dhcpv6_client enable
Command: config ipif System dhcpv6_client enable

Success.

DGS-2000-28MP: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-2000-28MP:5#  show ipif
Command: show ipif

 IP Setting Mode              : Static
 Interface Name               : System
 Interface VLAN Name          : default
 IP Address                   : 10.90.90.90
 Subnet Mask                  : 255.0.0.0
 Default Gateway              : 0.0.0.0
 Interface Admin State        : Enabled
 IPv4 State                   : Enabled
 IPv6 State                   : Enabled

DGS-2000-28MP:5#
```

enable ipif

Purpose	To enable an IP interface on the switch.
Syntax	**enable ipif [<ipif_name 12> | all]**
Description	The **enable ipif** command will create an IP interface.
Parameters	*[<ipif_name 12> | all]* - Specifies the IP interface name or all IP interface to be enabled.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To enable all IP interface:

```
DGS-2000-28MP:5# enable ipif all
Command: enable ipif all

Success.
DGS-2000-28MP:5#
```

disable ipif

Purpose	To disable an IP interface on the switch.
Syntax	**disable ipif [<ipif_name 12> | all]**

Description	The **disable ipif** command will create an IP interface.
Parameters	*[<ipif_name 12> | all]* - Specifies the IP interface name or all IP interface to be disabled.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To disable all IP interface:

```
DGS-2000-28MP:5# disable ipif all
Command: disable ipif all

Success.
DGS-2000-28MP:5#
```

delete ipif

Purpose	To delete an IP interface on the switch.
Syntax	**delete ipif [<ipif_name 12> | all]**
Description	The **delete ipif** command will delete an IP interface.
Parameters	*[<ipif_name 12> | all]* - Specifies the IP interface name or all IP interface to be deleted. Noted: The default interface cannot be deleted when issue delete ipif all. This mechanism helps to prevent user error configuration.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To delete an IP interface:

```
DGS-2000-28MP:5# delete ipif all
Command: delete ipif all

Success.
DGS-2000-28MP:5#
```

create iproute

Purpose	To create an IP route entry on the Switch.
Syntax	**create iproute [<network_address> | default] {metric <int 1-65535>} {primary | backup}**
Description	The **create iproute** command is used to create an IP route entry on the Switch. “Primary” and “backup” are mutually exclusive. Users can select only one when creating one new route. If a user sets neither of these, the system will try to set the new route first by primary and second by backup.
Parameters	<*network_address*> - The IP address and netmask of the IP interface that is the destination of the route. Specify the address and mask information using the traditional format (for example, 10.90.90.3/255.0.0.0 or in CIDR format, 10.90.90.3/8). *default* – To create a default IPv4 route entry. <*ipaddr*> – To specify the IPv4 address for the next hop route. · *metric <int 1-65535>* – To specify the hop cost, and the default

	is 1. The value ranges between 1 and 65535. · *primary* – To specify the route as the primary route to the destination. · *backup* – To specify the route as the backup route to the destination. If the route is not specified as the primary route or the backup route, then it will be auto-assigned by the system. The first created is the primary, the second created is the backup.
Restrictions	Only administrator, operator or power user-level users can issue this command.

Example usage:

To add a default route with a nexthop of 10.90.58.33 as primary route:

```
DGS-2000-28MP:5# create iproute default 10.90.58.33 primary
Command: create iproute default 10.90.58.33 primary

Success.
DGS-2000-28MP:5#
```

delete iproute

Purpose	Used to delete an IP route entry from the Switch's IP routing table.
Syntax	**delete iproute** [<network_address> | default] <ipaddr>
Description	The **delete iproute** command will delete an existing IP route entry from the Switch's IP routing table.
Parameters	<network_address> - The IP address and netmask of the IP interface that is the destination of the route. Specify the address and mask information using the traditional format (for example, 10.90.90.3/255.0.0.0 or in CIDR format, 10.90.90.3/8). default – Specifies to delete a default IP route entry. <ipaddr> – To specify the IPv4 address for the next hop router to be configured.
Restrictions	Only Administrator, operator and power user-level users can issue this command.

Example usage:

To delete the default route from the routing table:

```
DGS-2000-28MP:5# delete iproute 10.90.58.33
Command: delete iproute 10.90.58.33


Success.
DGS-2000-28MP:5#
```

show iproute

Purpose	Used to display the Switch's current IP routing table.
Syntax	**show iproute {static}**
Description	The **show iproute** command will display the Switch's current IP

	routing table.
Parameters	{static} – Specifies to display all the static route entries.
Restrictions	None.

Example usage:

To display the contents of the IP routing table:

```
DGS-2000-28MP:5# show iproute
Command: show iproute

Routing Table

IP Address/Netmask   Gateway        Interface   Cost      Protocol
------------------   ---------------- ------------ ---------- ----------
10.0.0.0/8           10.90.58.33    System      1         local


Total Entries      : 1

DGS-2000-28MP:5#
```

create ipv6route

Purpose	Used to create an IPv6 static route in the Switch's IP routing table.
Syntax	**create ipv6route [<ipv6networkaddr> | default] <ipv6addr> [metric <int 1-65535>] {primary | backup}**
Description	This **create ipv6route** command is used to create a primary and backup IP route entry to the Switch's IP routing table.
Parameters	*<ipv6networkaddr>* - Specifies the destination network for the route. *default* – To create a default IPv6 route entry. *<ipaddr>* – To specify the IPv6 address for the next hop route. · *metric <int 1-65535>* – To specify the hop cost, and the default is 1. The value ranges between 1 and 65535. · *primary* – To specify the route as the primary route to the destination. · *backup* – To specify the route as the backup route to the destination. If the route is not specified as the primary route or the backup route, then it will be auto-assigned by the system. The first created is the primary, the second created is the backup.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To add a single static IPv6 entry in IPv6 format:

```
DGS-2000-28MP:5# create ipv6route default FEC0::5
Command: create ipv6route default FEC0::5


Success.
DGS-2000-28MP:5#
```

delete ipv6route	
Purpose	Used to delete a static IPv6 route entry from the Switch's IP routing table.
Syntax	**delete ipv6route [<ipv6networkaddr> | default] <ipv6addr>**
Description	This **delete ipv6route** command will delete an existing static IPv6 entry from the Switch's IP routing table.
Parameters	*<ipv6networkaddr>* – To specify the IPv6 address that is the destination of the route to be deleted. *default* – Specifies to delete a default IP route entry. *<ipaddr>* – To specify the IPv6 address for the next hop router to be configured.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To delete a static IPv6 entry from the routing table:

```
DGS-2000-28MP:5# delete ipv6route default FEC0::5
Command: delete ipv6route default default FEC0::5


Success.
DGS-2000-28MP:5#
```

show ipv6route	
Purpose	Used to display a static IPv6 route entry from the Switch's IP routing table.
Syntax	**show ipv6route {static}**
Description	This **show ipv6route** command will display an existing static IPv6 entry from the Switch's IP routing table.
Parameters	*{static}* – Specifies to display all the IPv6 static route entries.
Restrictions	None.

Example usage:

To show a static IPv6 entry from the routing table:

```
DGS-2000-28MP:5# show ipv6route
Command: show ipv6route

IPv6 Prefix: ::/0                       Protocol: Static Metric: 1
Next Hop   : FEC0::5                    IPIF    : System

Total Entries: 1
DGS-2000-28MP:5#
```

23

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	<ipif_name 12> <ipv6_addr> <mac_addr>
delete ipv6 neighbor_cache	<ipif_name 12> [<ipv6_addr> | static | dynamic | all]
show ipv6 neighbor_cache	[ipv6address <ipv6_addr> | static | dynamic | all]
config ipv6 nd ns ipif	<ipif_name (12)> retrans_time {<int (1-3600)> | default}
show ipv6 nd ipif	<ipif_name (12)>
enable ipv6 nd flooding	
disable ipv6 nd flooding	
enable ipif_ipv6_link_local_auto	<ipif_name (12)>
disable ipif_ipv6_link_local_auto	<ipif_name (12)>

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-2000-28MP: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-2000-28MP: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	*<ivp6_addr>* –The IPv6 address of the neighbor. *static* – Delete matching static entries. *dynamic* – Delete matching dynamic entries. *all* – All entries including static and dynamic entries will be deleted.
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-2000-28MP:5# delete ipv6 neighbor_cache 3ffc::1
Command: delete ipv6 neighbor_cache 3ffc::1

Success.
DGS-2000-28MP: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	*ipv6address <ipv6_addr>* –The IPv6 address of the neighbor. *static* – Display all static neighbor cache entries. *dynamic* – Display all dynamic entries. *all* – Displays all entries including static and dynamic entries.
Restrictions	None.

Example usage:

To show all neighbor cache entries on the switch:

```
DGS-2000-28MP:5# show ipv6 neighbor_cache ipif all static
Command: show ipv6 neighbor_cache ipif all static

Neighbor                  Link Layer Address    Interface   State
------------------------------ ------------------   ---------- ------
3ffc::1                   00-01-02-03-04-05     System      Static

Total Entries      : 1

DGS-2000-28MP:5#
```

config ipv6 nd ns ipif

Purpose	Configures the IPv6 ND neighbor solicitation retransmit time，which is the time between the retransmission of neighbor solicitation messages to a neighbor, when resolving the address or when probing the reachability of a neighbor.
Syntax	**config ipv6 nd ns ipif 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	*retrans_time <integer 1 - 3600>* – Neighbor solicitation's retransmit timer in milliseconds. It has the same value as the RA retrans_time in the config IPv6 ND RA command. If the retrans_time parameter is configured in one of the commands, the retrans_time value in the other command will also change so that the values in both commands are the same. The range if 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-2000-28MP:5# config ipv6 nd ns ipif System retrans_time 100
Command: config ipv6 nd ns ipif System retrans_time 100

Success.
DGS-2000-28MP:5#
```

show ipv6 nd ipif

Purpose	Used to display information regarding neighbor detection on the switch.
Syntax	**show ipv6 nd ipif <ipif_name (12)>**
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-2000-28MP:5#  show ipv6 nd
Command: show ipv6 nd

Interface Name              : System
NS Retransmit Time          : 1(ms)

DGS-2000-28MP:5#
```

enable ipif_ipv6_link_local_auto

Purpose	Used to enable the autoconfiguration of the link local address when no IPv6 address is configured.

Syntax	**enable ipif_ipv6_link_local_auto <ipif_name (12)>**
Description	This **enable ipif_ipv6_link_local_auto <ipif_name (12)>** 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-2000-28MP:5# enable ipif_ipv6_link_local_auto System
Command: enable ipif_ipv6_link_local_auto System

Success.
DGS-2000-28MP:5#
```

disable ipif_ipv6_link_local_auto

Purpose	Used to disable the autoconfiguration of the IPv6 link local address.
Syntax	**disable ipif_ipv6_link_local_auto <ipif_name (12)>**
Description	This **disable ipif_ipv6_link_local_auto <ipif_name (12)>** 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-2000-28MP:5# disable ipif_ipv6_link_local_auto System
Command: disable ipif_ipv6_link_local_auto System

Success.
DGS-2000-28MP:5#
```

24

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 > | all] [enable | disable]
show mac_notification	

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-2000-28MP:5# enable mac_notification
Command: enable mac_notification

Success.
DGS-2000-28MP: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-2000-28MP:5# disable mac_notification
Command: disable mac_notification

Success.
DGS-2000-28MP: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	*interval <int 1-2147483647>* − The time in seconds between notifications. The user may choose an interval between 1 and 2147483647 seconds. *historysize <1-500>* − 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-2000-28MP:5# config mac_notification interval 1
Command: config mac_notification interval 1

Success.
DGS-2000-28MP:5#
```

config mac_notification ports

Purpose	Used to configure MAC address notification status settings.
Syntax	**config mac_notification ports [<portlist > | all] [enable | disable]**
Description	The **config mac_notification ports** command is used to monitor MAC addresses learned and entered into the FDB.
Parameters	*<portlist >* − Specifies a port or range of ports to be configured. *all* – Entering this command will set all ports on the system. *[enable | disable]* – 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-2000-28MP:5# config mac_notification ports 7 enable
Command: config mac_notification ports 7 enable

Success.
```

```
DGS-2000-28MP: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-2000-28MP:5# show mac_notification
Command: show mac_notification

Global Mac Notification Settings

State          : Enabled
Interval       : 1
History Size   : 1
DGS-2000-28MP:5#
```

show mac_notification ports

Purpose	Used to display the Switch's MAC address table notification status settings.
Syntax	**show mac_notification ports <portlist >**
Description	The **show mac_notification ports** command is used to display the Switch's MAC address table notification status settings.
Parameters	*<portlist>* − Specify a port or group of ports to be viewed. 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-2000-28MP: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-2000-28MP:5#
```

25

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}
config igmp_snooping	[vlan_name <string 20> | vlanid <vidlist> | all] [host_timeout <sec 130-153025> | router_timeout <sec 60-600> | fast_leave [enable | disable] | | report_suppression [enable | disable] | state [enable | disable] | proxy_reporting [state {enable | disable} source_ip <ipaddr>]]
config igmp_snooping querier	[vlan_name <string 20> | vlanid <vidlist> | all] state [enable | disable] {querier_version [2 | 3] | last_member_query_interval <sec 1-25> | query_interval <sec 60-600> | robustness_variable <value 2-255> | max_response_time <sec 10-25>}
create igmp_snooping static_group	[vlan <vlan_name 20> | vlanid <vlanid_list>] <ipaddr>
config igmp_snooping static_group	[vlan <vlan_name 20> | vlanid <vlanid_list>] <ipaddr> [add | delete] <portlist>
delete igmp_snooping static_group	[vlan <vlan_name 20> | vlanid <vlanid_list>] <ipaddr>
show igmp_snooping static_group	{vlan <vlan_name 20> | vlanid <vlanid_list> | <ipaddr>}
config igmp_snooping data_driven_learning	[all | vlan_name <string 20> | vlanid <vidlist>] {state [enable | disable] aged_out [enable | disable] [expiry_time <sec (130 - 153025)>] }
config igmp_snooping data_driven_learning max_learning_entry	<integer 1-1024>
clear igmp_snooping data_driven_group	[all | vlan_name <vlan_name 20> | vlanid < vidlist >] [all | MCGroupAddr <ipaddr>]
config router_ports	[vlan_name <string 20> | vlanid <vidlist> | all] [add | delete] <portlist>
config router_ports_forbidden	[vlan_name <string 20> | vlanid <vidlist> | all] [add | delete] <portlist>
show router_port	{vlan <vlan_name 32> | vlanid <vidlist> | static | dynamic | forbidden}
config igmp access_authentication ports	[<portlist> | all] state [enable | disable]
show igmp access_authentication ports	[<portlist> | all]
show igmp_snooping	{vlan <vlan_name 20> | vlanid <vidlist> }}

Command	Parameter
show igmp_snooping group	[vlan <vlan_name 32> | vlanid <vidlist>] <ipaddr> {data_driven}
show igmp_snooping forwarding	{vlan <vlan_name 32> | vlanid <vidlist>}
show igmp_snooping host	{ports <portlist> | group <ipaddr> | vlan <vlan_name 32> | vlanid <vidlist>}
show igmp_snooping statistic counter	[vlan_name <string 32> | vlanid <vidlist> | ports <portlist>]
clear igmp_snooping statistics counter	
config igmp_snooping rate_limit	state [enable | disable] rate <integer 1-200>
config igmp_snooping v3_src_filter	state [enable | disable]
show igmp_snooping v3_src_filter	

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	*{forward_mcrouter_only}* – Enables 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-2000-28MP:5# enable igmp_snooping
Command: enable igmp_snooping

Success.
DGS-2000-28MP: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. 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	*{forward_mcrouter_only}* – Disables forward mcrouter for IGMP Snooping on the Switch.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

TTo disable IGMP snooping on the Switch:

```
DGS-2000-28MP:5# disable igmp_snooping
Command: disable igmp_snooping


Success.
DGS-2000-28MP:5#
```

config igmp_snooping

Purpose	To configure IGMP snooping on the Switch.
Syntax	**config igmp_snooping [vlan_name <string 32> | vlanid <vidlist> | all] [host_timeout <sec 130-153025> | router_timeout <sec 60-600> | fast_leave [enable | disable] | report_suppression [enable | disable] | state [enable | disable] | proxy_reporting [state {enable | disable} source_ip <ipaddr>]]**
Description	The **config igmp_snooping** command configures IGMP snooping on the Switch.
Parameters	*vlan_name* <*string 32*> − The name of the VLAN for which IGMP snooping is to be configured. *vlanid* <*vidlist*> − The VLAN id for which IGMP snooping is to be configured. *all* − Specifies all VLAN for which IGMP snooping is to be configured. *host_timeout* <*sec 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. *router_timeout* <*sec 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. *fast_leave [enable* | *disable]* − Enables or disables the fast leave. *state [enable* | *disable]* − Enables or disables IGMP snooping for the specified VLAN. *proxy_reporting* **–**- Specifies the proxy reporting option *state* - Specifies the proxy reporting state. *enable* - Specifies that the proxy reporting option will be enabled. *disable* - Specifies that the proxy reporting option will be disabled. *source_ip* - Specifies the source IP address used. <*ipaddr*> - Enter the source IP address used here.
Restrictions	Only administrator, operator or power user-level users can issue this command.

Example usage:

To configure the igmp snooping:

```
DGS-2000-28MP:5# config igmp_snooping vlanid 2 fast_leave enable
```

```
host_timeout 130 leave_timer 2 report_suppression disable router_timeout 60
state enable
Command: config igmp_snooping vlanid 2 fast_leave enable host_timeout 130
leave_
timer 2 report_suppression disable router_timeout 60 state enable


Success.
DGS-2000-28MP:5#
```

config igmp_snooping querier

Purpose	To configure IGMP snooping querier on the Switch.
Syntax	**config igmp_snooping querier [vlan_name <string 32> | vlanid <vidlist> | all] state [enable | disable] {querier_version [2 | 3] | last_member_query_interval <sec 1-25> | query_interval <sec 60-600> | robustness_variable <value 2-255> | max_response_time <sec 10-25>}**
Description	The **config igmp_snooping querier** command enables IGMP snooping querier on a specific VLAN.
Parameters	*vlan_name* <*string 32*> − The name of the VLAN for which IGMP snooping is to be configured. Up to 20 characters can be used. *vlanid* <*vidlist*> − The VLAN id for which IGMP snooping is to be configured. *all* − Specifies all VLAN for which IGMP snooping is to be configured. *state [enable* | *disable]* − Enables/Disables IGMP Snooping Querier. *querier_version [2* | *3]* − Specifies the IGMP Querier version on the VLAN. *last_member_query_interval [sec 1-25]* − Specifies the IGMP last member query interval on the VLAN. *query_interval [sec 60-600]* − Specifies the IGMP query interval on the VLAN. *robustness_variable [value 2-255]* − Specifies the robustness on the VLAN. *max_response_time [sec 10-25]* − Specifies the max response time on the VLAN.
Restrictions	Only administrator, operator or power user-level users can issue this command.

Example usage:

To configure the igmp snooping:

```
DGS-2000-28MP:5# config igmp_snooping querier vlanid 2 state enable
Command: config igmp_snooping querier vlanid 2 state enable


Success .
DGS-2000-28MP:5#
```

create igmp_snooping static_group

Purpose	To create an IGMP snooping static group on the Switch.
Syntax	**create igmp_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipaddr>**
Description	The **create igmp_snooping static_group** command allows you to create an IGMP snooping static group. Member ports can be added to the static group. The static member and the dynamic member port from the member ports of a group. The statis group will only take effect when IGMP snooping is enabled on the VLAN. For those statis member ports, the device needs to emulate the IGMP protocol operation to the querier, and forward the traffic destined to the multicast group to the member ports.
Parameters	<*vlan_name 32*> − The name of the VLAN for which IGMP snooping statis group is to be created. Up to 32 characters can be used. <*vlanid_list*> − The ID of the VLAN for which IGMP snooping static group is to be created. The range is from 2 to 4094. <*ipaddr*> − Specify the static group address for which IGMP snooping to be created.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To create a igmp snooping static group 226.1.1.1 for VID 1:

```
DGS-2000-28MP:5# create igmp_snooping static_group vlanid 1 226.1.1.1
Command: create igmp_snooping static_group vlanid 1 226.1.1.1



Success.
DGS-2000-28MP:5#
```

config igmp_snooping static_group

Purpose	To configure the current IGMP snooping static group on the Switch.
Syntax	**config igmp_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipaddr> [add | delete] <portlist>**
Description	The **config igmp_snooping static_group** command is used to add or delete ports to /from the given static group.
Parameters	<*vlan_name 32*> − The name of the VLAN for which IGMP snooping static group is to be configured. Up to 32 characters can be used. *[add* | *delete]* − Specify whether to add or delete ports defined in the following parameter <ipaddr>. <*ipaddr*> − Specify the IP address to be configured with the IGMP snooping static group.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To add port 5 to static group 226.1.1.1 on VID 1:

```
DGS-2000-28MP:5# config igmp_snooping static group vlanid 1 226.1.1.1 and 5


Success.DGS-2000-28MP:5#
```

delete igmp_snooping static_group

Purpose	To delete the current IGMP snooping static group on the Switch.
Syntax	**delete igmp_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipaddr>**
Description	The **delete igmp_snooping static_group** command is used to delete an IGMP snooping statie group will not affect the IGMP snooping dynamic member ports of a group.
Parameters	<*vlan_name 32*> − The name of the VLAN for which IGMP snooping statis group is to be created. Up to 32 characters can be used. <*vlanid_list*> − The ID of the VLAN for which IGMP snooping static group is to be created. The range is from 2 to 4094. <*ipaddr*> − Specify the static group address for which IGMP snooping to be deleted.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To delete a static group 226.1.1.1 on VID 1:

```
DGS-2000-28MP:5# delete igmp_snooping static_group vlanid 1 226.1.1.1
Command: delete igmp_snooping static_group vlanid 1 226.1.1.1


Success.
DGS-2000-28MP:5#
```

show igmp_snooping static_group

Purpose	To display the IGMP snooping static group information on the Switch.
Syntax	show igmp_snooping **statis_group vlan <vlan_name 32> | vlanid <vlanid_list> | <ipaddr>}**
Description	The show igmp_snooping **statis_group** command displays the IGMP snooping static group information on the Switch.
Parameters	<*vlan_name 32*> − The name of the VLAN for which IGMP snooping static group to be displayed. <*vlanid_list*> − The VLAN id of IGMP snooping static group to be displayed. <*ipaddr*> − Specify the IP address of IGMP snooping static group to be displayed.
Restrictions	None.

Example usage:

To display the IGMP snooping static group information on the Switch:

```
DGS-2000-28MP:5# show igmp_snooping static_group vlan default
Command: show igmp_snooping static_group vlan default


 VLAN ID/Name     IP Address     Static Member Ports
 ----------------------  ---------------  --------------------------------
 1     default          226.1.1.1          None

Total Entries : 1

DGS-2000-28MP:5#
```

config igmp_snooping data_driven_learning

Purpose	To enable or disable the data driven learning of an IGMP snooping group. When data-driven learning is enabled for the VLAN, when the Switch receives the IP multicast traffic on this VLAN, an IGMP snooping group will be created. That is, the learning of an entry is not activated by IGMP membership registration, but activated by the traffic. For an ordinary IGMP snooping entry, the IGMP protocol will take care of the aging out of the entry. For a data-driven entry, the entry can be specified not to be aged out or to be aged out by the aged timer. When data driven learning is enabled, and the data driven table is not full, the multicast filtering mode for all ports is ignored. That is, the multicast packets will be forwarded to router ports. If the data driven learning table is full, the multicast packets will be forwarded according to the multicast filtering mode. Note that if a data-driven group is created and IGMP member ports are learned later, the entry will become an ordinary IGMP snooping entry. That is, the aging out mechanism will follow the ordinary IGMP snooping entry.
Syntax	**config igmp_snooping data_driven_learning [all | vlan_name <string 32> | vlanid <vidlist>] {state [enable | disable] aged_out [enable | disable]}**
Description	The **config igmp_snooping data_driven_learning** command is used to enable or disable the data driven learning of an IGMP snooping group.
Parameters	*all* – Specifies all VLANs to be configured. *vlan_name* <*string 32*> − The name of the VLAN for which IGMP snooping is to be configured. Up to 32 characters can be used. *vlanid* <*vidlist*> − Specifies the VLAN ID to be configured. *state [enable | disable]* – Specifies to enable or disable the data driven learning of an IGMP snooping group. The defaule is enabled. *age_out [enable | disable]* – Specifies to enable or disable the aging out of the entry.By default, the state is enabled.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To enable the data driven learning of an IGMP snooping group on the defaultVLAN:

```
DGS-2000-28MP:5# config igmp_snooping data_driven_learning vlan_name default
Command: config igmp_snooping data_driven_learning vlan_name default

Success.
DGS-2000-28MP:5#
```

config igmp_snooping data_driven_learning max_learning_entry

Purpose	To configure the maximum number of groups that can be learned by data driven. When the table is full, the system will stop the learning of the new dada-driven groups. Traffic for the new groups will be dropped.
Syntax	**config igmp_snooping data_driven_learning max_learned_entry <integer 1-1024>**
Description	The **config igmp_snooping data_driven_learning** command is used to configure the maximum number of groups that can be learned by data driven.
Parameters	*max_learned_entry <integer 1-1024>* – Specifies the maximum number of groups that can be learned by data drive. This value must be between 1 and 1024, and the suggested default setting is 56.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To set the maximum number of groups that can be learned by data driven:

```
DGS-2000-28MP:5# config igmp_snooping data_driven_learning max_learned_entry 50
Command: config igmp_snooping data_driven_learning max_learned_entry 50

Success.
DGS-2000-28MP:5#
```

clear igmp_snooping data_driven_group

Purpose	To clear the IGMP snooping group learned by data drive.
Syntax	**clear igmp_snooping data_driven_group [all | vlan_name <vlan_name 32> | vlanid <vidlist>] [all | MCGroupAddr <ipaddr>]**
Description	The **config igmp_snooping data_driven_learning** command is used to delete the IGMP snooping group learned by data drive. Note that this commands is currently only for layer 2 switches.
Parameters	*all* − Delete all data driven entries. *vlan_name <vlan_name 32>* − The name of the VLAN for which

	IGMP snooping is to be configured. Up to 32 characters can be used. *vlanid* <vidlist> − Specify the vlan id of the IGMP snooping data driven group on the Switch. <ipaddr> - Specifies the IP address.
Restrictions	Only administrator, operator or power user-level users can issue this command.

Example usage:

To clear the igmp snooping data driven group on the Switch:

```
DGS-2000-28MP:5# clear igmp_snooping data_driven_group all
Command: clear igmp_snooping data_driven_group all


Success.
DGS-2000-28MP:5#
```

config router_ports

Purpose	To configure ports as router ports.
Syntax	**config router_ports [vlan_name <string 32> | vlanid <vidlist> | all] [add | delete] <portlist>**
Description	The **config router_ports** command DGSignates 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	*vlan_name* <*string 32*> − The name of the VLAN on which the router port resides. Up to 32 characters can be used. *vlanid* <*vidlist*> − The VLAN id of the VLAN on which the router port resides. *all* − Specifies all ports on the Switch to be configured. *[add* | *delete]* – Specifies whether to add or delete ports defined in the following parameter <portlist>, to the router port function. <*portlist*> − A port or range of ports that will be configured as router ports.
Restrictions	Only administrator, operator or power user-level users can issue this command.

Example usage:

To add the static router ports 1-5:

```
DGS-2000-28MP:5# config router_ports vlanid 1 add 1-5
Command: config router_ports vlanid 1 add 1-5


Success.
DGS-2000-28MP:5#
```

config router_ports_forbidden

Purpose	To deny ports becoming router ports.

Syntax	**config router_ports_forbidden [vlan_name <string 32> | vlanid <vidlist> | all] [add | delete] <portlist>**
Description	The **config router_port_forbidden** command denies a range of ports access to multicast–enabled routers. This ensures all packets with such a router as its destination will not reach the multicast–enabled router − regardless of protocol, etc.
Parameters	*vlan_name* <*string 32*> − The name of the VLAN on which the router port resides. Up to 32 characters can be used. *vlanid* <*vidlist*> − The VLAN id of the VLAN on which the router port resides. *all* − Specifies all ports on the Switch to be configured. *[add* | *delete]* – Specifies whether to deny ports defined in the following parameter <portlist>, to the router port function. <*portlist*> − A port or range of ports that will be denied access as router ports.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To deny router ports:

```
DGS-2000-28MP:5# config router_ports_forbidden vlanid 2 add 10-12
Command: config router_ports_forbidden vlanid 2 add 10-12


Success.
DGS-2000-28MP:5#
```

show router_ports

Purpose	To display the currently configured router ports on the Switch.
Syntax	**show router_ports {vlan <vlan_name 32> | vlanid <vidlist> | static | dynamic | forbidden}**
Description	The **show router_ports** command displays the router ports currently configured on the Switch.
Parameters	*vlan* <*vlan_name 32*> − The name of the VLAN on which the router port resides. Up to 32 characters can be used. *vlanid* <*vidlist*> − The ID of the VLAN on which the router port resides. *static* − Displays router ports that have been statically configured. *dynamic* − Displays router ports that have been dynamically learned. *forbidden* − Displays router ports that have been forbidden configured.
Restrictions	None.

Example usage:

To display the router ports.

```
DGS-2000-28MP:5# show router_ports
Command: show router_ports

VLAN Name          : default
```

```
Static router port      :
Dynamic router port   :
Forbidden router port :

Total Entries : 1
DGS-2000-28MP:5#
```

config igmp access_authentication ports

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

Example usage:

To configure authentication port of IGMP:

```
DGS-2000-28MP:5# config igmp access_authentication ports all state enable
Command: config igmp access_authentication ports all state enable


Success.
DGS-2000-28MP:5#
```

show igmp access_authentication ports

Purpose	To display the IGMP access authentication configuration on the Switch.
Syntax	**show igmp access_authentication ports [<portlist> | all]**
Description	The **show igmp access_authentication** command displays the IGMP access authentication configuration on the Switch.
Parameters	*all* − Specifies all ports to be displayed. *<portlist>* − A port or range of ports to be displayed on the Switch.
Restrictions	Only administrator, operator or power user-level users can issue this command.

Example usage:

To display the IGMP access authentication:

```
DGS-2000-28MP:5# show igmp access_authentication ports 1-5
Command: show igmp access_authentication ports 1-5
```

```
Port  Authentication State
------ ----------------------------------
1      Disabled
2      Disabled
3      Disabled
4      Disabled
5      Disabled

DGS-2000-28MP:5#
```

show igmp_snooping

Purpose	To show the current status of IGMP snooping on the Switch.
Syntax	**show igmp_snooping** {**vlan <vlan_name 32> | vlanid <vidlist> | multicast_vlan <vlan_name 32> | multicast_vlan_group <vlan_name 32>}**
Description	The **show igmp_snooping** command displays the current IGMP snooping configuration on the Switch.
Parameters	<*vlan_name 32*> − The name of the VLAN for which IGMP snooping configuration is to be displayed. Up to 32 characters can be used. <*vidlist*> − The vid of the VLAN for which IGMP snooping configuration is to be displayed.
Restrictions	None.

Example usage:

To show igmp snooping:

```
DGS-2000-28MP:5# show igmp_snooping vlan default
Command: show igmp_snooping 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 group

Purpose	To display the current IGMP snooping group configuration on the Switch.
Syntax	**show igmp_snooping group [vlan <vlan_name 32> | vlanid <vidlist>] <ipaddr> {data_driven}**
Description	The **show igmp_snooping group** command displays the current IGMP snooping group configuration on the Switch.
Parameters	*vlan <vlan_name 32>* − The name of the VLAN for which IGMP snooping group configuration information is to be displayed. Up to 32 characters can be used. *vlanid <vidlist>* − The ID of the VLAN for which IGMP snooping group configuration infor mation is to be displayed. *<ipaddr>* − The IP address of the VLAN for which IGMP snooping group configuration infor mation is to be displayed. *{data_driven}* − Specifies to display the data driven of IGMP snooping group.
Restrictions	None.

Example usage:

To show igmp snooping group:

```
DGS-2000-28MP:5# show igmp_snooping group vlan default
Command: show igmp_snooping group vlan default


Total Entries : 0


DGS-2000-28MP:5#
```

show igmp_snooping forwarding

Purpose	To display the IGMP snooping forwarding table entries on the Switch.
Syntax	**show igmp_snooping forwarding {vlan <vlan_name 32> | vlanid <vidlist>}**
Description	The **show igmp_snooping forwarding** command displays the current IGMP snooping forwarding table entries currently configured on the Switch.
Parameters	*vlan <vlan_name 32>* − The name of the VLAN for which IGMP snooping forwarding table information is to be displayed. Up to 32 characters can be used. *vlanid <vidlist>* − The vid of the VLAN for which IGMP snooping forwarding table information is to be displayed.
Restrictions	None.

Example usage:

To view the IGMP snooping forwarding table for VLAN 'Trinity':

```
DGS-2000-28MP:5# show igmp_snooping forwarding vlan default
Command: show igmp_snooping forwarding vlan default

VLAN Name      : Trinity
Multicast group : 224.0.0.2
MAC address    : 01-00-5E-00-00-02
Port Member    : 3,4
Total Entries  : 1

DGS-2000-28MP:5#
```

show igmp_snooping host

Purpose	To display the IGMP snooping host table entries on the Switch.
Syntax	**show igmp_snooping host {ports <portlist> | group <ipaddr> | vlan <vlan_name 32> | vlanid <vidlist>}**
Description	The **show igmp_snooping host** command displays the current IGMP snooping forwarding table entries currently configured on the Switch.
Parameters	*ports* <*portlist*> − The ports of IGMP snooping host table information are to be displayed. *group* <*ipaddr*> − The IP address of IGMP snooping host table information are to be displayed. *vlan* <*vlan_name 32*> − The name of the VLAN for which IGMP snooping host table information is to be displayed. Up to 32 characters can be used. *vlanid* <*vidlist*> − The vid of the VLAN for which IGMP snooping host table information is to be displayed.
Restrictions	None.

Example usage:

To view the IGMP snooping host table on the Switch:

```
DGS-2000-28MP:5# show igmp_snooping host
Command: show igmp_snooping host

VLAN ID    Group                Port No     IGMP Host
 ------    ---------------------  ---------   ------------


Total Entries : 0

DGS-2000-28MP:5#
```

show igmp_snooping statistic counter

Purpose	To display the statistics counter for IGMP protocol packets that are received by the Switch since IGMP snooping was enabled.
Syntax	**show igmp_snooping statistic counter [vlan_name <string 32> |**

	vlanid <vidlist> | ports <portlist>]
Description	The **show igmp_snooping statistic counter** command displays the statistics counter for IGMP protocol packets that are received by the Switch since IGMP snooping was enabled.
Parameters	*vlan_name <string 32>* − Specify the VLAN name to be displayed. *vlanid <vidlist>* − Specify the VLAN ID to be displayed. *ports <portlist>* - Specify a list of ports to be displayed.
Restrictions	None.

Example usage:

To display the IGMP snooping statistics counter for VLAN ID 1:

```
DGS-2000-28MP:5# show igmp_snooping statistic counter vlanid 1
Command: show igmp_snooping statistic counter vlanid 1

VLAN Name       : default
------------------------------------------------------------------
Group Number                          : 0

Receive Statistics
   Query
     IGMP v1 Query                    : 0
     IGMP v2 Query                    : 0
     IGMP v3 Query                    : 0
     Total                            : 0
     Dropped By Multicast VLAN        : 0

   Report & Leave
     IGMP v1 Report                   : 0
     IGMP v2 Report                   : 0
     IGMP v3 Report                   : 0
     IGMP v2 Leave                    : 0
     Total                            : 0
     Dropped By Max Group Limitation  : 0
     Dropped By Multicast VLAN        : 0

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

clear igmp_snooping statistic counter

Purpose	To clear the IGMP snooping statistics counter.
Syntax	**clear igmp_snooping statistic counter**
Description	The **clear igmp_snooping statistic counter** command used to clear the IGMP snooping statistics counter.
Parameters	None.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To clear the IGMP snooping statistics counter:

```
DGS-2000-28MP:5# clear igmp_snooping statistics counter
Command: clear igmp_snooping statistics counter


Success.
DGS-2000-28MP:5#
```

config igmp_snooping rate_limit

Purpose	To configure the maximum rate for switch to process IGMP control packets.
Syntax	**config igmp_snooping rate_limit state [enable | disable] rate <integer 1-200>**
Description	This command is used to limit the maximum rate that switch to process the IGMP control packet (IGMP report, IGMP leave, IGMP query). The overlimt packets will be ignored.
Parameters	*state* – the state of limiting IGMP control packets *enable* – Enable the limiting feature *disable* – Disable the limiting feature *rate* – Specify the rate in PPS <*integer 1-200*> - Specify the range in 1-200
Restrictions	Only administrator or operator-level users can issue this command..

Example usage:

To configure the maximum rate to 100pps of IGMP control packets:

```
DGS-2000-28:5# config igmp_snooping rate_limit rate 100 state enable
Command: config igmp_snooping rate_limit rate 100 state enable


Success.
DGS-2000-28:5# show igmp_snooping
Command: show igmp_snooping


 IGMP Snooping Global State    : Enable
 Host Timeout              : 260
 Router Timeout            : 125
 Max Learned Entry Value       : 1024
 Forward Router Only           : Disable
 Rate Limit Status         : Enable
 Rate Limit Value          : 100
```

config igmp_snooping v3_src_filter

Purpose	To configure larning mode of IGMPv3.
Syntax	**config igmp_snooping v3_src_filter state [enable | disable]**

Description	This command is change the learning mode of IGMPv3 network. The system changed to “host mode” when v3_src_filter enabled.
Parameters	*state* – the state of limiting IGMP control packets *enable* – Enable the limiting feature *disable* – Disable the limiting feature
Restrictions	Only administrator or operator-level users can issue this command..

Example usage:

To configure IGMPv3 source filter mode enabled:

```
DGS-2000-28MP:5# config igmp_snooping v3_src_filter state enable
Command: config igmp_snooping v3_src_filter state enable


Success.

DGS-2000-28MP:5#
```

show igmp_snooping v3_src_filter

Purpose	To display larning mode of IGMPv3.
Syntax	**show igmp_snooping v3_src_filter**
Description	This command is show the learning mode of IGMPv3 network.
Parameters	None
Restrictions	None

Example usage:

To display the IGMPv3 source filter mode:

```
DGS-2000-28MP:5# show igmp_snooping v3_src_filter state
Command: show igmp_snooping v3_src_filter state

igmp_snooping v3_src_filter state : Enabled
DGS-2000-28MP:5#
```

26

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 <string 20> | vlanid <vidlist> | all] [host_timeout <sec 130-153025> | router_timeout <sec 60-600> | fast_leave [enable | disable] | | report_suppression [enable | disable] | state [enable | disable] | proxy_reporting [state {enable | disable} source_ip <ipaddr>]]
config mld_snooping querier	[vlan_name <string 20> | vlanid <vidlist> | all] state [enable | disable] {querier_version [2 | 3] | last_member_query_interval <sec 1-25> | query_interval <sec 60-600> | robustness_variable <value 2-255> | max_response_time <sec 10-25>}
config mld_snooping data_driven_learning	[all | vlan_name <string 20> | vlanid <vidlist>] {state [enable | disable] aged_out [enable | disable] [expiry_time <sec (130 - 153025)>] }
config mld_snooping data_driven_learning max_learning_entry	<integer 1-1024>
clear mld_snooping data_driven_group	{all | {vlan_name <string (20)> | vlanid <vidlist> } [<ipv6_addr>] [all]}
config mld_snooping mrouter_ports	[vlan_name <string 20> | vlanid <vidlist> | all] [add | delete] <portlist>
config mld_snooping mrouter_ports_forbidden	[vlan_name <string 20> | vlanid <vidlist> | all] [add | delete] <portlist>
show mld_snooping mrouter_ports	{vlan <vlan_name 20> | vlanid <vidlist> | static | dynamic | forbidden}
show mld_snooping	{vlan_name <string (20)> | vlanid <vidlist> | all}
show mld_snooping group	{vlan_name <string (20)> | vlanid <vidlist> | ports <portlist> | all} [<ipv6_addr>] [data_driven]
show mld_snooping forwarding	{vlan <vlan_name 20> | vlanid <vidlist>}
show mld_snooping host	{vlan_name <string 20> | vlanid <vidlist> | ports <portlist> | group <ipv6_addr> | all }
show mld_snooping statistic counter	[vlan_name <string 20> | vlanid <vidlist> | ports <portlist>]
clear mld_snooping statistics counter	
config mld_snooping v3_src_filter	state [enable | disable]

Command	Parameter
show mld_snooping v3_src_filter	

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-2000-28MP:5# enable mld_snooping
Command: enable mld_snooping

Success !
DGS-2000-28MP: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-2000-28MP:5# disable mld_snooping
Command: disable mld_snooping

Success !
DGS-2000-28MP:5#
```

config mld_snooping

Purpose	To configure mld snooping.
Syntax	**config mld_snooping [vlan_name < string 32> | vlanid <vidlist> | all] {fast_done [enable | disable] | host_timeout <sec 130-153025> | leave_timer <sec 1-25> | report_suppression [enable | disable] | router_timeout <sec 60-600> | state [enable | disable]}**

Description	The **config mld_snooping** command defines mld snooping on the VLAN.
Parameters	*vlan_name <string 32>* – Specifies that the mld snooping applies only to this previously created VLAN. vlanid <vidlist> – Specifies that the mld snooping applies only to this VLAN id. *all* – specifies that MLD snooping is to be configured for all VLANs on the Switch. *fast_done [enable | disable]* – Specifies the fast down to be enabled or disabled. *host_timeout <sec 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. *leave_timer <sec 1-25>* – Specifies the maximum amount of time a host can be a member of a multicast group after sending a done timer membership report. The default is 10 seconds. *report_suppression [enable | disable]* – Specifies the report suppression to be enabled or disabled. *router_timeout <sec 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 done timer. The default is 300 seconds. *state [enable | disable]*– Allows the user to enable or disable MLD snooping for the specified VLAN.
Restrictions	Only administrator, operator or power user–level users can issue this command.

Example usage:

To configure mld snooping:

DGS-2000-28MP:5# config mld_snooping vlan_name default fast_done disable host_timeout 130 leave_timer 3 router_timeout 60 state enable

Command: config mld_snooping vlan_name default fast_done disable host_timeout 130 leave_timer 3 router_timeout 60 state enable

Success.

DGS-2000-28MP: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 <string 32> | vlanid <vidlist> | all] [last_listener_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 maximum time to wait for reports from listeners and the permitted packet loss guaranteed by MLD snooping.

Parameters	*vlan_name* <*string 32*> – Specifies that the mld snooping applies only to this previously created VLAN. *vlanid* <*vidlist*> – specifies that the mld snooping applies only to this previously created VLAN id. *all* – specifies that MLD snooping is to be configured for all VLANs on the Switch. *last_listener_query_interval* <*sec 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. *max_response_time* <*sec 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. *query_interval* <*sec 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. *robustness_variable* <*value 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. *state [enable*	*disable]* – 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. *version* <*value 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.
Restrictions	Only administrator, operator or power user–level users can issue this command.

Example usage:

To configure MLD snooping querier:

```
DGS-2000-28MP:5#config mld_snooping querier all last_listener_query_interval 1 max_response_time 10 query_interval 60 robustness_variable 2 state disable version 1
Command: config mld_snooping querier all last_listener_query_interval 1 max_response_time 10 query_interval 60 robustness_variable 2 state disable version 1

Success.
DGS-2000-28MP:5#
```

config mld_snooping data_driven_learning

Purpose	To enable or disable the data-driven learning of an MLD snooping group on the Switch.
Syntax	**config mld_snooping data_driven_learning [max_learned_entry <value 1-1024>| vlan_name <string 32> | vlanid <vidlist> | all] [age_out [disable | enable] | expiry_time <sec 130-1530255> | state [enable | disable]]**
Description	The **config mld_snooping data driven_learning** command used to

	enable or disable the data-driven learning of an MLD snooping group.
Parameters	*max_learned_entry <value 1-1024>* – Speciifies the maximum learning entry value. *vlan_name <string 32>* – Specifies that the mld snooping applies only to this previously created VLAN. *vlanid <vidlist>* – Specifies that the mld snooping applies only to this previously created VLAN id. *all* – Specifies that MLD snooping is to be configured for all VLANs on the Switch. *age_out [disable | disable]* –Enable or disable the aging out of entries. By default, the state is disabled. *expiry_time <sec 130-1530255>* –Specify the data driven group lifetime, in seconds. The value is between 130 and 1530255. *state [enable | disable]* –Specify to enable or disable the data driven learning of MLD snooping groups.
Restrictions	Only administrator–level users can issue this command.

Example usage:

To enable the data driven learning of an MLD snooping group on the default VLAN:

```
ES-1210-28:5# config mld_snooping data_driven_learning vlan_name default state enable
Command: config mld_snooping data_driven_learning vlan_name default state enable

Success.
DGS-2000-28MP:5#
```

config mld_snooping data_driven_learning max_learned_entry

Purpose	To configure the maximum number of groups that can be learned by data driven. When the table is full, the system will stop the learning of the new dada-driven groups. Traffic for the new groups will be dropped.
Syntax	**config mld_snooping data_driven_learning max_learned_entry <integer 1-1024>**
Description	The **config mld_snooping data_driven_learning** command is used to configure the maximum number of groups that can be learned by data driven.
Parameters	*max_learned_entry <integer 1-1024>* – Specifies the maximum number of groups that can be learned by data drive. This value must be between 1 and 1024, and the suggested default setting is 56.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To set the maximum number of groups that can be learned by data driven:

```
DGS-2000-28MP:5# config mld_snooping data_driven_learning max_learned_entry 50
```

```
Command: config mld_snooping data_driven_learning max_learned_entry 50


Success.
DGS-2000-28MP:5#
```

clear mld_snooping data_driven_group

Purpose	To clear the mld snooping data driven group on the Switch.
Syntax	**clear mld_snooping data_driven_group [vlan_name <string 32> | vlanid <vidlist> | all] {<ipv6_addr> | all}**
Description	The **clear mld_snooping data_driven_group** command used to clear the mld snooping data driven group on the Switch.
Parameters	*vlan_name* <*string 32*> – Clear that the mld snooping applies only to this previously created VLAN. *vlanid* <*vidlist*> – Clear that the mld snooping applies only to this previously created VLAN id. *all* – Clear that MLD snooping is to be configured for all VLANs on the Switch. *{<ipv6_addr> | all}* – Specifies the IPv6 address or all of mld snooping data driven group to be removed.
Restrictions	Only administrator–level users can issue this command.

Example usage:

To clear MLD snooping data driven group:

```
DGS-2000-28MP:5# clear mld_snooping data_driven_group vlan_name rd1
Command: clear mld_snooping data_driven_group vlan_name rd1


Success.
DGS-2000-28MP:5#
```

config mld_snooping mrouter_ports

Purpose	To enable mld mrouter ports.
Syntax	**config mld_snooping mrouter_ports** [vlan_name **<string 32> | vlanid <vidlist> | all] [add | delete] <portlist>**
Description	The **config mld_snooping mrouter_ports** command defines a port that is connected to a multicast router port.
Parameters	*vlan_name* <*string 32*> – specifies that the mld snooping applies only to this previously created VLAN. *vlanid* <*vidlist*> – specifies that the mld snooping applies only to this previously created VLAN id. *all* – specifies that MLD snooping is to be configured for all VLANs on the Switch. *add* – Adds a specified port to the mld snooping mrouter port. *delete* – Deletes a specified port to the mld snooping mrouter port. <*portlist*> – Defines the ports to be included from the mld snooping mrouter group.

Restrictions	Only administrator, operator or power user–level users can issue this command. Separate non–consecutive Ethernet ports with a comma and no spaces; use a hyphen to DGSignate a range of ports. These ports are defined as connected to a multicast router.

Example usage:

To configure mld mrouter ports:

```
DGS-2000-28MP:5# config mld_snooping mrouter_ports vlanid 1 add 1-3
Command: config mld_snooping mrouter_ports vlanid 1 add 1-3


Success.
DGS-2000-28MP:5#
```

config mld_snooping mrouter_ports_forbidden

Purpose	To define mld mrouter ports forbidden on the Switch.
Syntax	**config mld_snooping mrouter_ports_forbidden [vlan_name <string 32> | vlanid <vidlist> | all] [add | delete] <portlist>**
Description	The **config mld_snooping mrouter_ports_forbidden** command forbids a port from being defined as a multicast router port by static configuration or by automatic learning.
Parameters	*vlan_name <string 32>* – Specifies that the mld snooping applies only to this previously created VLAN. *vlanid <vidlist>* – specifies that the mld snooping applies only to this previously created VLAN id. *all* – specifies that MLD snooping is to be configured for all VLANs on the Switch. *add* – Adds a specified port to the mld snooping mrouter port. *delete* – Deletes a specified port to the mld snooping mrouter port. <*portlist*> – Defines the ports to be included from the mld snooping mrouter group.
Restrictions	Only administrato–level users can issue this command.

Example usage:

To define the MLD snooping mrouter forbidden:

```
DGS-2000-28MP:5# config mld_snooping mrouter_ports_forbidden vlanid 1 add 8
Command: config mld_snooping mrouter_ports_forbidden vlanid 1 add 8


Success.
DGS-2000-28MP:5#
```

show mld_snooping mrouter_ports

Purpose	To display information on dynamically learnt and static multicast router interfaces.
Syntax	**show mld_snooping mrouter_ports [vlan_name <string 32> | vlanid <vidlist> | all] [dynamic | static | forbidden]**

Description	The **show mld_snooping mrouter_port** command displays on dynamically learnt and static multicast router interfaces.
Parameters	*vlan_name* <*string 32*> – Specifies on which VLAN mld snooping groups should be shown. *vlanid* <*vidlist*> – Displays that the mld snooping applies only to this previously created VLAN id. *all* – Displays that all MLD snooping which configured for all VLANs on the Switch. *static* − Displays statically configured MLD router ports. *dynamic* − Displays dynamically configured MLD router ports. *forbidden* – Displays forbidden router ports that have been statically configured.
Restrictions	None.

Example usage:

To show the MLD_snooping mrouterport:

```
DGS-2000-28MP:5# show mld_snooping mrouter_ports vlanid 1 static
Command: show mld_snooping mrouter_ports vlanid 1 static

VLAN Name          : default
Static router port    : 1-3

Total Entries : 1
DGS-2000-28MP: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	*vlan* <*vlan_name 20*> – Displays that the mld snooping applies only to this previously created VLAN. *vlanid* <*vidlist 1-4094*> – Displays that the mld snooping applies only to this previously created VLAN id. *all* – Displays that MLD snooping which configured for all VLANs on the Switch.
Restrictions	None.

Example usage:

To show the MLD snooping:

```
DGS-2000-28MP: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-2000-28MP: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	*vlan <vlan_name 20>* – The name of the VLAN for which to view the MLD snooping group configurations. *vlanid <vidlist 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-2000-28MP:5#  show mld_snooping group vlan default
Command: show mld_snooping group vlan default

Total Entries: 0

DGS-2000-28MP:5#
```

show mld_snooping forwarding

Purpose	To display mld snooping settings on the Switch.
Syntax	**show mld_snooping forwarding [vlan_name <string 32> | vlanid <vidlist> | all]**
Description	The **show mld_snooping forwarding** command displays the current MLD snooping forwarding table entries currently configured on the Switch.
Parameters	*vlan_name <string 32>* – Displays that the mld snooping applies only to this previously created VLAN.

	vlanid <*vidlist*> – Displays that the mld snooping applies only to this previously created VLAN id. *all* – Displays that all MLD snooping which configured for all VLANs on the Switch.
Restrictions	None.

Example usage:

To display the MLD snooping forwarding:

```
DGS-2000-28MP:5# show mld_snooping forwarding all
Command: show mld_snooping forwarding all


Total Entries : 0
DGS-2000-28MP:5#
```

show mld_snooping host

Purpose	To display information of MLD snooping host on the Switch.
Syntax	**show mld_snooping host [vlan_name <string 32> | vlanid <vidlist> | all | ports <portlist> | group <ipv6_addr>]**
Description	The **show mld_snooping host** command displays information of MLD snooping host on the Switch.
Parameters	*vlan_name* <*string 32*> – Specifies on which VLAN mld snooping groups should be shown. *vlanid* <*vidlist*> – Displays that the mld snooping applies only to this previously created VLAN id. *all* – Displays that all MLD snooping which configured for all VLANs on the Switch. *ports* <*portlist*> – Specifies the ports of MLD snooping host to be displayed. *group* <*ipv6_addr*> – Specifies the IPv6 address.
Restrictions	None.

Example usage:

To show the MLD_snooping host:

```
DGS-2000-28MP:5#  show mld_snooping host vlan_name default
Command: show mld_snooping host vlan_name default


Total Entries : 0
DGS-2000-28MP:5#
```

show mld_snooping statistics counter

Purpose	To display display the statistics counter for MLD protocol packets that are received by the Switch since MLD snooping was enabled.
Syntax	**show mld_snooping statistics counter [vlan_name <string 32> | vlanid <vlanid_list> | ports <portlist>]**

Description	The **show mld_snooping statistics counter** command displays the statistics counter for MLD protocol packets that are received by the Switch since MLD snooping was enabled.
Parameters	*vlan_name <string 32>* – Specifies on which VLAN name to be displayed. *vlanid <vidlist>* – Specifies on which VLAN ID to be displayed. *ports <portlist>* – Specifies the ports of MLD snooping ports to be displayed.
Restrictions	None.

Example usage:

To display the MLD_snooping statistics counter for port 1 to 3:

```
DGS-2000-28MP:5# show mld_snooping statistic counter ports 1-3
Command: show mld_snooping statistic counter ports 1-3

 Total Entries : 0


DGS-2000-28MP:5#
```

clear mld_snooping statistics counter

Purpose	To clear MLD snooping statistics counters.
Syntax	**clear mld_snooping statistics counter**
Description	The **clear mld_snooping statistics counter** command clears MLD snooping statistics counters.
Parameters	None.
Restrictions	Only administrator–level users can issue this command.

Example usage:

To clear the MLD_snooping statistics counters:

```
DGS-2000-28MP:5# clear mld_snooping statistics counter
Command: clear mld_snooping statistics counter


Success.
DGS-2000-28MP:5#
```

config mld_snooping v3_src_filter

Purpose	To configure larning mode of MLDv2.
Syntax	**config mld_snooping v3_src_filter state [enable | disable]**
Description	This command is change the learning mode of MLDv2 network. The system changed to “host mode” when v3_src_filter enabled.
Parameters	*state* – the state of limiting IGMP control packets *enable* – Enable the limiting feature *disable* – Disable the limiting feature

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

Example usage:

To configure IGMPv3 source filter mode enabled:

```
DGS-2000-28MP:5# config mld_snooping v3_src_filter state enable
Command: config mld_snooping v3_src_filter state enable


Success.

DGS-2000-28MP:5#
```

show mld_snooping v3_src_filter

Purpose	To display larning mode of MLDv2.
Syntax	**show mld_snooping v3_src_filter**
Description	This command is show the learning mode of MLDv2 network.
Parameters	None
Restrictions	None

Example usage:

To display the IGMPv3 source filter mode:

```
DGS-2000-28MP:5# show mld_snooping v3_src_filter state
Command: show mld_snooping v3_src_filter state

mld_snooping v3_src_filter state : Enabled
DGS-2000-28MP:5#
```

27

MULTICAST VLAN COMMANDS

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

Command	Parameter
enable igmp_snooping multicast_vlan	
disable igmp_snooping multicast_vlan	
create igmp_snooping multicast_vlan	<vlan_name 20> <vlanid 2-4094>
config igmp_snooping multicast_vlan	<vlan_name 20> [add | delete] [member_port <portlist> | source_port <portlist> | untag_source_port <portlist> | tag_member_port <portlist>] state [enable | disable] {replace_source_ip [none | <ipaddr>]}
delete igmp_snooping multicast_vlan	[all | <vlan_name 20>]
show igmp_snooping multicast_vlan	{<vlan_name 32>}
config igmp_snooping multicast_vlan_group	<vlan_name 20> [add | delete] ipv4_range <mcastaddr> <mcastaddr>
show igmp_snooping multicast_vlan_group	{<vlan_name 32>}
enable mld_snooping multicast_vlan	
disable mld_snooping multicast_vlan	
create mld_snooping multicast_vlan	<vlan_name 20> <vlanid 2-4094>
config mld_snooping multicast_vlan	<vlan_name 20> {[add | delete] {member_port <portlist> | tag_member_port <portlist> | source_port <portlist>} | state [enable | disable] | replace_source_ipv6 [<ipv6addr> | none]}(1)
delete mld_snooping multicast_vlan	[<vlan_name (20)> | all]
show mld_snooping multicast_vlan	{<vlan_name 20>}
config mld_snooping multicast_vlan_group	<vlan_name 20> [add | delete] ipv6_range <ipv6_mcast_addr> [{<ipv6_mcast_addr>}
show mld_snooping multicast_vlan_group	{<vlan_name 20>}

Each command is listed in detail, as follows:

enable igmp_snooping multicast_vlan

Purpose	To enable IGMP snooping on the Switch.
Syntax	**enable igmp_snooping multicast_vlan**
Description	Multicast VLAN is designed specially for multicast traffic. With proper configuration, multicast traffic can be forwarded across tranditional 802.1Q VLANs.
Parameters	None.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To enable IGMP snooping multicast VLAN feature:

```
DGS-2000-28MP:5# enable igmp_snooping multicast_vlan
Command: enable igmp_snooping multicast_vlan


Success.

DGS-2000-28MP:5#
```

disable igmp_snooping multicast_vlan

Purpose	To disable IGMP snooping on the Switch.
Syntax	**disable igmp_snooping multicast_vlan**
Description	Multicast VLAN is designed specially for multicast traffic. With proper configuration, multicast traffic can be forwarded across tranditional 802.1Q VLANs.
Parameters	None.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To enable IGMP snooping multicast VLAN feature:

```
DGS-2000-28MP:5# disable igmp_snooping multicast_vlan
Command: disable igmp_snooping multicast_vlan


Success.

DGS-2000-28MP: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 32> <vlanid 2-4094>**
Description	The **create igmp_snooping multicast_vlan** command creates an IGMP snooping multicast VLAN on the Switch.

Parameters	<*vlan_name 32*> − The name of the VLAN for which IGMP snooping is to be created. Up to 32 characters can be used. <*vlanid 2-4094*> − 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 a igmp snooping multicast VLAN:

```
DGS-2000-28MP:5# create igmp_snooping multicast_vlan mvln2 5
Command: create igmp_snooping multicast_vlan mvln2 5


Success.
DGS-2000-28MP: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> | source_port <portlist> | untag_source_port <portlist> | tag_member_port <portlist>] state [enable | disable] {replace_source_ip [none | <ipaddr>]}**
Description	The **config igmp_snooping multicast_vlan** command enables IGMP snooping multicast VLAN on the Switch.
Parameters	<*vlan_name 32*> − The name of the VLAN for which IGMP snooping is to be configured. Up to 32 characters can be used. *[add | delete] − Add or delete the specified multicast VLAN of IGMP snooping.* *member_port <portlist>* − Specifies a port or a range of ports to be the member port for the multicast VLAN of IGMP snooping. *source_port <portlist>* − Specifies a port or a range of ports to be the source port for the multicast VLAN of IGMP snooping. *untag_source_port <portlist>* − Specifies a port or a range of ports to be the untage source port for the multicast VLAN of IGMP snooping. *tag_member_port <portlist>* − Specifies a port or a range of ports to be the tagged port for the multicast VLAN of IGMP snooping. *state [enable | disable]* − Enables/Disables IGMP Snooping multicast VLAN. *replace_source_ip [none | <ipaddr>]* – Specifies the replace source IP or none.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure the igmp snooping multicast VLAN:

```
DGS-2000-28MP:5# config igmp_snooping multicast_vlan default state enable
Command: config igmp_snooping multicast_vlan default state enable

Success.
DGS-2000-28MP:5#
```

delete igmp_snooping multicast_vlan

Purpose	To remove an IGMP snooping multicast VLAN on the Switch.
Syntax	**delete igmp_snooping multicast_vlan [all | <vlan_name 32>]**
Description	The **delete igmp_snooping multicast_vlan** command removes IGMP snooping multicast VLAN on the Switch.
Parameters	*all* − Specify all vlans to be removed. *<vlan_name 32>* − Specify the multicast vlan name to be removed on the Switch.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To remove the igmp snooping multicast VLAN 'rd1':

```
DGS-2000-28MP:5# delete igmp_snooping multicast_vlan rd1
Command: delete igmp_snooping multicast_vlan rd1


Success.
DGS-2000-28MP:5#
```

show igmp_snooping multicast_vlan

Purpose	To display the IGMP snooping multicast vlan table entries on the Switch.
Syntax	**show igmp_snooping multicast_vlan {<vlan_name 20>}**
Description	The **show igmp_snooping multicast_vlan** command displays the current IGMP snooping forwarding table entries currently configured on the Switch.
Parameters	*<vlan_name 20>* − The name of the VLAN for which IGMP snooping host table information is to be displayed. Up to 20 characters can be used.
Restrictions	None.

Example usage:

To view the IGMP snooping multicast vlan information on the Switch:

```
DGS-2000-28MP:5# show igmp_snooping multicast_vlan
Command: show igmp_snooping multicast_vlan

Multicast VLAN Global State : Enabled

VLAN Name          : test
VID              : 2
Member Ports       :
Tagged Member Ports :
Source Ports       :
Status           : Enabled
Replace Source IP  :
```

```
DGS-2000-28MP:5#
```

config igmp_snooping multicast_vlan_group

Purpose	To specify MLD multicast address for multicast VLAN.
Syntax	**config igmp_snooping multicast_vlan_group <vlan_name 20> [add | delete] ipv4_range <mcast_addr> <mcast_addr>**
Description	**Multicast_vlan_group** is control list that filtered the multicast traffic NOT in the list.
Parameters	<*vlan_name 32*> − The name of the VLAN for which IGMP snooping is to be configured. Up to 32 characters can be used. *[add* | *delete]* − Specify whether to add or delete ports defined in the following parameter <ipaddr>. <*ipaddr*> − Specify the IP address range to be configured with the IGMP snooping multicast VLAN group.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure the igmp snooping multicast VLAN:

```
DGS-2000-28MP:5# config igmp_snooping multicast_vlan_group test add ipv4_range 239.0.0.100 239.0.0.200
Command: config igmp_snooping multicast_vlan_group test add ipv4_range 239.0.0.100 239.0.0.200


Success.

DGS-2000-28MP:5#
```

show igmp_snooping multicast_vlan_group

Purpose	To display the IGMP snooping multicast vlan group table entries on the Switch.
Syntax	**show igmp_snooping multicast_vlan_group {<vlan_name 32>}**
Description	The **show igmp_snooping multicast_vlan_group** command displays the current IGMP snooping forwarding table entries currently configured on the Switch.
Parameters	<*vlan_name 32*> − The name of the VLAN for which IGMP snooping host table information is to be displayed. Up to 20 characters can be used.
Restrictions	None.

Example usage:

To view the IGMP snooping multicast vlan group information on the Switch:

```
DGS-2000-28MP:5# show igmp_snooping multicast_vlan_group
Command: show igmp_snooping multicast_vlan_group

VLAN Name    VLAN ID    From              To
```

```
------------ --------- ------------------- -------------------
test         2         239.0.0.100         239.0.0.200

DGS-2000-28MP:5#
```

enable mld_snooping multicast_vlan

Purpose	To enable MLD snooping on the Switch.
Syntax	**enable mld_snooping multicast_vlan**
Description	Multicast VLAN is designed specially for multicast traffic. With proper configuration, multicast traffic can be forwarded across tranditional 802.1Q VLANs.
Parameters	None.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To enable MLD snooping multicast VLAN feature:

```
DGS-2000-28MP:5# enable mld_snooping multicast_vlan
Command: enable mld_snooping multicast_vlan


Success.

DGS-2000-28MP:5#
```

disable mld_snooping multicast_vlan

Purpose	To disable MLD snooping on the Switch.
Syntax	**disable mld_snooping multicast_vlan**
Description	Multicast VLAN is designed specially for multicast traffic. With proper configuration, multicast traffic can be forwarded across tranditional 802.1Q VLANs.
Parameters	None.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To enable IGMP snooping multicast VLAN feature:

```
DGS-2000-28MP:5# disable mld_snooping multicast_vlan
Command: disable mld_snooping multicast_vlan


Success.

DGS-2000-28MP:5#
```

create mld_snooping multicast_vlan

Purpose	To create an MLD snooping multicast VLAN on the Switch.
Syntax	**create MLD_snooping multicast_vlan <vlan_name 32> <vlanid 2-4094>**
Description	Multicast VLAN is designed specially for multicast traffic. With proper configuration, multicast traffic can be forwarded across tranditional 802.1Q VLANs.
Parameters	*<vlan_name 32>* − The name of the VLAN for which MLD snooping is to be created. Up to 32 characters can be used. *<vlanid 2-4094>* − The ID of the VLAN for which MLD 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 MLD snooping multicast VLAN:

```
DGS-2000-28MP:5# create mld_snooping multicast_vlan MLD_test 100
Command: create mld_snooping multicast_vlan MLD_test 100


Success.

DGS-2000-28MP:5#
```

config mld_snooping multicast_vlan

Purpose	To configure IGMP snooping multicast VLAN on the Switch.
Syntax	**config mld_snooping multicast_vlan <vlan_name 20> {[add | delete] {member_port <portlist> | tag_member_port <portlist> | source_port <portlist>} | state [enable | disable] | replace_source_ipv6 [<ipv6addr> | none]}**
Description	Multicast VLAN is designed specially for multicast traffic. With proper configuration, multicast traffic can be forwarded across tranditional 802.1Q VLANs.
Parameters	*<vlan_name 20>* − The name of the VLAN for which MLD snooping is to be configured. Up to 32 characters can be used. *[add | delete] − Add or delete the specified multicast VLAN of IGMP snooping.* *member_port <portlist>* − Specifies a port or a range of ports to be the member port for the multicast VLAN of IGMP snooping. *source_port <portlist>* − Specifies a port or a range of ports to be the source port for the multicast VLAN of IGMP snooping. *untag_source_port <portlist>* − Specifies a port or a range of ports to be the untage source port for the multicast VLAN of IGMP snooping. *tag_member_port <portlist>* − Specifies a port or a range of ports to be the tagged port for the multicast VLAN of IGMP snooping. *state [enable | disable]* − Enables/Disables IGMP Snooping multicast VLAN. *replace_source_ip [none* | ipv6add *]* – Specifies the replace source IPv6 ip address or none.

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

Example usage:

To configure the MLD snooping multicast VLAN:

```
DGS-2000-28MP:5# config mld_snooping multicast_vlan MLD_test add source_port 10 member_port 11 state enable
Command: config mld_snooping multicast_vlan MLD_test add source_port 10 member_port 11 state enable

Success.

DGS-2000-28MP:5#
```

delete mld_snooping multicast_vlan

Purpose	To remove an MLD snooping multicast VLAN on the Switch.
Syntax	**delete mld_snooping multicast_vlan [all | <vlan_name 20>]**
Description	Multicast VLAN is designed specially for multicast traffic. With proper configuration, multicast traffic can be forwarded across tranditional 802.1Q VLANs. The **delete mld_snooping multicast_vlan** command removes IGMP snooping multicast VLAN on the Switch.
Parameters	*all* − Specify all vlans to be removed. *<vlan_name 20>* − Specify the multicast vlan name to be removed on the Switch.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To remove the MLD snooping multicast VLAN ‘rd1’:

```
DGS-2000-28MP:5# delete mld_snooping multicast_vlan rd1
Command: delete mld_snooping multicast_vlan rd1

Success.
DGS-2000-28MP:5#
```

show mld_snooping multicast_vlan

Purpose	To display the MLD snooping multicast vlan table entries on the Switch.
Syntax	**show mld_snooping multicast_vlan {<vlan_name 20>}**
Description	Multicast VLAN is designed specially for multicast traffic. With proper configuration, multicast traffic can be forwarded across tranditional 802.1Q VLANs. The **show mld_snooping multicast_vlan** command displays the current IGMP snooping forwarding table entries currently configured on the Switch.
Parameters	*<vlan_name 20>* − The name of the VLAN for which IGMP snooping host table information is to be displayed. Up to 20 characters can be

	used.
Restrictions	None.

Example usage:

To view the MLD snooping multicast vlan information on the Switch:

```
DGS-2000-28MP:5# show mld_snooping multicast_vlan
Command: show mld_snooping multicast_vlan

Multicast VLAN Global State : Enabled

VLAN Name          : MLD_test
VID              : 100
Member Ports       : 11
Tagged Member Ports :
Source Ports       : 10
Status           : Enabled
Replace Source IP  :

DGS-2000-28MP:5#
```

config mld_snooping multicast_vlan_group

Purpose	To specify MLD multicast address for multicast VLAN.
Syntax	**config mld_snooping multicast_vlan_group <vlan_name 20> [add | delete] ipv6_range <ipv6_mcast_addr> [{<ipv6_mcast_addr>}**
Description	**Multicast_vlan_group** is control list that filtered the multicast traffic NOT in the list.
Parameters	<*vlan_name 32*> − The name of the VLAN for which IGMP snooping is to be configured. Up to 32 characters can be used. *[add* | *delete]* − Specify whether to add or delete ports defined in the following parameter <ipaddr>. <*ipaddr*> − Specify the IP address range to be configured with the IGMP snooping multicast VLAN group.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure the MLD snooping multicast group:

```
DGS-2000-28MP:5# config mld_snooping multicast_vlan_group MLD_test add ipv6_range ff04::01 ff04::100
Command: config mld_snooping multicast_vlan_group MLD_test add ipv6_range ff04::01 ff04::100

Success.

DGS-2000-28MP:5#
```

show mld_snooping multicast_vlan_group	
Purpose	To display the MLD snooping multicast vlan group table entries on the Switch.
Syntax	**show mld_snooping multicast_vlan_group {<vlan_name 20>}**
Description	The **show mld_snooping multicast_vlan_group** command displays the current MLD snooping forwarding table entries currently configured on the Switch.
Parameters	*<vlan_name 20>* − The name of the VLAN for which IGMP snooping host table information is to be displayed. Up to 20 characters can be used.
Restrictions	None.

Example usage:

To view the MLD snooping multicast vlan group information:

```
DGS-2000-28MP:5# show mld_snooping multicast_vlan_group
Command: show mld_snooping multicast_vlan_group

VLAN Name     VLAN ID    From                To
------------- ---------  ------------------  ------------------
MLD_test      100        ff04::1             ff04::100

DGS-2000-28MP:5#
```

28

LIMITED IP MULTICAST ADDRESS COMMANDS

The Multicast Filter 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_32>
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 > [ipv4 | ipv6] {[add | delete] [[profile_id <integer 1-24> | profile_name <string 32> | all]] {access [permit | deny]} }
show limited_multicast_addr ports	<portlist > {[ipv4 | ipv6]}
config max_mcast_group ports	<portlist> [ipv4 | ipv6] max_group <integer 1-32>
show max_mcast_group ports	<portlist > {[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	*[ipv4* | *ipv6]* – Specify the IPv4 or IPv6 of multicast filter profile to be created on the Switch. *profile_id <integer 1-24>* - Specify the profile id of multicast filter profile on the Switch. *profile_name string* - Specify the profile name of 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-2000-28MP: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-2000-28MP: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	*profile_id <integer 1-24>* - Specify the profile id to be added or deleted for the multicast filter. *profile_name <string 32>* - The name of the VLAN on which the MAC address resides. *[add | delete]* – Add or delete the profile id which user specified. <*mcast_addr*> – Specify the range of IPv4 address.
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-2000-28MP: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-2000-28MP: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	*profile_id <integer 1-24>* - Specify the profile id to be added or deleted for the multicast filter. *profile_name <string 32>* - The name of the VLAN on which the MAC address resides. *[add | delete]* – Add or delete the profile id which user specified. <*ipv6_mcast_addr*> – Lists the IPv6 multicast addresses to put in

	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-2000-28MP:5# config mcast_filter_profile ipv6 profile_id 4 add FF0E::100:0:0:20 FF0E::100:0:0:22
Command: config mcast_filter_profile ipv6 profile_id 4 add FF0E::100:0:0:20 FF0E::100:0:0:22

Success.
DGS-2000-28MP:5#
```

delete mcast_filter_profile

Purpose	To delete an entry in the Switch's forwarding database.
Syntax	**delete mcast_filter_profile [ipv4 | ipv6] [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	*[ipv4* | *ipv6]* – Specify the IPv4 or IPv6 of multicast filter profile to be removed on the Switch. *profile_id <integer 1-24>* − The profile id of the VLAN on which the multicast forwarding filtering database resides. *profile_name <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-2000-28MP:5# delete mcast_filter_profile ipv4 profile_name rd3
Command: delete mcast_filter_profile ipv4 profile_name rd3

Success.
DGS-2000-28MP:5#
```

show mcast_filter_profile

Purpose	To display multicast filtering settings on the Switch.
Syntax	**show mcast_filter_profile {[ipv4 | ipv6]} {profile_id <integer 1-24> | profile_name <string 32>}**
Description	The **show mcast_filter_profile** command displays the multicast filtering profiles settings.
Parameters	*[ipv4* | *ipv6]* – Specify the IPv4 or IPv6 of multicast filter profile to be displayed on the Switch. *profile_id <integer 1-24>* - Specify the profile id of multicast filter profile to be displayed. *profile_name <string 32>* - Specify the profile name of multicast filter profile to be displayed.

Restrictions	None.

Example usage:

To display all the defined multicast address profiles:

```
DGS-2000-28MP: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-2000-28MP:5#
```

config limited_multicast_addr ports

Purpose	To configure the multicast address filtering function a port.
Syntax	**config limited_multicast_addr ports <portlist > [ipv4 | ipv6] {[add | delete] [[profile_id <integer 1-24> | profile_name <string 32>]] {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	*ports <portlist >* – A port or range of port on which the limited multicast address range to be configured has been assigned. *[ipv4 | ipv6]* – Specify the IPv4 or IPv6 of multicast filter profile to be configured. *add* – Add a multicast address profile to a port. *delete* – Delete a multicast address profile to a port. *profile_id <integer 1-24>* - Allow to select by multicast filter profile ID *profile_name <string 32>* - Allow to select by multicast filter profile name *permit* – Specifies that the packet that matches the addresses defined in the profiles will be permitted. The default mode is permit. *deny* – Specifies that the packet matches the addresses defined in the profiles will be denied.
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-2000-28MP:5# config limited_multicast_addr ports 3 ipv4 add profile_id 1
Command: config limited_multicast_addr ports 3 ipv4 add profile_id 1


Success.
```

```
DGS-2000-28MP: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 > {[ipv4 | ipv6]}**
Description	The **show limited_multicast_addr ports** command is to display the multicast address range by port or by VLAN.
Parameters	*<portlist >* – Used to show the per-port Limited IP multicast address range. *[ipv4 | ipv6]* – 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 3:

```
DGS-2000-28MP:5# show limited_multicast_addr ports 3
Command: show limited_multicast_addr ports 3


Port  : 3
Access: permit

Type  Profile ID     Name                    Multicast Addresses

----- ---------- -------------------------------- --------------------------

v4    1            profile1                239.1.1.10

Port  : 3
Access: permit

Type  Profile ID     Name                    Multicast Addresses

----- ---------- -------------------------------- --------------------------



DGS-2000-28MP:5#
```

config max_mcast_group ports

Purpose	To configure maximum multicast group ports on the Switch.
Syntax	**confg max_mcast_group ports <portlist > [ipv4 | ipv6] max_group <integer 1-32>**
Description	The feature helps to limit the maximum multicast group can be dynamic learned in port basis.

Parameters	<*portlist*> - Specify a port or range of ports to be displayed. *{[ipv4 | ipv6]}* – Specify the IPv4 or IPv6 to be displayed. max_group <*integer 1-32*> - The maximum groups can be learned.
Restrictions	None.

Example usage:

To configure the max IGMP group can be learned in port 10:

```
DGS-2000-28MP:5# config max_mcast_group ports 10 ipv4 max_group 20
Command: config max_mcast_group ports 10 ipv4 max_group 20


Success.

DGS-2000-28MP:5#
```

show max_mcast_group ports

Purpose	To display maximum multicast group ports on the Switch.
Syntax	**show max_mcast_group ports <portlist > {[ipv4 | ipv6]}**
Description	The **show max_mcast_group ports** command displays the multicast filtering profiles settings.
Parameters	<*portlist*> - Specify a port or range of ports to be displayed. *{[ipv4 | ipv6]}* – Specify the IPv4 or IPv6 to be displayed.
Restrictions	None.

Example usage:

To show maximum multicast group port 10:

```
DGS-2000-28MP:5# show max_mcast_group ports 10
Command: show max_mcast_group ports 10

Port        IPv4 MaxMcastGroup      IPv6 MaxMcastGroup
-----       --------------------    --------------------
10          20                      32

DGS-2000-28MP:5#
```

29

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 auth_state	{ports <portlist>}
show 802.1x auth_configuration	{ports <portlist>}
config 802.1x auth_parameter ports	[<portlist> | all] [default | { port_control [force_unauth | auto | force_auth] | quiet_period <sec 0-65535> | tx_period <sec 1-65535> | supp_timeout <sec 1-65535> | server_timeout <sec 1-65535> | max_req <value 1-10> | reauth_period <sec 1-65535> | enable_reauth [enable | disable] | direction [both | in]}]
config 802.1x init	port_based ports [<portlist> | all]
config 802.1x auth_protocol	[radius_eap | local]
config 802.1x reauth	port_based ports [<portlist> | all]
config radius add	<server_index 1-3> [<ipaddr> | <ipv6_addr>] [key <passwd 32>] {default | auth_port <udp_port_number 1-65535> | acct_port <udp_port_number 1-65535> | retransmit <int 1-255> | timeout <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> | <ipv6_addr>] | retransmit <int 1-255> | timeout <int 1-255>}
show radius	
config 802.1x fwd_pdu system	[enable | disable]
show 802.1x fwd_pdu system status	
config 802.1x auth_mode	[port_based | mac_based]
create 802.1x guest vlan	<vlan_name 32>
delete 802.1x guest vlan	<vlan_name 32>
config 802.1x guest_vlan ports	[<portlist> | all] state [enable | disable]
show 802.1x	

Command	Parameter
guest_vlan	
create 802.1x user	<username 15>
show 802.1x user	
delete 802.1x user	<username 15>
config 802.1x capability ports	[<portlist> | 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, operator or power user-level users can issue this command.

Example usage:

To enable 802.1x switch wide:

```
DGS-2000-28MP:5# enable 802.1x
Command: enable 802.1x


Success.
DGS-2000-28MP: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, operator or power user-level users can issue this command.

Example usage:

To disable 802.1x on the Switch:

```
DGS-2000-28MP:5# disable 802.1x
Command: disable 802.1x
```

```
Success.
DGS-2000-28MP: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-2000-28MP:5# show 802.1x
Command: show 802.1x

802.1X                  : Enable
Authentication Mode     : Port_base
Authentication Method   : Local

Success.
DGS-2000-28MP: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>}**
Description	The **show 802.1x auth_state** command displays the current 802.1x authentication state of the specified ports of the Port-based Network Access Control server application on the Switch. The following details are displayed: Port number − Shows the physical port number on the Switch. Auth PAE State: Initialize / Disconnected / Connecting / Authenticating / Authenticated / Held / ForceAuth / ForceUnauth − Shows the current state of the Authenticator PAE. Backend State: Request / Response / Fail / Idle / Initialize / Success / Timeout − Shows the current state of the Backend Authenticator. Port Status: Authorized / Unauthorized − Shows the result of the authentication process. Authorized means that the user was authenticated, and can access the network. Unauthorized means that the user was not authenticated, and cannot access the network.
Parameters	*ports* <*portlist*> − A port or range of ports whose settings are to be displayed.
Restrictions	None.

Example usage:

To display the 802.1x authentication states for port 1~5 (stacking disabled) for Port-based 802.1x:

```
DGS-2000-28MP:5# show 802.1x auth_state ports 1-5
Command: show 802.1x auth_state ports 1-5

Port   Auth PAE State  Backend State   Port Status
------ ---------------------- -------------------- ---------------
1      ForceAuth       Success         Authorized
2      ForceAuth       Success         Authorized
3      ForceAuth       Success         Authorized
4      ForceAuth       Success         Authorized
5      ForceAuth       Success         Authorized
DGS-2000-28MP: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>}**
Description	The **show 802.1x auth_configuration** command displays the current configuration of the 802.1x Port-based Network Access Control server application on the Switch. The following details are displayed: *802.1x:* Enabled/Disabled − Shows the current status of 802.1x functions on the Switch. *Authentication Mode:* Port-based/Mac-based/None − Shows the 802.1x authorization mode. Authentication Method: Remote/none − Shows the type of authentication protocol suite in use between the Switch and a RADIUS server. *Port number :* Shows the physical port number on the Switch. *AdminCrlDir:* Both/In − Shows whether a controlled Port that is unauthorized will exert control over communication in both receiving and transmitting directions, or just the receiving direction. *OpenCrlDir:* Both/In − Shows whether a controlled Port that is unauthorized will exert control over communication in both receiving and transmitting directions, or just the receiving direction. *Port Control:* ForceAuth/ForceUnauth/Auto − Shows the administrative control over the port's authorization status. ForceAuth forces the Authenticator of the port to become Authorized. ForceUnauth forces the port to become Unauthorized. *QuietPeriod :* Shows the time interval between authentication failure and the start of a new authentication attempt. *TxPeriod :* Shows the time to wait for a response from a supplicant (user) to send EAP Request/Identity packets. *SuppTimeout :* Shows the time to wait for a response from a supplicant (user) for all EAP packets, except for the Request/Identity packets. *ServerTimeout :* Shows the length of time to wait for a response from a RADIUS server. *MaxReq :* Shows the maximum number of times to retry sending packets to the supplicant. *ReAuthPeriod :* Shows the time interval between successive

	reauthentications. *ReAuthenticate:* true/false − Shows whether or not to reauthenticate.
Parameters	*ports <portlist>* − Specifies a port or range of ports to be viewed.
Restrictions	None.

Example usage:

To display the 802.1x configurations of port 2:

```
DGS-2000-28MP:5# show 802.1x auth_configuration ports 2
Command: show 802.1x auth_configuration ports 2

Authentication Mode    : Port_base

Port number     : 2
Capability      : none
AdminCrlDir     : Both
OpenCrlDir      : Both
Port Control    : ForceAuthorized
QuietPeriod     : 60    sec
TxPeriod        : 30    sec
SuppTimeout     : 30    sec
ServerTimeout   : 30    sec
MaxReq          : 2     times
ReAuthPeriod    : 3600  sec
ReAuthenticate  : Disable

DGS-2000-28MP: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> | 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	*[<portlist> | all]* – A port, range of ports or all ports to be configured. *all* – Specifies all of the ports on the Switch. *default* – Returns all of the ports in the specified range to their 802.1x default settings. *port_control* – Configures the administrative control over the authentication process for the range of ports. The options are: • *force_auth* – Forces the Authenticator for the port to become authorized. Network access is allowed.

	• *auto* – Allows the port's status to reflect the outcome of the authentication process. • *force_unauth* – Forces the Authenticator for the port to become unauthorized. Network access is blocked. *quiet_period* <*sec 0-65535*> – Configures the time interval between authentication failure and the start of a new authentication attempt. *tx_period* <*sec 1-65535*> - Configures the time to wait for a response from a supplicant (user) to send EAP Request/Identity packets. *supp_timeout* <*sec 1-65535*> - Configures the time to wait for a response from a supplicant (user) for all EAP packets, except for the Request/Identity packets. *server_timeout* <*sec 1-65535*> - Configures the length of time to wait for a response from a RADIUS server. *max_req* <*value 1-10*> – Configures the number of times to retry sending packets to a supplicant (user). *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. Enabled causes 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, operator or power user-level users can issue this command.

Example usage:

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

```
DGS-2000-28MP:5# config 802.1x auth_parameter ports 1-5 direction both
Command: config 802.1x auth_parameter ports 1-5 direction both


Success.
DGS-2000-28MP:5#
```

config 802.1x init

Purpose	To initialize the 802.1x function on a range of ports.
Syntax	**config 802.1x init port_based ports [<portlist> | all]**
Description	The **config 802.1x init** command initializes the 802.1x functions on a specified range of ports or for specified MAC addresses operating from a specified range of ports.
Parameters	*port_based* – Instructs the Switch to initialize 802.1x functions based only on the port number. Ports approved for initialization can then be specified. *ports* <*portlist*> – A port or range of ports to be configured. *all* – Specifies all of the ports on the Switch.

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

Example usage:

To initialize the authentication state machine of all ports:

```
DGS-2000-28MP:5# config 802.1x init port_based ports all
Command: config 802.1x init port_based ports all

Success.
DGS-2000-28MP: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	*radius_eap* – Uses the list of RADIUS EAP servers for authentication. *local* – Uses no authentication.
Restrictions	Only Administrator, operator or power user-level users can issue this command.

Example usage:

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

```
DGS-2000-28MP:5# config 802.1x auth_protocol local
Command: config 802.1x auth_protocol local

Success.
DGS-2000-28MP:5#
```

config 802.1x reauth

Purpose	To configure the 802.1x re-authentication feature of the Switch.
Syntax	**config 802.1x reauth port_based ports [<portlist> | all]**
Description	The **config 802.1x reauth** command re-authenticates a previously authenticated device based on port number.
Parameters	*port_based* – Instructs the Switch to re-authorize 802.1x functions based only on the port number. Ports approved for re-authorization can then be specified. *ports <portlist>* – A port or range of ports to be re-authorized. *all* – Specifies all of the ports on the Switch.
Restrictions	Only Administrator, operator or power user-level users can issue this command.

Example usage:

To configure 802.1x reauthentication for ports 1-18:

```
DGS-2000-28MP:5# config 802.1x reauth port_based ports 1-18
Command: config 802.1x reauth port_based ports 1-18

Success.
DGS-2000-28MP:5#
```

config radius add

Purpose	To configure the settings the Switch uses to communicate with a RADIUS server.
Syntax	**config radius add <server_index 1-3> [<ipaddr> | <ipv6_addr>] [key <passwd 32> | encryption_key <passwd 66>] {default | auth_port <udp_port_number 1-65535> | acct_port <udp_port_number 1-65535> | retransmit <int 1-255> | timeout <int 1-255>}**
Description	The **config radius add** command configures the settings the Switch uses to communicate with a RADIUS server.
Parameters	*<server_index 1-3>* – The index of the RADIUS server. *[<ipaddr>* | *<ipv6_addr]>* – The IPv4 or IPv6 address of the RADIUS server. *[key* | *encryption_key]* – Specifies that a password and encryption key are to be used between the Switch and the RADIUS server. *<passwd 32>* – The shared-secret key used by the RADIUS server and the Switch. Up to 128 characters can be used. *default* – Uses the default udp port number in both the *auth_port* and *acct_port* settings. *auth_port <udp_port_number 1-65535>* – The UDP port number for authentication requests. The default is 1812. *acct_port <udp_port_number 1-65535>* – The UDP port number for accounting requests. The default is 1813. *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. *timeout <int 1-255>* – Specifies the connection timeout. The value may be between 1 and 255 seconds.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure the RADIUS server communication settings:

```
DGS-2000-28MP:5# config radius add 1 3000::2 key 9999 acct_port 10 auth_port
12 retransmit 2 timeout 5
Command: config radius add 1 3000::2 key 9999 acct_port 10 auth_port 12
retransmit 2 timeout 5


Success.
DGS-2000-28MP: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-2000-28MP:5# config radius delete 1
Command: config radius delete 1

Success.
DGS-2000-28MP: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> | <ipv6_addr>] | retransmit <int 1-255> | timeout <int 1-255>}**
Description	The **config radius** command configures the Switch's RADIUS settings.
Parameters	*<server_index 1-3>* – The index of the RADIUS server. *key* – Specifies that a password and encryption key are to be used between the Switch and the RADIUS server. • *<passwd 32>* – The shared-secret key used by the RADIUS server and the Switch. Up to 32 characters can be used. *auth_port <udp_port_number 1-65535>* – The UDP port number for authentication requests. The default is 1812. *acct_port <udp_port_number 1-65535>* – The UDP port number for accounting requests. The default is 1813. *ipaddress [<ipaddr> | <ipv6_addr>]* – The IPv4 or IPv6 address of the RADIUS server. *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. *timeout <int 1-255>* – Specifies the connection timeout. The value may be between 1 and 255 seconds.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure the RADIUS settings:

```
DGS-2000-28MP:5# config radius 1 ipaddress 10.48.47.11
Command: config radius 1 ipaddress 10.48.47.11


Success.
DGS-2000-28MP: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-2000-28MP:5# show radius
Command: show radius

Index  Ip Address      Auth-Port  Acct-Port  Timeout  Retransmit  Key
                                              (secs)
-----  ----------------  ---------  ----------  ---------  ----------  ------
1      10.48.74.121      1812       1813       5          10          dlink

Total Entries : 1


Success.
DGS-2000-28MP:5#
```

config 802.1x fwd_pdu system

Purpose	To configure the 802.1x forwarding EAPOL PDU on the Switch.
Syntax	**config 802.1x fwd_pdu system [enable | disable]**
Description	The **config 802.1x fwd_pdu system** command is used to configure the control of forwarding EAPOL PDUs. Then the 802.1x functionality is disabled, for a port, and if the 802.1x forwarding PDU is enabled both globally and for the port, a received EAPOL packet on the port will be flooded on the same VLAN to those ports of which the 802.1x forwarding PDU is enabled and 802.1x is disabled (globally or just for the port).
Parameters	*[enable | disable]* – Specifies the forwarding of EAPOL PDU is enabled or disabled. The default is disabled.
Restrictions	Only Administrator, operator or power user-level users can issue this command.

Example usage:

To enable 802.1x forwarding EAPOL PDU

```
DGS-2000-28MP:5# config 802.1x fwd_pdu system enable
Command: config 802.1x fwd_pdu system enable


Success.
DGS-2000-28MP:5#
```

show 802.1x fwd_pdu system status

Purpose	To display the 802.1x forwarding EAPOL PDU status on the Switch.
Syntax	**show 802.1x fwd_pdu system status**
Description	The **show 802.1x fwd_pdu system status** command is used to display the control of forwarding EAPOL PDUs.
Parameters	None.
Restrictions	None.

Example usage:

To show 802.1x forwarding EAPOL PDU status:

```
DGS-2000-28MP:5# show 802.1x fwd_pdu system status
Command: show 802.1x fwd_pdu system status

PNAC control packet (eap) is forwarding....

Success.
DGS-2000-28MP: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	*[port_based* | *mac_based]* – Specifies whether 802.1x authentication is by port or MAC address.
Restrictions	Only Administrator, operator or power user-level users can issue this command.

Example usage:

To configure 802.1x authentication by port address:

```
DGS-2000-28MP:5# config 802.1x auth_mode port_based
Command: config 802.1x auth_mode port_based


Success.
DGS-2000-28MP:5#
```

create 802.1x guest_vlan

Purpose	Enables network access to a Guest VLAN.
Syntax	**create 802.1x guest_vlan <vlan_name 32>**
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 32*> − 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-2000-28MP:5# create 802.1x guest_vlan default
Command: create 802.1x guest_vlan default

Success.

DGS-2000-28MP:5#
```

delete 802.1x guest_vlan

Purpose	Disables network access to a Guest VLAN.
Syntax	**delete 802.1x guest_vlan <vlan_name 32>**
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	None.
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-2000-28MP:5# delete 802.1x guest_vlan default
Command: delete 802.1x guest_vlan default

Success.

DGS-2000-28MP: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> | 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 be configured to provide limited network access to authorized member ports. If a member port is denied network access via port–based authorization, but the 802.1x Guest VLAN is enabled, the member port receives limited network access. For example, a network administrator can use the 802.1x Guest VLAN to deny internal network access via port–based authentication, but grant Internet access to unauthorized users.
Parameters	*<portlist>* – A port or range of ports to be configured to the Guest VLAN. *All* – Indicates all ports to be configured to the guest vlan. *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-2000-28MP:5# config 802.1x guest_vlan ports 1-5 state enable
Command: config 802.1x guest_vlan ports 1-5 state enable

Success.

DGS-2000-28MP: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-2000-28MP: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-2000-28MP: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, operator or power user-level users can issue this command.

Example usage:

To create a 802.1x user:

```
DGS-2000-28MP: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-2000-28MP:5#
```

show 802.1x user

Purpose	Displays the user information for the Guest VLAN.
Syntax	**show 802.1x user**
Description	The **show 802.1x user** command displays the 802.1x user information on the Switch.
Parameters	None.
Restrictions	Only Administrator, operator or power user-level users can issue this command.

Example usage:

To display the 802.1x user information:

```
DGS-2000-28MP:5# show 802.1x user
Command: show 802.1x user

Index       Username
----------  ---------------
  1         dlink

Total Entries: 1

Success.
DGS-2000-28MP:5#
```

delete 802.1x user

Purpose	Deletes network access to a 802.1x user.
Syntax	**delete 802.1x user <username 15>**
Description	The **delete 802.1x user** command deletes network access to a 802.1x user.
Parameters	*<username 15>* − The name of the 802.1x user to be deleted.
Restrictions	Only Administrator, operator or power user-level users can issue this command.

Example usage:

To delete the 802.1x user:

```
DGS-2000-28MP:5# delete 802.1x user dlink
Command: delete 802.1x user dlink


Success.
DGS-2000-28MP:5#
```

config 802.1x capability ports

Purpose	Defines a port or range of ports to be members of the Guest VLAN.
Syntax	**config 802.1x capability ports [<portlist> | all] [authenticator | none]**
Description	Th **config 802.1x capability ports** is used to configure the capability for the 802.1x on the Switch.
Parameters	*<portlist>* – 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, operator or power user-level users can issue this command.

Example usage:

To configure capability ports to the 802.1x on the Switch:

```
DGS-2000-28MP:5# config 802.1x capability ports all authenticator
Command: config 802.1x capability ports all authenticator


Success.
DGS-2000-28MP:5#
```

30

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> | all] [admin_state [enable | disable] | max_learning_addr <max_lock_no 0-128> | lock_address_mode [Permanent | DeleteOnTimeout | DeleteOnReset]
show port_security	{ports <portlist>}
delete port_security_entry	[vlan <vlan_name 32> | vlanid <vlanid 1-4094>] mac_address <macaddr>
clear port_security_entry	[all | port <portlist>]

Each command is listed in detail, as follows:

config port_security

Purpose	To configure port security settings.
Syntax	**config port_security [<portlist> | all] [admin_state [enable | disable] | max_learning_addr <max_lock_no 0-128> | lock_address_mode [Permanent | DeleteOnTimeout | DeleteOnReset]**
Description	The **config port_security** command configures port security settings for specific ports.
Parameters	*<portlist>* – A port or range of ports to be configured. *all* – Configures port security for all ports on the Switch. *admin_state [enable | disable]* – Enables or disables port security for the listed ports. *max_learning_addr <int 0-128>* - Specify the max learning address. The range is 0 to 128. 1-128 Limits the number of MAC addresses dynamically listed in the FDB for the ports. *lock_address_mode – Defines the TBD and contains the following options:* • *Permenant – Learns up to the maximum number of dynamic addresses allowed on the port. The learned addresses are not aged out or relearned on other port for as long as the port is locked.* • *DeleteOnReset – Deletes the current dynamic MAC addresses associated with the port. Learn up to the maximum addresses allowed on the port (this number is also configurable). Aging is disabled; the addresses are deleted on reset* • *DeleteOnTimeout – Deletes the current dynamic MAC addresses associated with the port. The port learns up to*

	the maximum addresses allowed on the port. Re-learned MAC addresses and address aging out are also enabled. The MAC addresses are deleted when the device is reset and on when the address is aged out.
Restrictions	Only administrator or operator-level users can issue this command

Example usage:

To configure port security:

```
DGS-2000-28MP: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-2000-28MP:5#
```

show port_security

Purpose	To display the current port security configuration.
Syntax	**show port_security {ports <portlist>}**
Description	The **show port_security** command displays port security information for the Switch's ports. The information displayed incluDGS port security, admin state, maximum number of learning address and lock mode and trap interval.
Parameters	*ports* <*portlist*> – A port or range of ports whose settings are to be displayed.
Restrictions	None.

Example usage:

To display the port security configuration:

```
DGS-2000-28MP: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-2000-28MP:5#
```

delete port_security _entry	
Purpose	To delete a port security entry by VLAN, VLAN ID, and MAC address.
Syntax	**delete port_security_entry [vlan <vlan_name 32> | vlanid <vlanid 1-4094>] mac_address <macaddr>**
Description	The **delete port_security_entry** command is used to delete a port security entry by VLAN, VLAN ID, and MAC address.
Parameters	*<vlan_name 32>* – Specifies the VLAN name. *<vlanid 1-4094>* - Specifies the VLAN ID. *<macaddr>* - Specifies the MAC address.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To delete the port security entry with a MAC address of 00-01-30-10-2c-c7 on the default VLAN:

```
DGS-2000-28MP:5# delete port_security_entry vlan default mac_address 00-01-30-10-2C-C7
Command: delete port_security_entry vlan default mac_address 00-01-30-10-2C-C7

Success.
DGS-2000-28MP:5#
```

clear port_security _entry	
Purpose	To clear the MAC entries learned by the port security function.
Syntax	**clear port_security_entry [all | port <portlist>]**
Description	The **clear port_security_entry** command is used to clear the MAC entries learned by the port security function.
Parameters	*[all | port <portlist>]* – Specify all ports or a list of port for MAC entries to be cleared.
Restrictions	Only administrator or operator-level users can issue this command

Example usage:

To clear all port security entries:

```
DGS-2000-28MP:5# clear port_security_entry all
Command: clear port_security_entry all

Success.

DGS-2000-28MP:5#
```

31

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
enable sntp	
disable sntp	
config sntp	{primary [<ipaddr> | <ipv6addr>] | secondary [<ipaddr> | <ipv6addr>] | poll-interval <sec 30-99999>}
show sntp	
config time	<date> <systime>
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:

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-2000-28MP:5# enable sntp
Command: enable sntp

Success.
DGS-2000-28MP: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-2000-28MP:5# disable sntp
Command: disable sntp

Success.
DGS-2000-28MP:5#
```

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	*primary [<ipaddr>| <ipv6addr>]* – Specifies the IPv4 or IPv6 address of the primary SNTP server. *secondary [<ipaddr>| <ipv6addr>]* – Specifies the IPv4 or IPv6 address of the secondary SNTP server. *poll-interval <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).
Restrictions	Only administrator or operate-level users can issue this command. SNTP service must be enabled for this command to function (enable sntp).

Example usage:

To configure SNTP settings:

```
DGS-2000-28MP: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-2000-28MP: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-2000-28MP: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-2000-28MP:5#
```

config time

Purpose	To manually configure system time and date settings.
Syntax	**config time <date> <systime>**
Description	The **config time date** command configures the system time and date settings. These will be overridden if SNTP is configured and enabled.
Parameters	<*date*> –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. <*systime* > – Specifies the system time, using the format hh:mm:ss; that is, two numerical characters each for the hour using a 24-hour clock, the minute and second. For example: 19:42:30.
Restrictions	Only administrator or operate-level users can issue this command. Manually configured system time and date settings are overridden if SNTP support is enabled.

Example usage:

To manually set system time and date settings:

```
DGS-2000-28MP:5# config time 09jan2012 15:50:50
Command: config time 09jan2012 15:50:50

Success.
DGS-2000-28MP: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	*operator* – May be (+) to add or (-) to subtract time to adjust for time zone relative to GMT. *hour <gmt_hour 0-13>* – Specifies the number of hours difference from GMT. *minute <minute 0-59>* – Specifies the number of minutes added or subtracted to adjust the time zone.
Restrictions	Only administrator or operator level users can issue this command.

Example usage:

To configure time zone settings:

```
DGS-2000-28MP:5# config time_zone operator + hour 2 minute 30
Command: config time_zone operator + hour 2 minute 30

Success.
DGS-2000-28MP:5#
```

config dst

Purpose	To configure time adjustments to allow for the use of Daylight Saving Time (DST).
Syntax	**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]]]**
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	*disable* – Disables the DST seasonal time adjustment for the Switch. *annual* – Enables DST seasonal time adjustment on an annual basis. Annual mode requires that the DST beginning and ending date be specified concisely. For example, specify to begin DST on April 3 and end DST on October 14. The format for annual mode is as follows, and in the order listed: • *s_date <start_date 1-31>* - The day of the month to begin DST, expressed numerically**.** • *s_mth <start_mth 1-12>* - The month of the year to begin DST, expressed numerically. • *s_time <start_time>* - The time of day to begin DST in hours and minutes, expressed using a 24-hour clock. • *end_date <int 1-31>* - The day of the month to end DST, expressed numerically**.** • *e_mth <end_mth 1-12>* - The month of the year to end DST, expressed numerically. • *e_time<end_time>* - The time of day to end DST, in hours and minutes, expressed using a 24-hour clock. *offset [30 | 60 | 90 | 120]* – Indicates the number of minutes to add during the summertime. The possible offset times are 30, 60, 90,

	and 120. The default value is 60.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure daylight savings time on the Switch to run from the 2nd Tuesday in April at 3 PM until the 2nd Wednesday in October at 3:30 PM and add 30 minutes at the onset of DST:

```
DGS-2000-28MP: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-2000-28MP: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 cuurently set on the Switch's System clock:

```
DGS-2000-28MP: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-2000-28MP:5#
```

32

ARP COMMANDS

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

Command	Parameter
create arpentry	<ipaddr> <macaddr>
config arpentry	<ipaddr> <macaddr>
delete arpentry	[<ipaddr> | all]
show arpentry	{information | interface_name {system} | ip_address <ipaddr> | mac_address <macaddr> | summary | static }
clear arptable	{[static | dynamic | all]}
config arp_aging time	<value 0-65535 >
show arpentry aging_time	

Each command is listed in detail, as follows:

create arpentry	
Purpose	To create an entry for ARP table on the Switch.
Syntax	**create arpentry <ipaddr> <macaddr>**
Description	The **create arpentry <ipaddr> <macaddr>** command is used to create an entry for ARP table on the Switch.
Parameters	*<ipaddr>* – Specify the IP address to be configured. *<macaddr>* – Specify the MAC address to be configured.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To create an ARP entry:

```
DGS-2000-28MP:5# create arpentry 10.90.90.94 00-00-00-01-02-03
Command: create arpentry 10.90.90.94 00-00-00-01-02-03


Success.

DGS-2000-28MP:5#
```

config arpentry	
Purpose	To configure the entry for ARP table on the Switch.
Syntax	**config arpentry <ipaddr> <macaddr>**

Description	The **config arpentry** command is used to configure the entry for ARP table on the Switch.
Parameters	*<ipaddr>* – Specify the IP address to be configured. *<macaddr>* – Specify the MAC address to be configured.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure ARP entry:

```
DGS-2000-28MP:5# config arpentry 10.90.90.94 00-00-00-01-02-05
Command: config arpentry 10.90.90.94 00-00-00-01-02-05


Success.

DGS-2000-28MP:5#
```

delete arpentry

Purpose	To remove the entry for ARP table on the Switch.
Syntax	**delete arpentry [<ipaddr> | all]**
Description	The **delete arp_aging time** command is used to configure the entry for ARP table on the Switch.
Parameters	*[<ipaddr> | all]* – Specifiy the IP address or all of ARP entry to be removed.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To remove the ARP entry:

```
DGS-2000-28MP:5# delete arpentry 10.90.90.94
Command: delete arpentry 10.90.90.94


Success.

DGS-2000-28MP: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	*interface_name {system}* – Displays the interface name of ARP entry. *ip_address <ipaddr>* – Displays the IP address of ARP entry.
Restrictions	None.

Example usage:

To display all ARP entries on the Switch:

```
DGS-2000-28MP: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-2000-28MP:5#
```

clear arptable

Purpose	To remove all dynamic ARP table entries.
Syntax	clear arptable
Description	The clear arptable command is used to remove dynamic ARP table entries from the Switch's ARP table. Static ARP table entries are not affected.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To remove dynamic entries in the ARP table:

```
DGS-2000-28MP:5# clear arptable
Command: clear arptable

Success.

DGS-2000-28MP:5#
```

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	*<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-2000-28MP:5# config arp_aging time 30
Command: config arp_aging time 30

Success.

DGS-2000-28MP:5#
```

show arpentry aging_time

Purpose	To displays the ARP entry aging time on the Switch.
Syntax	**show arpentry aging_time**
Description	The **show arpentry aging_time** command displays the ARP entry aging time on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display the ARP entry aging time on the Switch:

```
DGS-2000-28MP:5# show arpentry aging_time
Command: show arpentry aging_time

ARP Aging Time = 30 (minutes)

DGS-2000-28MP:5#
```

33

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
?	
config command_history	<value (1-40)>
show command_history	

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-2000-28MP:5# ?
Command: ?


USEREXEC commands :
?
cable diagnostic port
clear
clear address_binding dhcp_snoop binding_entry ports
clear arptable
clear counters
clear ethernet_oam ports
clear fdb
clear flood_fdb
clear igmp_snooping data_driven_group
clear igmp_snooping statistics counter
clear log
clear mld_snooping statistics counter
clear port_security_entry port
clear tech support
compute dlink-SHA1
config 802.1p default_priority
config 802.1x auth_mode
config 802.1x auth_parameter ports
config 802.1x auth_protocol
config 802.1x capability ports
config 802.1x fwd_pdu system
config 802.1x guest_vlan ports
config 802.1x init port_based ports
config 802.1x radius_acct state
config 802.1x reauth port_based ports
config 802.1x user
config EEE port
config access_profile profile_id
config account
config address_binding auto_scan from_ip
config address_binding dhcp_snoop max_entry ports
config address_binding ip_mac ports
config admin local_enable
config arp_aging time
config arpentry
config authen application
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a ALL
```

config command_history	
Purpose	To limit the entries of command shown in command history.
Syntax	**config command_history <value 1-40>**
Description	The **config command_history** command limits the maximum commands record.
Parameters	<*value 1-40*>: The number entries
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To display the command history:

```
DGS-2000-28MP:5# config command_history 2
Command: config command_history 2

Success.
```

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-2000-28MP:5# show command_history
Command: show command_history


show command_history
config command_history 20
```

34

ACCESS CONTROL LIST COMMANDS

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

Command	Parameter
create access_profile ethernet	{vlan | source_mac <macmask> | destination_mac <macmask> | ethernet_type | 802.1p} profile_id <value 1-150>
config access_profile profile_id	<value 1-150> add access_id [<value 1-200> | auto_assign] **ethernet** {vlan <vlanid 1-4094> | source_mac <macaddr> mask <macmask> | destination_mac <macaddr> mask <macmask> | ethernet_type <hex 0x0-0xffff> | 802.1p <value 0-7>} port [<portlist> | all] [permit {[replace_dscp_with <value 0-63> | rx_rate [<value 16-1000000> | no_limit] | replace_priority_with <value (0-7)> | mirror]} | deny]
create access_profile ip	{ source_ip_mask <netmask> | destination_ip_mask <netmask> | [dscp | tos] |[icmp {{type | code}(1)} | igmp {type} | tcp {{src_port_mask <hex_mask 0x8000-0xffff> | dst_port_mask <hex_mask 0x8000-0xffff> | flag_mask}(1)} | udp {{src_port_mask <hex_mask 0x8000-0xffff> | dst_port_mask <hex_mask 0x8000-0xffff>}(1)} | protocol_id_mask <hex_mask 0x80-0xff>]}(1) profile_id <value 1-150>
config access_profile profile_id	<value 1-150> add access_id [<value 1-200> | auto_assign] **ip** { source_ip <ipaddr> | destination_ip <ipaddr>] | {dscp <value 0-63> | tos <value 0-7>}] | [{icmp {type <value 0-255> | code <value 0-255>}(1)} | {igmp type <value 0-255>} | {tcp {src_port <value 0-65535> | dst_port <value 0-65535> | urg | ack | psh | rst | syn | fin}(1)} | {udp {src_port <value 0-65535> | dst_port <value 0-65535>}(1)} | protocol_id <value 0-255>] }(1) port [<portlist> | all] [permit {[replace_dscp_with <value 0-63> | rx_rate [<value 16-1000000> | no_limit] | replace_priority_with <value 0-7> | mirror]} | deny]
create access_profile ipv6	{ class | source_ipv6_mask <ipv6mask> | destination_ipv6_mask <ipv6mask> |[icmp {{type | code}(1)} | tcp {{src_port_mask <hex_mask 0x8000-0xffff> | dst_port_mask <hex_mask 0x8000-0xffff> | flag_mask}(1)} | udp {{src_port_mask <hex_mask 0x8000-0xffff> | dst_port_mask <hex_mask 0x8000-0xffff>}(1)}]}(1) profile_id <value 1-150>
config access_profile profile_id	<value 1-150> add access_id [<value 1-200> | auto_assign] **ipv6** { class <value 0-255> | source_ipv6 <ipv6addr> | destination_ipv6 <ipv6addr> | [icmp {{type <value 0-255> | code <value 0-255>}(1)} | tcp {{src_port <value 0-65535> | dst_port <value 0-65535> | urg | ack | psh | rst | syn | fin}(1)} | udp {{src_port <value 0-65535> | dst_port <value 0-65535>}(1)}] }(1) port [<portlist> | all] [permit {[replace_dscp_with <value 0-63> | rx_rate [<value 16-1000000> | no_limit] | replace_priority_with <value 0-7> | mirror]} | deny]
create access_profile packet_content_mask	([offset1 <value (0-31)> <hex (0x0-0xffffffff)>] [offset2 <value (0-31)> <hex (0x0-0xffffffff)>] [offset3 <value (0-31)> <hex (0x0-0xffffffff)>] [offset4 <value (0-31)> <hex (0x0-0xffffffff)>]) profile_id <value (1-150)>
config access_profile profile_id	<value (1-150)> add access_id {<value (1-200)> | auto_assign} **packet_content** ([offset_chunk_1 <hex (0x0-0xffffffff)>] [offset_chunk_1_mask <hex (0x0-0xffffffff)>] [offset_chunk_2 <hex (0x0-0xffffffff)>] [offset_chunk_2_mask <hex

Command	Parameter
	(0x0-0xffffffff)>] [offset_chunk_3 <hex (0x0-0xffffffff)>] [offset_chunk_3_mask <hex (0x0-0xffffffff)>] [offset_chunk_4 <hex (0x0-0xffffffff)>] [offset_chunk_4_mask <hex (0x0-0xffffffff)>]) port {<portlist> | all} {permit [{replace_dscp_with <value (0-63)> | rx_rate {<value (16-1000000)> | no_limit} | replace_priority_with <value (0-7)> | mirror}] | deny}
delete access_profile	[profile_id <value 1-150> | all]
config access_profile profile_id	<value 1-150> delete access_id <value 1-200>
show access_profile	{profile_id <value 1-150>}
create cpu_access_profile ethernet	{vlan | source_mac <macmask> | destination_mac <macmask> | ethernet_type | 802.1p}(1) profile_id <value 1-3>
config cpu_access_profile profile_id	<value 1-3> add access_id [<value 1-10> | auto_assign] **ethernet** {vlan <vlanid 1-4094> | source_mac <macaddr> | destination_mac <macaddr> | ethernet_type <hex 0x0-0xffff> | 802.1p <value 0-7>}(1) port [<portlist> | all] [permit | deny]
create cpu_access_profile ip	{ source_ip_mask <netmask> | destination_ip_mask <netmask> | dscp |[icmp {{type | code}(1)} | igmp {type} | tcp {{src_port_mask <hex_mask 0x8000-0xffff> | dst_port_mask <hex_mask 0x8000-0xffff> | flag_mask}(1)} | udp {{src_port_mask <hex_mask 0x8000-0xffff> | dst_port_mask <hex_mask 0x8000-0xffff>}(1)} | protocol_id_mask <hex_mask 0x0-0xff>] }(1) profile_id <value 1-3>
config cpu_access_profile profile_id	<value 1-3> add access_id [<value 1-10> | auto_assign] **ip** { source_ip <ipaddr> | destination_ip <ipaddr> | dscp <value 0-63> | [icmp {{type <value 0-255> | code <value 0-255>}(1)} | igmp {type <value 0-255>} | tcp {{src_port <value 0-65535> | dst_port <value 0-65535> | urg | ack | psh | rst | syn | fin}(1)} | udp {{src_port <value 0-65535> | dst_port <value 0-65535>}(1)} | protocol_id <value 0-255>] }(1) port [<portlist> | all] [permit | deny]
create cpu_access_profile ipv6	{ class | source_ipv6_mask <ipv6mask> | destination_ipv6_mask <ipv6mask> }(1) profile_id <value 1-3>
config cpu_access_profile profile_id	<value 1-3> add access_id [<value 1-10> | auto_assign] ipv6 { class <value 0-255> | source_ipv6 <ipv6addr> | destination_ipv6 <ipv6addr> }(1) port [<portlist> | all] [permit | deny]
create cpu_access_profile packet_content	([offset_0-15 <hex (0x0-0xffffffff)> <hex (0x0-0xffffffff)> <hex (0x0-0xffffffff)> <hex (0x0-0xffffffff)>] [offset_16-31 <hex (0x0-0xffffffff)> <hex (0x0-0xffffffff)> <hex (0x0-0xffffffff)> <hex (0x0-0xffffffff)>] [offset_32-47 <hex (0x0-0xffffffff)> <hex (0x0-0xffffffff)> <hex (0x0-0xffffffff)> <hex (0x0-0xffffffff)>] [offset_48-63 <hex (0x0-0xffffffff)> <hex (0x0-0xffffffff)> <hex (0x0-0xffffffff)> <hex (0x0-0xffffffff)>] [offset_64-79 <hex (0x0-0xffffffff)> <hex (0x0-0xffffffff)> <hex (0x0-0xffffffff)> <hex (0x0-0xffffffff)>]) profile_id <value (1-3)>
config cpu_access_profile profile_id	<value (1-3)> add access_id {<value (1-5)> | auto_assign} packet_content ([offset_0-15 <hex (0x0-0xffffffff)> <hex (0x0-0xffffffff)> <hex (0x0-0xffffffff)> <hex (0x0-0xffffffff)>] [offset_16-31 <hex (0x0-0xffffffff)> <hex (0x0-0xffffffff)> <hex (0x0-0xffffffff)> <hex (0x0-0xffffffff)>] [offset_32-47 <hex (0x0-0xffffffff)> <hex (0x0-0xffffffff)> <hex (0x0-0xffffffff)> <hex (0x0-0xffffffff)>] [offset_48-63 <hex (0x0-0xffffffff)> <hex (0x0-0xffffffff)> <hex (0x0-0xffffffff)> <hex (0x0-0xffffffff)>] [offset_64-79 <hex (0x0-0xffffffff)> <hex (0x0-0xffffffff)> <hex (0x0-0xffffffff)> <hex (0x0-0xffffffff)>]) port {<portlist> | all} {permit | deny}
delete cpu access_profile	profile_id <value 1-3>

Command	Parameter
config cpu_access_profile profile_id	<value 1-3> delete access_id <value 1-10>
show cpu access_profile	{profile_id <value 1-3>}

Each command is listed in detail, as follows:

create access_profile ethernet	
Purpose	To create an access profile on the Switch by examining the Ethernet part of the packet header. Masks entered are combined with the values the Switch finds in the specified frame header fields. Specific values for the rules are entered using the **config access_profile** command, below.
Syntax	**create access_profile ehernet {vlan | source_mac <macmask> | destination_mac <macmask> | ethernet_type | 802.1p} profile_id <value 1-150>**
Description	The **create access_profile** command creates a profile for packets that may be accepted or denied by the Switch by examining the Ethernet part of the packet header. Specific values for rules pertaining to the Ethernet part of the packet header may be defined by configuring the **config access_profile** command for Ethernet, as stated below.
Parameters	*ethernet* - Specifies that the Switch examines the layer 2 part of each packet header with emphasis on one or more of the following: • *vlan* – Specifies that the Switch examine the VLAN part of each packet header. • *source_mac <macmask>* – Specifies a MAC address mask for the source MAC address. This mask is entered in the following hexadecimal format: 000000000000-FFFFFFFFFFFF. • *destination_mac <macmask>* – Specifies a MAC address mask for the destination MAC address in the following format: 000000000000-FFFFFFFFFFFF. • *802.1p* – Specifies that the Switch examine the 802.1p priority value in the frame's header. • *ethernet_type* – Specifies that the Switch examine the Ethernet type value in each frame's header. *profile_id <value 1-150>* – Specifies an index number between 1 and 150 that identifies the access profile being created with this command. The maximum entries for profile ID is 150.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To configure a rule for the Ethernet access profile:

```
Command: create access_profile ethernet source_mac fffffffffffff profile_id 1
```

```
Success.

DGS-2000-28MP:5#
```

config access_profile

Purpose	To create an access profile on the Switch by examining the Ethernet part of the packet header. Masks entered are combined with the values the Switch finds in the specified frame header fields. Specific values for the rules are entered using the **config access_profile** command, below.
Syntax	**config access_profile profile_id <value 1-150> add access_id [<value 1-200> | auto_assign] ethernet {vlan <vlanid 1-4094> | source_mac <macaddr> mask <macmask> | destination_mac <macaddr> mask <macmask> | ethernet_type <hex 0x0-0xffff> | 802.1p <value 0-7>} port [<portlist> | all] [permit {[replace_dscp_with <value 0-63> | rx_rate [<value 16-1000000> | no_limit] | replace_priority_with <value (0-7)> | mirror]} | deny]**
Description	The **config access_profile ethernet** command defines the rules used by the Switch to either filter or forward packets based on the Ethernet part of each packet header.
Parameters	*profile_id <value 1-150>* – Specifies the access profile id to be configured with this command. This value is assigned to the access profile when it is created with the **create access_profile** command. The lower the profile ID, the higher the priority the rule will be given. *[add | delete] access_id <value 1-200>* – Adds or deletes an additional rule to the above specified access profile. The value specifies the relative priority of the additional rule. The entire system is capble for up to 200 access rules. • *auto_assign* – Configures the Switch to automatically assign a numerical value (between 1 and 128) for the rule being configured. *ethernet* – Specifies that the Switch examine only the layer 2 part of each packet to determine if it is to be filtered or forwarded based on one or more of the following: • *vlan <vlanid 1-4094>* – Specifies that the access profile applies only to this previously created VLAN. • *source_mac <macaddr>* – Specifies that the access profile applies only to packets with this source MAC address. MAC address entries may be made in the following format: 000000000000-FFFFFFFFFFFF. • *destination_mac <macaddr>* – Specifies that the access profile applies only to packets with this destination MAC address. MAC address entries may be made in the following format: 000000000000-FFFFFFFFFFFF • *802.1p <value 0-7>* – Specifies that the access profile applies only to packets with this 802.1p priority value. • *ethernet_type <hex 0x05dd-0xffff>* – Specifies that the access profile applies only to packets with this hexadecimal 802.1Q Ethernet type value in the packet header. *ports <portlist>* - The access profile for Ethernet may be defined for each port on the Switch.

	• *mirror* – Specifies the action to mirror before being forwarded by the Switch. • *replace_dscp_with <value 0-63>* – Specifies a value to be written to the DSCP field of an incoming packet that meets the criteria specified in the first part of the command. This value will over-write the value in the DSCP field of the packet. • *rx_rate <value 64-1024000>* – Specifies the rate limit to limit Rx bandwidth for for the profile being configured. This rate is implemented using the following equation – 1 value = 64kbit/sec. (ex. If the user selects a rx rate limit of 10 then the ingress rate is 640kbit/sec.) The user many select a value between 64- 1024000 or no limit. The default setting is no limit. *deny* – Specifies that packets that do not match the access profile are not permitted to be forwarded by the Switch and will be filtered.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To configure a rule for the Ethernet access profile:

```
DGS-2000-28MP:5# config access_profile profile_id 1 add access_id auto_assign
ethernet source_mac 02:03:04:05:06:07 port 3 deny
Command: config access_profile profile_id 1 add access_id auto_assign ethernet s
ource_mac 02:03:04:05:06:07 port 3 deny

Success.

DGS-2000-28MP:5#
```

create access_profile ip

Purpose	To create an access profile on the Switch by examining the Ethernet part of the packet header. Masks entered are combined with the values the Switch finds in the specified frame header fields. Specific values for the rules are entered using the **config access_profile** command, below.
Syntax	**create access_profile { source_ip_mask <netmask> | destination_ip_mask <netmask> | [dscp | tos] |[icmp {{type | code}} | igmp {type} | tcp {{src_port_mask <hex_mask 0x8000-0xffff> | dst_port_mask <hex_mask 0x8000-0xffff> | flag_mask}} | udp {{src_port_mask <hex_mask 0x8000-0xffff> | dst_port_mask <hex_mask 0x8000-0xffff>}} | protocol_id_mask <hex_mask 0x80-0xff>]} profile_id <value 1-150>**
Description	The **create access_profile** command creates a profile for packets that may be accepted or denied by the Switch by examining the Ethernet part of the packet header. Specific values for rules pertaining to the Ethernet part of the packet header may be defined by configuring the **config access_profile** command for Ethernet, as stated below.
Parameters	*ip* - Specifies that the Switch examines the IP fields in each packet

	with special emphasis on one or more of the following: *icmp* – Specifies that the Switch examines the Protocol field in each frame's IP header , and that the value must be 1 (Internet Control Message Protocol- ICMP) for the action to take place. • *type* – Specifies that the Switch examines each frame's ICMP Type field. • *code* – Specifies that the Switch examines each frame's ICMP Code field. *igmp* – Specifies that the Switch examine each frame's protocol field and it must be 2 (Internet Group Management Protocol- IGMP) for the action to take place. • *type* – Specifies that the Switch examine each frame's IGMP Type field. *tcp* – Specifies that the Switch examines each frames protocol field and its value must be 6 (Transmission Control Protocol- TCP) for the action to take place. • *src_port_mask <hex 0x0-0xffff>* – Specifies a TCP port mask for the source port. • *dst_port_mask <hex 0x0-0xffff>* – Specifies a TCP port mask for the destination port. • *flag_mask* – Specifies the appropriate flag_mask parameter. *udp* – Specifies that the Switch examines each frame's protocol field and it's value must be 17 (User Datagram Protocol-UDP) in order for the action to take place.. • *src_port_mask <hex 0x0-0xffff>* – Specifies a UDP port mask for the source port. • *dst_port_mask <hex 0x0-0xffff>* – Specifies a UDP port mask for the destination port. • *flag_mask* – Specifies the appropriate flag_mask parameter. *protocol_id_mask*– Specifies that the Switch examines each frame's protocol field. • *hex_mask <0x80-0xff>* – Specifies a IP protocol mask for the source port. *profile_id <value 1-150>* – Specifies an index number between 1 and 150 that identifies the access profile being created with this command. The maximum entries for profile ID is 150.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To configure a rule for the IP access profile:

```
DGS-2000-28MP:5# create access_profile ip source_ip_mask 255.255.255.255 profile_id 2
Command: create access_profile ip source_ip_mask 255.255.255.255 profile_id 2


Success.

DGS-2000-28MP:5#
```

config access_profile

Purpose	To create an access profile on the Switch by examining the Ethernet part of the packet header. Masks entered are combined with the values the Switch finds in the specified frame header fields. Specific values for the rules are entered using the **config access_profile** command, below.
Syntax	**config access_profile profile_id <value 1-150> add access_id [<value 1-200> | auto_assign] ip { source_ip <ipaddr> | destination_ip <ipaddr>] | {dscp <value 0-63> | tos <value 0-7>}] | [{icmp {type <value 0-255> | code <value 0-255>}(1)} | {igmp type <value 0-255>} | {tcp {src_port <value 0-65535> | dst_port <value 0-65535> | urg | ack | psh | rst | syn | fin}(1)} | {udp {src_port <value 0-65535> | dst_port <value 0-65535>}(1)} | protocol_id <value 0-255>] }(1) port [<portlist> | all] [permit {[replace_dscp_with <value 0-63> | rx_rate [<value 16-1000000> | no_limit] | replace_priority_with <value 0-7> | mirror]} | deny]**
Description	The **config access_profile ethernet** command defines the rules used by the Switch to either filter or forward packets based on the Ethernet part of each packet header.
Parameters	*profile_id <value 1-50>* – Specifies the access profile id to be configured with this command. This value is assigned to the access profile when it is created with the **create access_profile** command. The lower the profile ID, the higher the priority the rule will be given. *[add | delete] access_id <value 1-150>* – Adds or deletes an additional rule to the above specified access profile. The value specifies the relative priority of the additional rule. Up to 65535 rules may be configured for the Ethernet access profile. • *auto_assign* – Configures the Switch to automatically assign a numerical value (between 1 and 128) for the rule being configured. *ip* – Specifies that the Switch examine the IP fields in each packet to determine if it will be either forwarded or filtered based on one or more of the following: • *source_ip <ipaddr>* – Specifies that the access profile applies only to packets with this source IP address. • *protocol_id <value 0-255>* – Specifies that the Switch examine the Protocol field in each packet and if this field contains the value entered here, apply the appropriate rules. • *destination_ip <ipaddr>* – Specifies that the access profile applies only to packets with this destination IP address. • *dscp <value 0-63>* – Specifies that the access profile applies only to packets that have this value in their Type-of-Service (DiffServ code point, DSCP) field in their IP packet header. • *icmp* – Specifies that the Switch examine the protocol field in each frame's header and it should match Internet Control Message Protocol (ICMP). • *type* – Specifies that the Switch examine each frame's ICMP Type field. • *code* – Specifies that the Switch examine each frame's ICMP Code field. • *igmp* – Specifies that the Switch examine each frame's protocol and it should match Internet Group Management

	Protocol (IGMP) field. • *type* – Specifies that the Switch examine each frame's IGMP Type field. • *tcp* - Specifies that the Switch examine each frame's protocol and it should matchTransport Control Protocol (TCP) field. • *src_port* <*value 0-65535*> – Specifies that the access profile applies only to packets that have this TCP source port in their TCP header. • *dst_port* <*value 0-65535*> – Specifies that the access profile applies only to packets that have this TCP destination port in their TCP header. • *flag {+ | –} {urg | ack | psh | rst | syn | fin }}* – Specifies the appropriate flag parameter. All incoming packets have TCP flag bits associated with them which are parts of a packet that determine what to do with the packet. The user may deny packets by denying certain flag bits within the packets. *To specify flag bits that should be "1" type + and the flag bit name, to specify bits that should be "0" type – and the flag bit name.* • *udp* – Specifies that the Switch examine the protocol field in each packet and it should match User Datagram Protocol (UDP). • *src_port* <*value 0-65535*> – Specifies that the access profile applies only to packets that have this UDP source port in their header. • *dst_port* <*value 0-65535*> – Specifies that the access profile applies only to packets that have this UDP destination port in their header. *port [<portlist> | all|* - The access profile for IP may be defined for each port on the Switch. *permit* – Specifies that packets that match the access profile are permitted to be forwarded by the Switch. • *mirror* – Specifies the action to mirror before being forwarded by the Switch. • *replace_dscp_with* <*value 0-63*> – Specifies a value to be written to the DSCP field of an incoming packet that meets the criteria specified in the first part of the command. This value will over-write the value in the DSCP field of the packet. *rx_rate* <*value 64-1024000*> – Specifies the rate limit to limit Rx bandwidth for for the profile being configured. This rate is implemented using the following equation – 1 value = 64kbit/sec. (ex. If the user selects a rx rate limit of 10 then the ingress rate is 640kbit/sec.) The user many select a value between 64- 1024000 or no limit. The default setting is no limit.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To configure a rule for the IP access profile:

```
DGS-2000-28MP:5# config access_profile profile_id 2 add access_id auto_assign ip
source_ip 10.10.10.10 port 5 deny
Command: config access_profile profile_id 2 add access_id auto_assign ip source_
```

```
ip 10.10.10.10 port 5 deny

Success.

DGS-2000-28MP:5#
```

create access_profile ipv6

Purpose	To create an access profile on the Switch by examining the Ethernet part of the packet header. Masks entered are combined with the values the Switch finds in the specified frame header fields. Specific values for the rules are entered using the **config access_profile** command, below.
Syntax	**create access_profile { class | source_ipv6_mask <ipv6mask> | destination_ipv6_mask <ipv6mask> |[icmp {{type | code}} | tcp {{src_port_mask <hex_mask 0x8000-0xffff> | dst_port_mask <hex_mask 0x8000-0xffff> | flag_mask}} | udp {{src_port_mask <hex_mask 0x8000-0xffff> | dst_port_mask <hex_mask 0x8000-0xffff>}}]} profile_id <value 1-150>**
Description	The **create access_profile** command creates a profile for packets that may be accepted or denied by the Switch by examining the Ethernet part of the packet header. Specific values for rules pertaining to the Ethernet part of the packet header may be defined by configuring the **config access_profile** command for Ethernet, as stated below.
Parameters	*ipv6* – Specifies that the Switch examines the IPv6 fields in each packet with special emphasis on one or more of the following: *class* – Examine the class field of the IPv6 header. *source_ipv6_mask* <*ipv6mask*> – Specifies the IPv6 address mask for the source IP. *destination_ipv6_mask* <*ipv6mask*> – Specifies the IPv6 address mask for the destination IP. *tcp* – Specifies that the Switch examines each frames protocol field and its value must be 6 (Transmission Control Protocol-TCP) for the action to take place. • *src_port_mask* <*hex 0x0-0xffff*> – Specifies a TCP port mask for the source port. • *dst_port_mask* <*hex 0x0-0xffff*> – Specifies a TCP port mask for the destination port. *udp* – Specifies that the Switch examines each frame's protocol field and it's value must be 17 (User Datagram Protocol-UDP) in order for the action to take place.. • *src_port_mask* <*hex 0x0-0xffff*> – Specifies a UDP port mask for the source port. • *dst_port_mask* <*hex 0x0-0xffff*> – Specifies a UDP port mask for the destination port. *icmp* – Specifies that the Switch examines the Protocol field in each frame's IP header , and that the value must be 1 (Internet Control Message Protocol- ICMP) for the action to take place. • *type* – Specifies that the Switch examines each frame's ICMP Type field.

	• *code* – Specifies that the Switch examines each frame's ICMP Code field. *profile_id <value 1-50>* – Specifies an index number between 1 and 50 that identifies the access profile being created with this command. The maximum entries for profile ID is 6.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To configure a rule for the IPv6 access profile:

```
DGS-2000-28MP:5# create access_profile ipv6 source_ipv6_mask ffff:: profile_id 3

Command: create access_profile ipv6 source_ipv6_mask ffff:: profile_id 3



Success.

DGS-2000-28MP:5#
```

config access_profile profile_id

Purpose	To create an access profile on the Switch by examining the Ethernet part of the packet header. Masks entered are combined with the values the Switch finds in the specified frame header fields. Specific values for the rules are entered using the **config access_profile** command, below.
Syntax	**config access_profile profile_id <value 1-150> add access_id [<value 1-200> | auto_assign] ipv6 { class <value 0-255> | source_ipv6 <ipv6addr> | destination_ipv6 <ipv6addr> | [icmp {{type <value 0-255> | code <value 0-255>}} | tcp {{src_port <value 0-65535> | dst_port <value 0-65535> | urg | ack | psh | rst | syn | fin})} | udp {{src_port <value 0-65535> | dst_port <value 0-65535>}}] } port [<portlist> | all] [permit {[replace_dscp_with <value 0-63> | rx_rate [<value 16-1000000> | no_limit] | replace_priority_with <value 0-7> | mirror]} | deny]**
Description	The **config access_profile ethernet** command defines the rules used by the Switch to either filter or forward packets based on the Ethernet part of each packet header.
Parameters	*profile_id <value 1-150>* – Specifies the access profile id to be configured with this command. This value is assigned to the access profile when it is created with the **create access_profile** command. The lower the profile ID, the higher the priority the rule will be given. *[add | delete] access_id <value 1-128>* – Adds or deletes an additional rule to the above specified access profile. The value specifies the relative priority of the additional rule. Up to 65535 rules may be configured for the Ethernet access profile. • *auto_assign* – Configures the Switch to automatically assign a numerical value (between 1 and 128) for the rule being configured. *ipv6* – Specifies that the Switch examines the IPv6 fields in each packet with special emphasis on one or more of the following: *class <value 0-255>* – Examine the class field of IPv6 header.

	The range is 0 to 255. *source_ipv6 <ipv6addr>* – Specifies that the access profile applies only to packets with this source IPv6 address. *destination_ipv6 <ipv6addr>* – Specifies that the access profile applies only to packets with this destination IPv6 address. *tcp* – Specifies that the Switch examines each frames protocol field and its value must be 6 (Transmission Control Protocol-TCP) for the action to take place. • *src_port <value 0-65535>* – Specifies the TCP source port range. The range is between 0 and 65535. • *dst_port <value 0-65535>* – Specifies the TCP destination port range. The range is between 0 and 65535. *udp* – Specifies that the Switch examines each frame's protocol field and it's value must be 17 (User Datagram Protocol-UDP) in order for the action to take place. • *src_port <value 0-65535>* –Specifies the UDP source port range. The range is between 0 and 65535. • *dst_port <value 0-65535>* –Specifies the UDP destination port range. The range is between 0 and 65535. *icmp* – Specifies that the Switch examines the Protocol field in each frame's IP header , and that the value must be 1 (Internet Control Message Protocol- ICMP) for the action to take place. • *type <value 0-255>* – Specifies that the Switch examines each frame's ICMP Type field. The range is between 0 and 255. • *code <value 0-255>* – Specifies that the Switch examines each frame's ICMP Code field. The range is between 0 and 255. *port [<portlist> | all|* - The access profile for IP may be defined for each port on the Switch. *permit* – Specifies that packets that match the access profile are permitted to be forwarded by the Switch. • *mirror* – Specifies the action to mirror before being forwarded by the Switch. • *replace_dscp_with <value 0-63>* – Specifies a value to be written to the DSCP field of an incoming packet that meets the criteria specified in the first part of the command. This value will over-write the value in the DSCP field of the packet. *rx_rate <value 64-1024000>* – Specifies the rate limit to limit Rx bandwidth for for the profile being configured. This rate is implemented using the following equation – 1 value = 64kbit/sec. (ex. If the user selects a rx rate limit of 10 then the ingress rate is 640kbit/sec.) The user many select a value between 64- 1024000 or no limit. The default setting is no limit.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To configure a rule for the IPv6 access profile:

```
DGS-2000-28MP:5# config access_profile profile_id 3 add access_id auto_assign
ipv6 source_ipv6 2001::34 port 12 deny
```

```
Command: config access_profile profile_id 3 add access_id auto_assign ipv6 sourc
e_ipv6 2001::34 port 12 deny


Success.

DGS-2000-28MP:5#
```

create access_profile packet_content_mask

Purpose	To create an access profile on the Switch by examining the Ethernet part of the packet header. Masks entered are combined with the values the Switch finds in the specified frame header fields. Specific values for the rules are entered using the **config access_profile** command, below.
Syntax	**create access_profile ([offset1 <value (0-31)> <hex (0x0-0xffffffff)>] [offset2 <value (0-31)> <hex (0x0-0xffffffff)>] [offset3 <value (0-31)> <hex (0x0-0xffffffff)>] [offset4 <value (0-31)> <hex (0x0-0xffffffff)>]) profile_id <value (1-150)>**
Description	The **create access_profile** command creates a profile for packets that may be accepted or denied by the Switch by examining the Ethernet part of the packet header. Specific values for rules pertaining to the Ethernet part of the packet header may be defined by configuring the **config access_profile** command for Ethernet, as stated below.
Parameters	*packet_content_mask* – Specifies the frame content mask. *[offset1 | offset2 | offset3 | offset4]* – Specifies the mask pattern offset of frame. *profile_id <value 1-150>* – Specifies an index number between 1 and 50 that identifies the access profile being created with this command. The maximum entries for profile ID is 150. The following table indicates the precise location of packet content user looking for. For example: 1st byte = offset3, loation 0 12th byte = offset2, location 3

Chunk	C0	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12	C13	C14	C15
Offset	127	3	7	11	15	19	23	27	31	35	39	43	47	51	55	59
Offset	128	4	8	12	16	20	24	28	32	36	40	44	48	52	56	60
Offset	1	5	9	13	17	21	25	29	33	37	41	45	49	53	57	61
Offset	2	6	10	14	18	22	26	30	34	38	42	46	50	54	58	62

Chunk	C16	C17	C18	C19	C20	C21	C22	C23	C24	C25	C26	C27	C28	C29	C30	C31
Offset	63	67	71	75	79	83	87	91	95	99	103	107	111	115	119	123
Offset	64	68	72	76	80	84	88	92	96	100	104	108	112	116	120	124
Offset	65	69	73	77	81	85	89	93	97	101	105	109	113	117	121	125
Offset	66	70	74	78	82	86	90	94	98	102	106	110	114	118	122	126

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

Example usage:

To configure a rule for the packet content access profile for 119th byte:

```
DGS-2000-28MP:5# create access_profile packet_content_mask offset1 30 0xffffffff
profile_id 4
Command: create access_profile packet_content_mask offset1 30 0xffffffff profile_id
4


Success.

DGS-2000-28MP:5#
```

config access_profile profile_id

Purpose	To create an access profile on the Switch by examining the Ethernet part of the packet header. Masks entered are combined with the values the Switch finds in the specified frame header fields. Specific values for the rules are entered using the **config access_profile** command, below.
Syntax	**config access_profile profile_id <value (1-150)> add access_id {<value (1-200)> | auto_assign} packet_content ([offset_chunk_1 <hex (0x0-0xffffffff)>] [offset_chunk_1_mask <hex (0x0-0xffffffff)>] [offset_chunk_2 <hex (0x0-0xffffffff)>] [offset_chunk_2_mask <hex (0x0-0xffffffff)>] [offset_chunk_3 <hex (0x0-0xffffffff)>] [offset_chunk_3_mask <hex (0x0-0xffffffff)>] [offset_chunk_4 <hex (0x0-0xffffffff)>] [offset_chunk_4_mask <hex (0x0-0xffffffff)>]) port {<portlist> | all} {permit [{replace_dscp_with <value (0-63)> | rx_rate {<value (16-1000000)> | no_limit} | replace_priority_with <value (0-7)> | mirror}] | deny}**
Description	The **config access_profile ethernet** command defines the rules used by the Switch to either filter or forward packets based on the Ethernet part of each packet header.
Parameters	*profile_id <value 1-150>* – Specifies the access profile id to be configured with this command. This value is assigned to the access profile when it is created with the **create access_profile** command. The lower the profile ID, the higher the priority the rule will be given. *add access_id <value 1-200>* – Adds an additional rule to the above specified access profile. The value specifies the relative priority of the additional rule. Up to 200 rules may be configured for the access profile. • *auto_assign* – Configures the Switch to automatically assign a numerical value (between 1 and 128) for the rule being configured. *packet_content* – Specifies particular packet partner: • *offset_chunk_1* - Specifies the contents of the offset chunk 1 to be monitored. - Enter the contents of the offset trunk 1 to be monitored here. • *offset_chunk_1_mask* - Specifies an additional mask for each field. - Enter the additional mask value used here. • *offset_chunk_2* - Specifies the contents of the offset chunk 2 to be monitored. - Enter the contents of the offset trunk 2 to be monitored here. • offset_chunk_2 _mask - Specifies an additional mask for

	each field. - Enter the additional mask value used here. • *offset_chunk_3* - Specifies the contents of the offset chunk 3 to be monitored. - Enter the contents of the offset trunk 3 to be monitored here. • *offset_chunk_3_mask* - Specifies an additional mask for each field. - Enter the additional mask value used here. • *offset_chunk_4* - Specifies the contents of the offset chunk 4 to be monitored. - Enter the contents of the offset trunk 4 to be monitored here. • *offset_chunk_4_mask* - Specifies an additional mask for each field. - Enter the additional mask value used here *permit* – Specifies that packets that match the access profile are permitted to be forwarded by the Switch. • *mirror* – Specifies the action to mirror before being forwarded by the Switch. • *replace_dscp_with <value 0-63>* – Specifies a value to be written to the DSCP field of an incoming packet that meets the criteria specified in the first part of the command. This value will over-write the value in the DSCP field of the packet. *rx_rate <value 64-1024000>* – Specifies the rate limit to limit Rx bandwidth for for the profile being configured. This rate is implemented using the following equation – 1 value = 64kbit/sec. (ex. If the user selects a rx rate limit of 10 then the ingress rate is 640kbit/sec.) The user many select a value between 64- 1024000 or no limit. The default setting is no limit.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To configure a rule for the packet content access profile:

```
DGS-2000-28MP:5# config access_profile profile_id 4 add access_id auto_assign
packet_content offset_chunk_1 0x00111100 port 12 deny
Command: config access_profile profile_id 4 add access_id auto_assign
packet_content offset_chunk_1 0x00111100 port 12 deny

Success.

DGS-2000-28MP:5#
```

delete access_profile

Purpose	To delete a previously created access profile
Syntax	**delete access_profile [all | profile_id <value 1-150>]**
Description	The **delete access_profile** command deletes a previously created access profile on the Switch.
Parameters	*all* – Specifies all acc profiles to be deleted. *profile_id <value 1-150>* – Specifies the access profile to be deleted.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

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

```
DGS-2000-28MP:5# delete access_profile profile_id 1
Command: delete access_profile profile_id 1

Success.

DGS-2000-28MP:5#
```

config access_profile profile_id

Purpose	To delete specific access rule.
Syntax	**confg access_profile profile_id <value 1-150> delete access_id <value 1-200>**
Description	This command is used to remove the specific access rule..
Parameters	*profile_id <value 1-150>* – Specifies the access profile id to be configured with this command. *delete access_id <value 1-200>* – Specifies the access rule ID.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

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

```
DGS-2000-28MP:5# config access_profile profile_id 1 delete access_id 1

Command: config access_profile profile_id 1 delete access_id 1


Success.

DGS-2000-28MP:5#
```

show access_profile

Purpose	To display the currently configured access profiles on the Switch.
Syntax	**show access_profile {profile_id <value 1-150>}**
Description	The **show access_profile** command displays the currently configured access profiles.
Parameters	*profile_id <value 1-150>* – Specifies the access profile to be displayed. This value is assigned to the access profile when it is created with the **create access_profile** command. If the *profile_id* parameter is omitted, all access profile entries are displayed.
Restrictions	None.

Example usage:

To display the currently configured access profiles which profile id is 1 on the Switch:

```
DGS-2000-28MP:5# show access_profile profile_id 1
Command: show access_profile profile_id 1


Access Profile Table

Access Profile ID: 1          Type: Ethernet
------------------------------------------------------------------------
------------------------------------------------------------------------
Mask Option:
VLAN   802.1p
------------------------------------------------------------------------


DGS-2000-28MP:5#
```

create cpu_access_profile ethernet

Purpose	To create an access profile on the Switch by examining the Ethernet part of the packet header. Masks entered are combined with the values the Switch finds in the specified frame header fields. Specific values for the rules are entered using the **config access_profile** command, below.
Syntax	**create cpu_access_profile {vlan | source_mac <macmask> | destination_mac <macmask> | ethernet_type | 802.1p}(1) profile_id <value 1-3>**
Description	The **create cpu_access_profile** command is used to create CPU access list rules on the Switch.
Parameters	*ethernet* - Specifies that the Switch examines the layer 2 part of each packet header with emphasis on one or more of the following: • *vlan* – Specifies a VLAN mask. • *source_mac* <*macmask* > – Specifies the source MAC mask. • *destination_mac* <*macmask*> – Specifies the destination MAC mask. • *802.1p* – Specifies 802.1p priority tag mask. *ethernet_type* – Specifies the Ethernet type mask. *profile_id* <*value 1-3*> – Specifies the cpu access profile to be displayed.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To create a CPU IP access profile:

```
DGS-2000-28MP:5# create cpu access_profile ip source_ip_mask 20.0.0.0 destination_ip_mask 10.0.0.0 dscp icmp type profile_id 2
Command: create cpu access_profile ip source_ip_mask 20.0.0.0 destination_ip_mask 10.0.0.0 dscp icmp type profile_id 2

Success.
DGS-2000-28MP:5#
```

config cpu_access_profile profile_id

Purpose	To configures the settings of cpu access profiles.
Syntax	**config cpu_access_profile profile_id <value 1-3> add access_id [<value 1-10> | auto_assign] ethernet {vlan <vlanid 1-4094> | source_mac <macaddr> | destination_mac <macaddr> | ethernet_type <hex 0x0-0xffff> | 802.1p <value 0-7>} port [<portlist> | all] [permit | deny]**
Description	The **config cpu_access_profile** command configures the settings of cpu access profiles.
Parameters	*profile_id <value 1-3>* – Specifies the cpu access profile to be configured. *[add | delete]* – Add or delete the profile id. *access_id [<value 1-5> | auto_assign]* – Specifies the access id value or use auto assign. *ethernet* – Specifies that the Switch examine only the layer 2 part of each packet to determine if it is to be filtered or forwarded based on one or more of the following: • *802.1p <value 0-7>* – Specifies the 802.1p value. The range is between 0 and 7. • *destination_mac <macaddrf>* – Specifies the destination MAC address. • *ethernet_type* – Specifies the Ethernet type mask. • *<portlist>* – Specifies the port or ports to be configured. • *source_mac <macaddr>* – Specifies the source MAC address. *vlan <vlanid 1-4094>* – Specifies the VLAN id.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To configure a rule for the CPU IP access profile:

```
DGS-2000-28MP:5# config cpu access_profile profile_id 2 add access_id auto_assignip destination_ip 10.48.100.2 ports 1-3 permit
Command: config cpu access_profile profile_id 2 add access_id auto_assign ip destination_ip 10.48.100.2 ports 1-3 permit

Success.

DGS-2000-28MP:5#
```

create cpu_access_profile ip

Purpose	To create an access profile on the Switch by examining the Ethernet part of the packet header. Masks entered are combined with the values the Switch finds in the specified frame header fields. Specific values for the rules are entered using the **config access_profile** command, below.
Syntax	**create cpu_access_profile ip { source_ip_mask <netmask> | destination_ip_mask <netmask> | dscp |[icmp {{type | code}} | igmp {type} | tcp {{src_port_mask <hex_mask 0x8000-0xffff> | dst_port_mask <hex_mask 0x8000-0xffff> | flag_mask}} | udp {{src_port_mask <hex_mask 0x8000-0xffff> | dst_port_mask <hex_mask 0x8000-0xffff>}} | protocol_id_mask <hex_mask 0x0-0xff>] } profile_id <value 1-3>**
Description	The **create cpu_access_profile** command is used to create CPU access list rules on the Switch.
Parameters	*ip* - Specifies that the Switch examines the IP fields in each packet with special emphasis on one or more of the following: • *type* – Specifies that the Switch examine each frame's ICMP Type field. • *code* – Specifies that the Switch examine each frame's ICMP code field. • *type* – Specifies that the Switch examine each frame's IGMP Type field. *tcp* – Specifies that the Switch examines each frames protocol field and its value must be 6 (Transmission Control Protocol-TCP) for the action to take place. • *src_port_mask* <*hex 0x0-0xffff*> – Specifies the TCP port mask for the source port. • *dst_port_mask* <*hex 0x0-0xffff*> – Specifies the TCP port mask for the destination port. • flag_mask - Specifies the appropriate flag. *udp* – Specifies that the Switch examines each frame's protocol field and it's value must be 17 (User Datagram Protocol-UDP) in order for the action to take place. • *src_port_mask* <*0x0-0xffff*> – Specifies the UDP port mask for the source port. • *dst_port_mask* <*0x0-0xffff*> – Specifies the UDP port mask for the destination port mask. • *protocol_id_mask* <*0x0-0xffff*> – Specifies the protocol id mask. • *source_ip_mask* <*netmask*> – Specifies the source IPv4 mask. • *destination_ip_mask* <*netmask*> – Specifies the destination IPv4 mask. *dscp* – Specifies that the Switch examines the DiffServ Code Point (DSCP) field in each frame's header. *profile_id* <*value 1-3*> – Specifies the cpu access profile to be displayed.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To create a CPU IP access profile:

```
DGS-2000-28MP:5# create cpu access_profile ip source_ip_mask 20.0.0.0 destination_ip_mask 10.0.0.0 dscp icmp type profile_id 2
Command: create cpu access_profile ip source_ip_mask 20.0.0.0 destination_ip_mask 10.0.0.0 dscp icmp type profile_id 2

Success.
DGS-2000-28MP:5#
```

config cpu_access_profile profile_id

Purpose	To configures the settings of cpu access profiles.
Syntax	**config cpu_access_profile profile_id <value 1-3> add access_id [<value 1-10> | auto_assign] ip { source_ip <ipaddr> | destination_ip <ipaddr> | dscp <value 0-63> | [icmp {{type <value 0-255> | code <value 0-255>}} | igmp {type <value 0-255>} | tcp {{src_port <value 0-65535> | dst_port <value 0-65535> | urg | ack | psh | rst | syn | fin}} | udp {{src_port <value 0-65535> | dst_port <value 0-65535>}(1)} | protocol_id <value 0-255>] } port [<portlist> | all] [permit | deny]**
Description	The **config cpu_access_profile** command configures the settings of cpu access profiles.
Parameters	*profile_id <value 1-3>* – Specifies the cpu access profile to be configured. *[add | delete]* – Add or delete the profile id. *access_id [<value 1-5> | auto_assign]* – Specifies the access id value or use auto assign. *ip* – Specifies that the Switch examine the IP fields in each packet to determine if it will be either forwarded or filtered based on one or more of the following: • *destination_ip <ip_addr>* – Specifies the destination IP address. • *dscp <value 0-63>* – Specifies the DSCP value. *icmp* – Specifies that the Switch examines the Protocol field in each frame's IP header , and that the value must be 1 (Internet Control Message Protocol- ICMP) for the action to take place. • *code <value 0-255>* –Specifies that the Switch examine each frame's ICMP code field. • *type <value 0-255>* –Specifies that the Switch examine each frame's ICMP Type field. *igmp* – Specifies that the Switch examine each frame's protocol field and it must be 2 (Internet Group Management Protocol- IGMP) for the action to take place. • *igmp_type <value 0-255>* – Specifies the IGMP type. *<portlist>* – Specifies the port or ports to be configured. *protocol_id <value 0-255>* – Specifies the protocol id. *source_ip <ip_addr>* –Specifies that the cpu access profile applies only to packets with this source IP address. *Tcp* – Specifies that the Switch examines each frames protocol field and its value must be 6 (Transmission Control Protocol- TCP) for the action to take place • *dst_port <value 0-65535>* –Specifies that the cpu access profile applies only to packets that have this TCP destination

	port in their header. • *flag <string>* – Specifies the appropriate flag parameter. • *src_port <value 0-65535>* –Specifies that the cpu access profile applies only to packets that have this TCP source port in their header. *udp* – Specifies that the Switch examines each frame's protocol field and it's value must be 17 (User Datagram Protocol-UDP) in order for the action to take place. • *dst_port <value 0-65535>* – Specifies that the CPU access profile applies only to packets that have this UDP destination port in their header. *src_port <value 0-65535>* – Specifies that the CPU access profile applies only to packets that have this UDP source port in their header.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To configure a rule for the CPU IP access profile:

```
DGS-2000-28MP:5# config cpu access_profile profile_id 2 add access_id auto_assignip destination_ip 10.48.100.2 ports 1-3 permit
Command: config cpu access_profile profile_id 2 add access_id auto_assign
ip destination_ip 10.48.100.2 ports 1-3 permit

Success.

DGS-2000-28MP:5#
```

create cpu_access_profile ipv6

Purpose	To create an access profile on the Switch by examining the Ethernet part of the packet header. Masks entered are combined with the values the Switch finds in the specified frame header fields. Specific values for the rules are entered using the **config access_profile** command, below.
Syntax	**create cpu_access_profile ipv6 { class | source_ipv6_mask <ipv6mask> | destination_ipv6_mask <ipv6mask> } profile_id <value 1-3>>**
Description	The **create cpu_access_profile** command is used to create CPU access list rules on the Switch.
Parameters	*ipv6* - Specifies that the Switch examines the IPv6 fields in each packet with special emphasis on one or more of the following: • *class* – Examine the class field of the IPv6 header. • *source_ipv6_mask <ipv6mask>* – Specifies the source IPv6 mask. • *destination_ipv6_mask < ipv6mask >* – Specifies the destination IPv6 mask. *profile_id <value 1-3>* – Specifies the cpu access profile to be displayed.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To create a CPU IP access profile:

```
DGS-2000-28MP:5# create cpu access_profile ip source_ip_mask 20.0.0.0 destination_ip_mask 10.0.0.0 dscp icmp type profile_id 2
Command: create cpu access_profile ip source_ip_mask 20.0.0.0 destination_ip_mask 10.0.0.0 dscp icmp type profile_id 2

Success.
DGS-2000-28MP:5#
```

config cpu_access_profile profile_id

Purpose	To configures the settings of cpu access profiles.
Syntax	**config cpu_access_profile profile_id <value 1-3> add access_id [<value 1-10> | auto_assign] ipv6 { class <value 0-255> | source_ipv6 <ipv6addr> | destination_ipv6 <ipv6addr> } port [<portlist> | all] [permit | deny]**
Description	The **config cpu_access_profile** command configures the settings of cpu access profiles.
Parameters	*profile_id <value 1-3>* – Specifies the cpu access profile to be configured. *[add | delete]* – Add or delete the profile id. *access_id [<value 1-5> | auto_assign]* – Specifies the access id value or use auto assign. *ipv6* - Specifies that the Switch examines the IPv6 fields in each packet with special emphasis on one or more of the following: • *class* – Examine the class field of the IPv6 header. • *source_ipv6 <ipv6addr>* – Specifies the source IPv6 address. • *destination_ipv6 < ipv6addr >* – Specifies the destination IPv6 address.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To configure a rule for the CPU IP access profile:

```
DGS-2000-28MP:5# config cpu access_profile profile_id 2 add access_id auto_assignip destination_ip 10.48.100.2 ports 1-3 permit
Command: config cpu access_profile profile_id 2 add access_id auto_assign
ip destination_ip 10.48.100.2 ports 1-3 permit

Success.

DGS-2000-28MP:5#
```

create cpu_access_profile packet_content

Purpose	To create an access profile on the Switch by examining the Ethernet part of the packet header. Masks entered are combined with the values the Switch finds in the specified frame header fields. Specific values for the rules are entered using the **config access_profile**

	command, below.
Syntax	**create cpu_access_profile packet_content ([offset_0-15 <hex (0x0-0xffffffff)> <hex (0x0-0xffffffff)> <hex (0x0-0xffffffff)> <hex (0x0-0xffffffff)>] [offset_16-31 <hex (0x0-0xffffffff)> <hex (0x0-0xffffffff)> <hex (0x0-0xffffffff)> <hex (0x0-0xffffffff)>] [offset_32-47 <hex (0x0-0xffffffff)> <hex (0x0-0xffffffff)> <hex (0x0-0xffffffff)> <hex (0x0-0xffffffff)>] [offset_48-63 <hex (0x0-0xffffffff)> <hex (0x0-0xffffffff)> <hex (0x0-0xffffffff)> <hex (0x0-0xffffffff)>] [offset_64-79 <hex (0x0-0xffffffff)> <hex (0x0-0xffffffff)> <hex (0x0-0xffffffff)> <hex (0x0-0xffffffff)>]) profile_id <value (1-3)>**
Description	The **create cpu_access_profile** command is used to create CPU access list rules on the Switch.
Parameters	*packet_content* - Specifies that the Switch examines the layer 2 part of each packet header with emphasis on one or more of the following: • *offset_0-15 <hex (0x0-0xffffffff)> <hex (0x0-0xffffffff)> <hex (0x0-0xffffffff)> <hex (0x0-0xffffffff)>*- Specifies the offset value for 1st byte to 16th byte. • *offset_16-31 <hex (0x0-0xffffffff)> <hex (0x0-0xffffffff)> <hex (0x0-0xffffffff)> <hex (0x0-0xffffffff)>*- Specifies the offset value for 17th byte to 31st byte. • *offset_32-47 <hex (0x0-0xffffffff)> <hex (0x0-0xffffffff)> <hex (0x0-0xffffffff)> <hex (0x0-0xffffffff)>*- Specifies the offset value for 32nd byte to 48th byte. • *offset_48-63 <hex (0x0-0xffffffff)> <hex (0x0-0xffffffff)> <hex (0x0-0xffffffff)> <hex (0x0-0xffffffff)>*- Specifies the offset value for 49th byte to 64th byte. • *offset_64-79 <hex (0x0-0xffffffff)> <hex (0x0-0xffffffff)> <hex (0x0-0xffffffff)> <hex (0x0-0xffffffff)>*- Specifies the offset value for 65th byte to 80th byte. *profile_id <value 1-3>* – Specifies the cpu access profile to be displayed.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To create a CPU packet content access profile:

```
DGS-2000-28MP:5# create cpu_access_profile packet_content offset_0-15 0xffffffff 0xffffffff 0xffffffff 0xffffffff profile_id 1
Command: create cpu_access_profile packet_content offset_0-15 0xffffffff 0xffffffff 0xffffffff 0xffffffff profile_id 1


Success.

DGS-2000-28MP:5#
```

config cpu_access_profile profile_id

Purpose	To configures the settings of cpu access profiles.
Syntax	**config cpu_access_profile profile_id <value (1-3)> add access_id {<value (1-5)> | auto_assign} packet_content**

	([offset_0-15 <hex (0x0-0xffffffff)> <hex (0x0-0xffffffff)> <hex (0x0-0xffffffff)> <hex (0x0-0xffffffff)>] [offset_16-31 <hex (0x0-0xffffffff)> <hex (0x0-0xffffffff)> <hex (0x0-0xffffffff)> <hex (0x0-0xffffffff)>] [offset_32-47 <hex (0x0-0xffffffff)> <hex (0x0-0xffffffff)> <hex (0x0-0xffffffff)> <hex (0x0-0xffffffff)>] [offset_48-63 <hex (0x0-0xffffffff)> <hex (0x0-0xffffffff)> <hex (0x0-0xffffffff)> <hex (0x0-0xffffffff)>] [offset_64-79 <hex (0x0-0xffffffff)> <hex (0x0-0xffffffff)> <hex (0x0-0xffffffff)> <hex (0x0-0xffffffff)>]) port {<portlist> | all} {permit | deny}
Description	The **config cpu_access_profile** command configures the settings of cpu access profiles.
Parameters	*profile_id* <*value 1-3*> – Specifies the cpu access profile to be configured. *[add* | *delete]* – Add or delete the profile id. *access_id [*<*value 1-10*> | *auto_assign]* – Specifies the access id value or use auto assign. *packet_content* - Specifies that the Switch examines the layer 2 part of each packet header with emphasis on one or more of the following: • *offset_0-15* <*hex (0x0-0xffffffff)*> <*hex (0x0-0xffffffff)*> <*hex (0x0-0xffffffff)*> <*hex (0x0-0xffffffff)*>- Specifies the offset value for 1st byte to 16th byte. • *offset_16-31* <*hex (0x0-0xffffffff)*> <*hex (0x0-0xffffffff)*> <*hex (0x0-0xffffffff)*> <*hex (0x0-0xffffffff)*>- Specifies the offset value for 17th byte to 31st byte. • *offset_32-47* <*hex (0x0-0xffffffff)*> <*hex (0x0-0xffffffff)*> <*hex (0x0-0xffffffff)*> <*hex (0x0-0xffffffff)*>- Specifies the offset value for 32nd byte to 48th byte. • *offset_48-63* <*hex (0x0-0xffffffff)*> <*hex (0x0-0xffffffff)*> <*hex (0x0-0xffffffff)*> <*hex (0x0-0xffffffff)*>- Specifies the offset value for 49th byte to 64th byte. • *offset_64-79* <*hex (0x0-0xffffffff)*> <*hex (0x0-0xffffffff)*> <*hex (0x0-0xffffffff)*> <*hex (0x0-0xffffffff)*>- Specifies the offset value for 65th byte to 80th byte.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To configure a rule for the CPU packet content access profile:

```
DGS-2000-28MP:5# config cpu_access_profile profile_id 1 add access_id auto_assign packet_content offset_0-15 0xf0fffff 0xf0fffff 0xf0fffff 0xf0fffff port 16 deny

Command: config cpu_access_profile profile_id 1 add access_id auto_assign packet_content offset_0-15 0xf0fffff 0xf0fffff 0xf0fffff 0xf0fffff port 16 deny

Success.

DGS-2000-28MP:5#
```

delete cpu_access_profile

Purpose	To delete a previously created cpu access profile.
Syntax	**delete cpu_access_profile profile_id <value 1-3>**
Description	The **delete cpu_access_profile** command deletes a previously created access profile on the Switch.
Parameters	*profile_id <value 1-3>* – Specifies the cpu access profile to be deleted.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

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

```
DGS-2000-28MP:5# delete cpu access_profile profile_id 1
Command: delete cpu access_profile profile_id 1

Success.

DGS-2000-28MP:5#
```

config cpu_access_profile profile_id

Purpose	To delete specific access rule.
Syntax	**confg cpu_access_profile profile_id <value 1-3> delete access_id <value 10>**
Description	This command is used to remove the specific access rule..
Parameters	*profile_id <value 1-3>* – Specifies the access profile id to be configured with this command. *delete access_id <value 1-10>* – Specifies the access rule ID.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

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

```
DGS-2000-28MP:5# config cpu_access_profile profile_id 1 delete access_id 1

Command: config cpu_access_profile profile_id 1 delete access_id 1


Success.

DGS-2000-28MP:5#
```

show cpu_access_profile

Purpose	To view the CPU access profile entry currently set in the Switch.

Syntax	**show cpu_access_profile {profile_id <value 1-3>}**
Description	The **show cpu access_profile** command is used view the current CPU interface filtering entries set on the Switch.
Parameters	*profile_id <value 1-3>* – Enter an integer between 1 and 3 that is used to identify the CPU access profile to be deleted with this command. This value is assigned to the access profile when it is created with the create cpu access_profile command.
Restrictions	None.

Example usage:

To show the CPU filtering state on the Switch:

```
DGS-2000-28MP:5# show cpu_access_profile
Command: show cpu_access_profile



Access Profile ID: 1    Type: Packet Content
-------------------------------- Option Mask --------------------------------
OffSet              Payload
00-15             : 0xffffffff  ffffffff  ffffffff  ffffffff
-------------------------------- Option End ---------------------------------

Profile ID         : 1
Access ID          : 1
Type               : packet content
OffSet              Payload
00-15             : 0x0f0fffff  0f0fffff  0f0fffff  0f0fffff


Profile Statistic    : 1/3
Rule  Statistic    : 1/30
DGS-2000-28MP:5#
```

35

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 [tacacs+ | 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>]
show authen_policy	
create authen_enable method_list_name	<string 15>
config authen_enable	[default | method_list_name <string 15>] method {tacacs+ | 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	
config authen application	{console | http | ssh | telnet | 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> | ipv6address <ipv6addr>] protocol [radius | tacacs+] { acct_port <int 1-65535> | port <int 1-65535> | key [<string 254> | encryption_key <string 800> | none] | timeout <int 1-255> | retransmit <int 1-255>}
config authen server_host	[<ipaddr> | ipv6address <ipv6addr>] protocol [tacacs+ | radius] {acct_port <int 1-65535> | port <int 1-65535> | encryption_key <string 800> | key [<string 254> | none] | timeout <int 1-255> | retransmit <int 1-255>}
delete authen server_host	[<ipaddr> | ipv6address <ipv6addr>] protocol [tacacs+ | radius]
show authen server_host	
create authen server_group	<string 15>
config authen server_group	[<string 15> | radius | tacacs+] [add | delete] server_host [<ipaddr> |

Command	Parameter
	ipv6address <ipv6addr>] protocol [radius | tacacs+]
delete authen server_group	<string 15>
show authen server_group	{<string 15>}
enable admin	
config admin local_enable	{encrypt {plain_text <password 15> | sha_1 <password 35>}}

Each command is listed in detail, as follows:

create authen_login method_list_name	
Purpose	To create a user-defined list of authentication methods for users logging on to the Switch.
Syntax	**create authen_login method_list_name <string 15>**
Description	The **create authen_login method_list_name** command creates a list of authentication techniques for user login. The Switch can support up to eight method lists, but one is reserved as a default and cannot be deleted. Multiple method lists must be created and configured separately.
Parameters	<*string 15*> - Defines the *method_list_name* to be created as a string of up to 15 alphanumeric characters.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To create the method list 'Trinity'.

```
DGS-2000-28MP:5# create authen_login method_list_name Trinity
Command: create authen_login method_list_name Trinity


Success.

DGS-2000-28MP:5#
```

config authen_login	
Purpose	To configure a user-defined or default *method list* of authentication methods for user login.
Syntax	**config authen_login [default | method_list_name <string 15>] method [tacacs+ | radius | local | server_group <string 15> | none]**
Description	The **config authen_login** command configures a user-defined or default *method list* of authentication methods for users logging on to the Switch. The sequence of methods implemented in this command affects the authentication result. For example, if a user enters a sequence of methods like *tacacs – local,* the Switch sends an authentication request to the first *tacacs* host in the server group. If

	no response comes from the server host, the Switch sends an authentication request to the second *tacacs* host in the server group and so on, until the list is exhausted. When the local method is used, the privilege level is dependant on the local account privilege configured on the Switch. Successful login using any of these methods gives the user a 'user' priviledge only. If the user wishes to upgrade his or her status to the administrator level, the user must implement the *enable admin* command, followed by a previously configured password. (*See the **enable admin** part of this section for more detailed information, concerning the **enable admin** command.)*
Parameters	*default* – The default method list for access authentication, as defined by the user. The user may choose one or more of the following authentication methods: ▪ *tacacs+* – Specifies that the user is to be authenticated using the *TACACS+* protocol from the remote TACACS+ *server hosts* of the TACACS+ *server group* list. ▪ *radius* - Specifies that the user is to be authenticated using the *RADIUS* protocol from the remote RADIUS *server hosts* of the RADIUS *server group* list. ▪ *local* - Specifies that the user is to be authenticated using the local *user account* database on the Switch. ▪ *server_group* <*string 15*> –Specifies that the user is to be authenticated using the server group *account* database on the Switch. ▪ *none* – Specifies that no authentication is required to access the Switch. *method_list_name* <*string 15*> – Specifies a previously created method list name defined by the user. One or more of the following authentication methods may be added to this method list: ▪ *tacacs+* – Specifies that the user is to be authenticated using the *TACACS+* protocol from a remote TACACS+ server. ▪ *radius* - Specifies that the user is to be authenticated using the *RADIUS* protocol from a remote RADIUS server. ▪ *local* - Specifies that the user is to be authenticated using the local *user account* database on the Switch. ▪ *server_group* <*string 15*> –Specifies that the user is to be authenticated using the server group *account* database on the Switch. ▪ *none* – Specifies that no authentication is required to access the Switch.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the user defined method list 'Trinity' with authentication methods TACACS+, RADIUS and local, in that order.

```
DGS-2000-28MP:5# config authen_login method_list_name Trinity method tacacs+ radius local
Command: config authen_login method_list_name Trinity method tacacs+ radius local


Success.

DGS-2000-28MP: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 *method_list_name* to delete.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete the method list name 'Trinity':

```
DGS-2000-28MP:5# delete authen_login method_list_name Trinity
Command: delete authen_login method_list_name Trinity

Success.

DGS-2000-28MP: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	*default* – Displays the default method list for users logging on to the Switch. *method_list_name* <*string 15*> - Specifies the *method_list_name* to display. *all* – Displays all the authentication login methods currently configured on the Switch. The command displays the following parameters: • Method List Name – The name of a previously configured method list name. • Method Name – Defines which security protocols are implemeted, per method list name.

Restrictions	Only Administrator-level users can issue this command.

Example usage:

To view all authentication login method list names:

```
DGS-2000-28MP:5# show authen_login all
Command: show authen_login all


Method List Name  Priority   Method Name      Comment
----------------------------  -----------  ---------------------  ------------------
default                 1          local                Keyword

Trinity                 1          none                 Keyword

DGS-2000-28MP: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 display the system access authentication policy status on the Switch.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To display the system access authentication policy:

```
DGS-2000-28MP:5# show authen_policy
Command: show authen_policy

Authentication Policy : Disabled

DGS-2000-28MP: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 *authen_enable method_list_name* to be created as a string of up to 15 alphanumeric characters.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To create a user-defined method list, named 'Permit' for promoting user privileges to Adminstrator privileges:

```
DGS-2000-28MP:5# create authen_enable method_list_name Permit
Command: create authen_enable method_list_name Permit

Success.

DGS-2000-28MP: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 {tacacs+ | radius | local | server_group <string 15> | none}**
Description	The **config authen_enable** command configures a user-defined list of authentication methods for promoting normal user level privileges to Administrator level privileges using authentication methods on the Switch. Once a user acquires normal user level privileges on the Switch, he or she must be authenticated by a method on the Switch to gain administrator privileges on the Switch, which is defined by the Administrator. A maximum of eight (8) enable method lists can be implemented simultaneously on the Switch. The sequence of methods implemented in this command affects the authentication result. For example, if a user enters a sequence of methods like *tacacs+ – radius – local_enable,* the Switch sends an authentication request to the first *TACACS+* host in the server group. If no verification is found, the Switch sends an authentication request to the second *TACACS+* host in the server group and so on, until the list is exhausted. At that point, the Switch restarts the same sequence with the following protocol listed, *radius*. If no authentication takes place using the *radius* list, the *local_enable* password set in the Switch is used to authenticate the user. Successful authentication using any of these methods gives the user an 'Admin' level privilege.
Parameters	*default* – The default method list for adminstration rights authentication, as defined by the user. The user may choose one or more of the following authentication methods: • *tacacs+* – Specifies that the user is to be authenticated using the *TACACS+* protocol from the remote TACACS+ *server hosts* of the TACACS+ *server group* list. • *radius* – Specifies that the user is to be authenticated using the *RADIUS* protocol from the remote RADIUS *server hosts* of the RADIUS *server group* list. • *local* - Specifies that the user is to be authenticated using

	the local *user account* database on the Switch. • *server_group* <*string 15*> – Specifies the server group name for authentication. • *none* – Specifies that no authentication is required to access the Switch. *method_list_name* <*string 15*> – Specifies a previously created *authen_enable method_list_name*. The user may add one or more of the following authentication methods to this method list: • *tacacs+* – Specifies that the user is to be authenticated using the *TACACS+* protocol from a remote TACACS+ server. • *radius* - Specifies that the user is to be authenticated using the *RADIUS* protocol from a remote RADIUS server. • *local* - Specifies that the user is to be authenticated using the local *user account* database on the Switch. The local enable password of the device can be configured using the '**config admin local_password**' command. • *server_group* <*string 15*> –Specifies that the user is to be authenticated using the server group account database on the Switch. • *none* – Specifies that no authentication is required to access the Switch.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the user defined method list 'Permit' with authentication methods TACACS+, RADIUS and local_enable, in that order.

```
DGS-2000-28MP:5# config authen_enable method_list_name Trinity method
tacacs+ radius local
Command: config authen_enable method_list_name Trinity method tacacs+ radius
local

Success.

DGS-2000-28MP: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 Adminstrator level privileges.
Parameters	<*string 15*> - The previously created *authen_enable method_list_name* to be deleted.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete the user-defined method list 'Permit'

```
DGS-2000-28MP:5# delete authen_enable method_list_name Permit
Command: delete authen_enable method_list_name Permit


Success.

DGS-2000-28MP: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 deletes a user-defined list of authentication methods for promoting user level privileges to Adminstrator level privileges.
Parameters	*default* – Displays the default method list for users attempting to gain access to Administrator level privileges on the Switch. *method_list_name* <*string 15*> – The *method_list_name* to be displayed. *all* – Displays all the authentication login methods currently configured on the Switch. The command displays the following parameters: • Method List Name – The name of a previously configured method list name. • Method Name – Defines which security protocols are implemeted, per method list name.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To display all method lists for promoting user level privileges to administrator level privileges.

```
DGS-2000-28MP:5# show authen_enable all
Command: show authen_enable all


Method List Name  Priority  Method Name   Comment
------------------------  --------  -------------------  ------------------
default                   1         local                Keyword

DGS-2000-28MP: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-level users can issue this command.

Example usage:

To enable the authentication policy:

```
DGS-2000-28MP:5# enable authen_policy
Command: enable authen_policy

Success.
DGS-2000-28MP: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-level users can issue this command.

Example usage:

To disable the authentication policy:

```
DGS-2000-28MP:5# disable authen_policy
Command: disable authen_policy

Success.
DGS-2000-28MP: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 | ssh | telnet | all] [login | enable] [default | method_list_name <string 15>]**
Description	The **config authen application** command configures Switch applications (console, Telnet, SSH) for login at the user level and at the administration level (*authen_enable*), utilizing a previously configured method list.
Parameters	*application* – Specifies the application to configure. One of the following four options may be selected: • *console* – Configures the command line interface login method. • *http* – Configures the http login method. • *ssh* – Configures the Secure Shell login method. • *telnet* – Configures the telnet login methods. • *all* – Configures all applications as (console, Telnet, SSH) login methods.

	login – Configures an application for normal login on the user level, using a previously configured method list. *enable* – Configures an application for upgrading a normal user level to administrator privileges, using a previously configured method list. *default* – Configures an application for user authentication using the default method list. *method_list_name* <*string 15*> – Configures an application for user authentication using a previously configured *method_list_name*.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the default method list for the command line interface:

```
DGS-2000-28MP:5# config authen application http login default
Command: config authen application http login default


Success.
DGS-2000-28MP: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	Only Administrator-level users can issue this command.

Example usage:

To display the login and enable method list for all applications on the Switch:

```
DGS-2000-28MP:5# show authen application
Command: show authen application


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

DGS-2000-28MP:5#
```

config authen parameter

Purpose	To provide 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 Provides user to configure the authentication parameters on the Switch.
Parameters	*attempt <integer 1-255>* – Specifies the attempt of authentication parameter on the Switch. The value range is between 1 and 255. *response_timout <integer 0-255>* – Specifies the response timout of authentication parameter on the Switch. The value range is between 0 and 255.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the default method list for the command line interface:

```
DGS-2000-28MP:5# config authen parameter attempt 10
Command: config authen parameter attempt 10


Success.
DGS-2000-28MP: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	Only Administrator-level users can issue this command.

Example usage:

To display the authentication parameters for all applications on the Switch:

```
DGS-2000-28MP:5# show authen parameter
Command: show authen parameter

Response Timeout : 30 seconds
User Attempts    : 3
DGS-2000-28MP:5#
```

create authen server_host

Purpose	To create an authentication server host.
Syntax	**create authen server_host [<ipaddr> | ipv6address <ipv6addr>]**

	protocol [radius | tacacs+] { acct_port <int 1-65535> | port <int 1-65535> | encryption_key <string 800> | key [<string 254> | none] | timeout <int 1-255> | retransmit <int 1-255>}
Description	The **create authen server_host** command creates an authentication server host for the TACACS+/RADIUS security protocols on the Switch. When a user attempts to access the Switch with authentication protocol enabled, the Switch sends authentication packets to a remote TACACS+/RADIUS server host on a remote host. The TACACS+/RADIUS server host then verifies or denies the request and returns the appropriate message to the Switch. More than one authentication protocol can be run on the same physical server host but, remember that TACACS+/RADIUS are separate entities and are not compatible with each other. The maximum supported number of server hosts is 16.
Parameters	*[<ipaddr> | ipv6address <ipv6addr>]* – The IPv4 or IPv6 address of the remote server host to add. *protocol* – The protocol used by the server host. The options are: • *tacacs+* – Specifies that the server host utilizes the TACACS+ protocol. • *radius* – Specifies that the server host utilizes the RADIUS protocol. *acct_port <int 1-65535>* - Specifies the accepted port number of the authentication protocol on a server host. *port <int 1-65535>* – The virtual port number of the authentication protocol on a server host. The value must be between 1 and 65535. The default port number is 49 for TACACS/TACACS+ servers and 1812 and 1813 for RADIUS servers but the user may set a unique port number for higher security. *encryption_key <string 800>* - Specifies the encryption key. *key [<string 254> | none]* – The authentication key to be shared with a configured TACACS+ or RADIUS server only. The value is a string of up to 254 alphanumeric characters, or *none*. *timeout <int 1-255>* – The time in seconds the Switch waits for the server host to reply to an authentication request. The default value is 5 seconds. *retransmit <int 1-255>* – The number of times the device resends an authentication request when the server does not respond. The value is between 1 and 255. This field is inoperable for the TACACS+ protocol.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To create a TACACS+ authentication server host, with port number 1234, a timeout value of 10 seconds and a retransmit count of 5.

DGS-2000-28MP:5# create authen server_host 10.1.1.121 protocol tacacs+ port 1234 timeout 10 retransmit 5

Command: create authen server_host 10.1.1.121 protocol tacacs+ port 1234 timeout 10 retransmit 5

Key is empty for TACACS+ or RADIUS.

Retransmit is meaningless for TACACS+.

Success.

DGS-2000-28MP:5#

config authen server_host

Purpose	To configure a user-defined authentication server host.
Syntax	**config authen server_host [<ipaddr> | ipv6address <ipv6addr>] protocol [tacacs+ | radius] {acct_port <int 1-65535> | port <int 1-65535> | encryption_key <string 800> | key [<string 254> | none] | timeout <int 1-255> | retransmit <int 1-255>}**
Description	The **config authen server_host** command configures a user-defined authentication server host for the TACACS+/RADIUS security protocols on the Switch. When a user attempts to access the Switch with the authentication protocol enabled, the Switch sends authentication packets to a remote TACACS+/RADIUS server host on a remote host. The TACACS+/RADIUS server host then verifies or denies the request and returns the appropriate message to the Switch. More than one authentication protocol can be run on the same physical server host but, remember that TACACS+/RADIUS are separate entities and are not compatible with each other. The maximum supported number of server hosts is 16.
Parameters	*[<ipaddr> | ipv6address <ipv6addr>]* – The IPv4 or IPv6 address of the remote server host the user wishes to alter. *protocol* – The protocol used by the server host. The options are: • *tacacs+* – Specifies that the server host utilizes the TACACS+ protocol. • *radius* – Specifies that the server host utilizes the RADIUS protocol. *acct_port <int 1-65535>* - Specifies the accepted port number of the authentication protocol on a server host. *port <int 1-65535>* – The virtual port number of the authentication protocol on a server host. The value must be between 1 and 65535. The default port number is 49 for TACACS/TACACS+ servers and 1812 and 1813 for RADIUS servers but the user may set a unique port number for higher security. *encryption_key <string 800>* - Specifies the encryption key. *key [<string 254> | none]* – The authentication key to be shared with a configured TACACS+ or RADIUS server only. The value is a string of up to 254 alphanumeric characters, or none. *timeout <int 1-255>* – The time in seconds the Switch waits for the server host to reply to an authentication request. The default value is 5 seconds.

	retransmit <int 1-255> – The number of times the device resends an authentication request when the server does not respond. The value is between 1 and 255. This field is inoperable for the TACACS+ protocol.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure a TACACS+ authentication server host, with port number 4321, a timeout value of 12 seconds and a retransmit count of 4.

```
DGS-2000-28MP:5# config authen server_host 10.1.1.121 protocol tacacs+ port 4321 timeout 12 retransmit 4
Command: config authen server_host 10.1.1.121 protocol tacacs+ port 4321 timeout 12 retransmit 4

Retransmit is meaningless for TACACS+.

Success.
DGS-2000-28MP:5#
```

delete authen server_host

Purpose	To delete a user-defined authentication server host.
Syntax	**delete authen server_host [<ipaddr> | ipv6address <ipv6addr>] protocol [tacacs+ | radius]**
Description	The **delete authen server_host** command deletes a user-defined authentication server host previously created on the Switch.
Parameters	*server_host [<ipaddr> | ipv6address <ipv6addr>]* - The IPv4 or IPv6 address of the remote server host to be deleted. *protocol* – The protocol used by the server host the user wishes to delete. The options are: • *tacacs+* – Specifies that the server host utilizes the TACACS+ protocol. • *radius* – Specifies that the server host utilizes the RADIUS protocol.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete a user-defined RADIUS authentication server host:

```
DGS-2000-28MP:5# delete authen server_host 10.1.1.121 protocol radius
Command: delete authen server_host 10.1.1.121 protocol radius

Success.
DGS-2000-28MP:5#
```

show authen server_host

Purpose	To view a user-defined authentication server host.

Syntax	**show authen server_host**
Description	The **show authen server_host** command displays user-defined authentication server hosts previously created on the Switch. The following parameters are displayed: *IP Address* – The IP address of the authentication server host. *Protocol* – The protocol used by the server host. Possible results include TACACS+ or RADIUS. *Port* – The virtual port number on the server host. The default value is 49. *Timeout* - The time in seconds the Switch waits for the server host to reply to an authentication request. *Retransmit* - The value in the retransmit field denotes how many times the device resends an authentication request when the TACACS server does not respond. This field is inoperable for the tacacs+ protocol. *Key* - Authentication key to be shared with a configured TACACS+ server only.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To view authenticaion server hosts currently set on the Switch:

```
DGS-2000-28MP:5# show authen server_host
Command: show authen server_host


IP Address     Protocol   Port   Timeout  Retransmit  Key
---------------  --------------  ------  ------------ ----- ----------  --------------------

10.1.1.121      tacacs+    4321    ------       -1


Total Entries : 1

DGS-2000-28MP: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-level users can issue this command.

Example usage:

To create a server group “dlinkgroup”:

```
DGS-2000-28MP:5# create authen server_group dlinkgroup
Command: create authen server_group dlinkgroup


Success.
DGS-2000-28MP:5#
```

config authen server_group

Purpose	To configure a user-defined authentication server host.
Syntax	**config authen server_group [<string 15> | radius | tacacs+] [add | delete] server_host [<ipaddr> | ipv6address <ipv6addr>] protocol [radius | tacacs+]**
Description	The **config authen server_ group** command configures a user-defined authentication server group for the TACACS+/RADIUS security protocols on the Switch. When a user attempts to access the Switch with the authentication protocol enabled, the Switch sends authentication packets to a remote TACACS+/RADIUS server group on a remote host. The TACACS+/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 TACACS+/RADIUS are separate entities and 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. *server_host [<ipaddr> | ipv6address <ipv6addr>]* – The IPv4 or IPv6 address of the remote server group the user wishes to alter. *[add | delete]* –Specifies the authentication server host will be add or deleted of the server group. *protocol* – The protocol used by the server host. The options are: • *tacacs+* – Specifies that the server host utilizes the TACACS+ protocol. • *radius* – Specifies that the server host utilizes the RADIUS protocol.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure a RADIUS authentication server group:

```
DGS-2000-28MP:5# config authen server_group dlinkgroup add server_host 10.1.1.121 protocol radius
Command: config authen server_group dlinkgroup add server_host 10.1.1.121 protocol radius

Success.
DGS-2000-28MP:5#
```

delete authen server_group	
Purpose	To delete a user-defined authentication server host.
Syntax	**delete authen server_group <string 15>**
Description	The **delete authen 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-level users can issue this command.

Example usage:

To delete a user-defined rd1 authentication server group:

```
DGS-2000-28MP:5# delete authen server_group dlinkgroup
Command: delete authen server_group dlinkgroup


Success.
DGS-2000-28MP:5#
```

show authen server_group	
Purpose	To view a user-defined authentication server host.
Syntax	**show authen server_group {<string 15>}**
Description	The **show authen 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. Possible results include TACACS+ or RADIUS.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To view authenticaion server hosts currently set on the Switch:

```
DGS-2000-28MP:5# show authen server_group dlinkgroup
Command: show authen server_group dlinkgroup

(1) Group Name: dlinkgroup

  (No servers in this group)


Total Entries : 1
DGS-2000-28MP:5#
```

enable admin

Purpose	To promote user level privileges 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, 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-2000-28MP:5# enable admin
Command: enable admin

Success.
DGS-2000-28MP:5#
```

config admin local_enable

Purpose	To configure the local_enable password for administrator level privileges.
Syntax	**config admin local_enable**
Description	The **config admin local_enable** command changes the locally enabled password for the **local_enable admin** command. When a user chooses the '*local_enable*' method to promote user level privileges to administrator privileges, the user is prompted to enter the password configured here. After entering the **config admin local_enable** command, the user is

	prompted to enter the old password then a new password in a string of no more than 15 alphanumeric characters, and finally prompted to enter the new password again for confirmation. See the example below.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure the password for the 'local_enable' authentication method:

```
DGS-2000-28MP:5# config admin local_enable
Command: config admin local_enable

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

DGS-2000-28MP:5#
```

36

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 >]] [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	*hibernation* – Configure the hibernation state to enable or disable. The default value is disabled. *led* – Configure the led state to enable or disable. The default value is disabled. *length_detection* – Configure the length detection state to enable or disable. The default value is disabled. *port* – Configure ports state to be enabled or disabled. *[enable* | *disable]* – Enable or disable the power saving feature.
Restrictions	Only Administrator or operator–level users can issue this command.

Example usage:

To configure the power saving mode on the switch:

```
DGS-2000-28MP:5#  config power_saving mode port hibernation enable
Command: config power_saving mode port hibernation enable


Success.
DGS-2000-28MP:5#
```

config power_saving

Purpose	To configure the power saving on the switch.
Syntax	**config power_saving [hibernation | led [all | <portlist >] | 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	hibernation – Configure the hibernation. *led [all | <portlist >]* – Configure the ports for led. *port* – Configure ports. *[add | delete]* – Add or delete time range for power saving mode. *time_range1 <range_name 20>* – Specifies the time range 1 to be configured. *time_range2 <range_name 20>* – Specifies the time range 2 to be configured. *{clear_time_range}* – Clear the time range setting for power saving on the Switch.
Restrictions	Only Administrator or operator–level users can issue this command.

Example usage:

To configure the power saving on the switch:

```
DGS-2000-28MP:5#  config power_saving mode port hibernation enable
Command: config power_saving mode port hibernation enable

Success.
DGS-2000-28MP: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	hibernation – Display the hibernation state. *led* –Display the led state. *length_detection* –Display the length detection state. *port* –Display ports state.
Restrictions	None.

Example usage:

To display power saving information on the switch:

```
DGS-2000-28MP:5#  show power_saving length_detection
Command: show power_saving length_detection

Length Detection State   : Enabled
DGS-2000-28MP:5#
```

37

ENERGY EFFICIENT ETHERNET COMMANDS

The Energy Efficient Ethernet (EEE) commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameter
config EEE port	[all | <portlist>] state [enable | disable]
show EEE_mode	{ports <portlist>}

Each command is listed in detail, as follows:

config EEE port

Purpose	To enable or disable the EEE function on the specified port(s) on the Switch.
Syntax	**config EEE port [all | <portlist>] state [enable | disable]**
Description	The **config EEE port** command is used to enable or disable the EEE function on the specified port(s) on the Switch. Energy Efficient Ethernet (EEE) is a mechanism the helps to save energy by automatically detect for cable length.
Parameters	*[all* | <*portlist*> - A range of ports or all ports to be configured. *[enable* | *diable]* – Specifies to enable or disable the EEE function for the specified ports.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To enable the EEE function of ports 1-5:

```
DGS-2000-28MP:5# config EEE port 1-5 state enable
Command: config EEE port 1-5 state enable



Success.

DGS-2000-28MP:5#
```

show EEE_mode port

Purpose	To display the EEE function state on the specified port(s).
Syntax	**show EEE_mode {ports <portlist>}**
Description	The **show EEE_mode port** command is used to display the EEE function state on the specified port(s).
Parameters	<*portlist*> - A range of ports or all ports to be displayed.

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

Example usage:

To display the EEE state:

```
DGS-2000-28MP:5# show EEE_mode ports 1-3
Command: show EEE_mode ports 1-3


Port  EEE state
----  ---------
1     Enabled
2     Enabled
3     Enabled


Success.

DGS-2000-28MP:5#
```

38

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>
config lldp notification_interval	<sec 5-3600>
show lldp	
show lldp ports	{<portlist>}
show lldp local_ports	{<portlist>} {mode[brief | normal | detailed]}
show lldp remote_ports	{<portlist>} {mode[brief | normal | detailed]}
config lldp ports	[<portlist> | all] notification [enable | disable]
config lldp ports	[<portlist> | all] admin_status [tx_only | rx_only | tx_and_rx | disable]
config lldp ports	[<portlist>|all] mgt_addr [ipv4 <ipaddr> | ipv6 <ipv6addr>] state [enable | disable]
config lldp ports	[<portlist>|all] basic_tlvs [all | {port_Description | system_name | system_Description | system_capabilities}] [enable | disable]
config lldp ports	[<portlist>|all] dot3_tlvs [all | link aggregation | mac_phy_configuration_status | maximum_frame_size | power_via_mdi] [enable | disable]
config lldp ports	[<portlist>|all] dot1_tlv_pvid [disable | enable]
config lldp ports	[<portlist>|all] dot1_tlv_protocol_identity [all | eapol | gvrp | lacp | stp][disable | enable]
config lldp ports	[<portlist>|all] dot1_tlv_vlan_name [vlan <vlan_name 32> | vlanid <vidlist>] [disable | enable]
config lldp ports	{all | <portlist>} power_pse_tlv {enable | disable}
show lldp mgt_addr	{ipv4 <ipaddr> | ipv6 <ipv6addr>}
show lldp statistics	{ports <portlist>}
show lldp power_pse_tlv	

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 *Link Layer Discovery Protocol* (LLDP) on the switch.
Parameters	None.
Restrictions	Only Administrator or operator–level users can issue this command.

Example usage:

To enable LLDP on the switch:

```
DGS-2000-28MP:5# enable lldp
Command: enable lldp

Success.
DGS-2000-28MP:5#
```

disable lldp

Purpose	To disable LLDP on the switch.
Syntax	**disable lldp**
Description	The disable **lldp** command disables the *Link Discovery Protocol* (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-2000-28MP:5# disable lldp
Command: disable lldp

Success.
DGS-2000-28MP: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-2000-28MP:5# config lldp message_tx_interval 10
Command: config lldp message_tx_interval 10

Success.

DGS-2000-28MP: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 *Link Layer Discovery Protocol* (LLDP) packet before discarding it.
Parameters	*message_tx_hold_multiplier (int 2-10)* – Specifies the hold time to be sent in the LLDP update packets as a multiple of the timer value. (Range: 2-10). The default configuration is 4.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure LLDP Message tx hold multiplier settings:

```
DGS-2000-28MP:5# config lldp message_tx_hold_multiplier 2
Command: config lldp message_tx_hold_multiplier 2

Success.

DGS-2000-28MP:5#
```

config lldp reinit_delay

Purpose	To define the lldp reinint–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-2000-28MP:5# config lldp reinit_delay 1
Command: config lldp reinit_delay 1


Success.

DGS-2000-28MP: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-2000-28MP:5# config lldp tx_delay 1
Command: config lldp tx_delay 1


Success.

DGS-2000-28MP:5#
```

config lldp notification_interval

Purpose	To configure the timer of the notification interval used to send notifications to configured SNMP trap receiver(s).
Syntax	**config lldp notification_interval <sec 5-3600>**
Description	The **config lldp notification_interval** command globally changes the interval between successive LLDP change notifications generated by the switch.
Parameters	*<sec 5-3600>* – The range is from 5 second to 3600 seconds. The default setting is 5 seconds.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To change the notification interval:

```
DGS-2000-28MP:5# config lldp notification_interval 10
Command: config lldp notification_interval 10


Success.

DGS-2000-28MP:5#
```

show lldp

Purpose	To display the *Link Layer Discovery Protocol* (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-2000-28MP:5# show lldp
Command: show lldp

LLDP System Information
   Chassis Id Subtype       : MAC Address
   Chassis Id               : 00-12-10-28-33-95
   System Name              :
   System Description       : DGS-2000-28MP        7.01.B030
   System Capabilities      : Bridge

LLDP Configurations
   LLDP Status              : Enable
   Message Tx Interval      : 30
   Message Tx Hold Multiplier: 4
   ReInit Delay             : 2
   Tx Delay                 : 2
   Notification Interval    : 5

DGS-2000-28MP:5#
```

show lldp ports

Purpose	To display the *Link Layer Discovery Protocol* (LLDP) ports configuration on the switch.
Syntax	**show lldp ports {<portlist>}**
Description	The **show lldp ports** command displays the information regarding the ports.
Parameters	<*portlist*> − A port or range of ports to be displayed.
Restrictions	None.

Example usage:

To show the information for port 1:

```
DGS-2000-28MP:5# show lldp ports 1

Port ID                    : 1
------------------------------------------------------------------------------
Admin Status               : TX_and_RX
Notification Status        : Disable
Advertised TLVs Option  :
   Port Description                                  Disable
   Port Description                                  Disable
   Port Description                                  Disable
   Port Description                                  Disable
   Enabled Management Address
      (NONE)
   Port VLAN ID                                      Disable
   Enabled Port_and_Protocol_VLAN_ID
      (None)
   Enabled VLAN Name
      (None)
   Enabled Protocol_Identity
      (None)
   MAC/PHY Configuration/Status                      Disable
   Power Via MDI                                     Disable
   Link Aggregation                                  Disable
   Maximum Frame Size                                Disable

DGS-2000-28MP:5#
```

show lldp local_ports

Purpose	To display the *Link Layer Discovery Protocol* (LLDP) configuration that is advertised from a specific port.
Syntax	**show lldp local_ports {<portlist>} {mode[brief | normal | detailed]}**
Description	The **show lldp local_ports** command displays the configuration that is advertised from a specific port.
Parameters	*<portlist>* − A port or range of ports to be displayed. *{mode[brief | normal | detailed]}* − defines which mode of information want to be displayed, brief, normal or detailed.
Restrictions	None.

Example usage:

To show the local port information for port 1 with mode brief:

```
DGS-2000-28MP:5# show lldp local_ports 1 mode brief
Command: show lldp local_ports 1 mode brief

Port ID : 1
------------------------------------------------
Port ID Subtype          : Local
Port ID                  : Slot0/1
Port ID Desctiption      : D-Link DGS-2000-28X Rev.B1/7.00.B055 Port 1


DGS-2000-28MP:5#
```

show lldp remote_ports

Purpose	To display information regarding the neighboring devices discovered using LLDP.
Syntax	**show lldp remote_ports {<portlist>} {mode[brief | normal | detailed]}**
Description	The **show lldp remote_ports command** displays the information regarding neighboring devices.
Parameters	*<portlist>* − A port or range of ports to be displayed. *[mode[brief | normal | detailed]}* − defines which mode of information want to be displayed, brief, normal or detailed.
Restrictions	None.

Example usage:

To show the information for remote ports:

```
DGS-2000-28MP: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-2000-28MP:5#
```

config lldp ports

Purpose	To enable LLDP notification on a port or ports.
Syntax	**config lldp ports [<portlist> | all] notification [enable | disable]**
Description	The **config lldp ports** notification command defines lldp notification per port on the switch.
Parameters	*ports [<portlist> | all]* – Specify a port or ports to be configured. *notification [enable | disable]*– defines is notification is enabled or disabled.
Restrictions	None.

Example usage:

To configure LLDP notification:

```
DGS-2000-28MP:5# config lldp ports 1-3 notification enable
Command: config lldp ports 1-3 notification enable


Success.

DGS-2000-28MP:5#
```

config lldp ports

Purpose	To define LLDP admin status on a port or ports.

Syntax	**config lldp ports [<portlist> | 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	*[<portlist> | all]* – Specify a port or ports to be configured. *Admin status* – Defines admin status of ports on the switch. Tx- Tx only. Rx – Rx only. Both – Tx and RX. Disable – admin status disabled.
Restrictions	None.

Example usage:

To configure LLDP admin status

```
DGS-2000-28MP:5# config lldp ports 2 admin_status disable
Command: config lldp ports 2 admin_status disable


Success.

DGS-2000-28MP:5#
```

config lldp ports

Purpose	To define LLDP management address advertisement on a port or ports.
Syntax	**config lldp ports [<portlist>|all] mgt_addr [ipv4 {<ipaddr>| auto} | ipv6 <ipv6addr>] [enable | disable]**
Description	The **config lldp ports** mgt_addr command defines if lldp will advertise the switch's IP address the command is per port on the switch.
Parameters	*[<portlist> | all]* – Specify a port or ports to be configured. *mgt_addr* - The port types specified for advertising indicated management address instance *ipv4* –Specify the IP address of IPv4 <*ipaddr*> - Specify the IP address of IPv4. *auto* – Automactically use the current interface IP address. *ipv6* - Specify the IP address of IPv6. <*ipv6addr*> - Specify the IP address of IPv6.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure LLDP management address advertisement:

```
DGS-2000-28MP: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-2000-28MP:5#
```

config lldp ports

Purpose	To define LLDP management basic TLVs advertisement on a port or ports.
Syntax	**config lldp ports [<portlist>|all] basic_tlvs [all | {port_description | system_name | system_description | system_capabilities}] [enable | disable]**
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	*[<portlist> | all]* – Specify a port or ports to be configured. *Basic TLVs:* *all* – Advertisement of all the basic TLVs *port description* – Advertisement of dort description *system name* – Advertisement of system name *system description* – Advertisement of system description *system capabilities* – Advertisement of system capabilities
Restrictions	None.

Example usage:

To configure LLDP Basis TLVs

```
DGS-2000-28MP:5# config lldp ports 1 basic_tlvs all enable
Command: config lldp ports 1 basic_tlvs all enable


Success.

DGS-2000-28MP: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 | power_via_mdi] [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	*[<portlist> | all]* – Specify a port or ports to be configured. *dot3_tlvs* – defines if the advertisement is enabled or disabled. The possible values are: link_aggregation, mac_phy_configuration_status, maximum_frame_size, power_via_mdi or all.

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

Example usage:

To configure LLDP mac_phy_configuration status:

```
DGS-2000-28MP:5# config lldp ports 2 dot3_tlvs mac_phy_configuration_status enable
Command: config lldp ports 2 dot3_tlvsmac_phy_configuration_status enable


Success.

DGS-2000-28MP:5#
```

config lldp ports

Purpose	To define LLDP management basic TLVs advertisement on a port or ports.
Syntax	**config lldp ports [<portlist>|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	*[<portlist> | all]* – Specify a port or ports to be configured. *[enable | disable]* - 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-2000-28MP:5# config lldp ports all dot1_tlv_pvid disable
Command: config lldp ports all dot1_tlv_pvid disable


Success.

DGS-2000-28MP:5#
```

config lldp ports

Purpose	To define LLDP management basic TLVs advertisement on a port or ports.
Syntax	**config lldp ports [<portlist>|all] dot1_tlv_protocol_identity [all | eapol | gvrp | lacp | stp][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	*[<portlist> | all]* – Specify a port or ports to be configured. *dot1_tlv_protocol_identity* − Defines if the advertisement is enabled or disabled. The possible values are: eapol, gvrp, lacp, stp or all.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure LLDP ports configuration status:

```
DGS-2000-28MP:5# config lldp ports all dot1_tlv_protocol_identity eapol enable
Command: config lldp ports all dot1_tlv_protocol_identity eapol enable


Success.

DGS-2000-28MP:5#
```

config lldp ports	
Purpose	To define LLDP management basic TLVs advertisement on a port or ports.
Syntax	**config lldp ports [<portlist>|all] dot1_tlv_vlan_name [vlan <vlan_name 32> | vlanid <vidlist>] [disable | enable]**
Description	The **config lldp ports** dot1 TLVs command defines lldp admin status per port on the switch.
Parameters	*[<portlist> | all]* – Specify a port or ports to be configured. *vlan <vlan_name 32>* –The name of the VLAN to be configured. *dot1_tlv_vlan_name* − Defines if the advertisement is enabled or disabled. *vlanid <vidlist>* –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-2000-28MP: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-2000-28MP:5#
```

config lldp ports	
Purpose	To define LLDP management basic TLVs advertisement on a port or ports.
Syntax	**config lldp ports [all | <portlist>] dot1_tlv_protocol_vid [vlan {all | <vlan_name (20)>} | vlanid <vidlist>} [enable | disable]**
Description	The **config lldp ports** dot1 TLVs command defines lldp admin status per port on the switch.
Parameters	*[<portlist> | all]* – Specify a port or ports to be configured. *vlan <vlan_name 32>* –The name of the VLAN to be configured. *dot1_tlv_protocol_vid* − This TLV optional data type determines whether the IEEE 802.1 organizationally defined port and protocol VLAN ID TLV transmission is allowed on a given LLDP transmission capable port. *vlan* –Specify a VLAN to be transmitted. *all* –Specify that all VLAN names will be transmitted <*vlan_name 32*> - Specify a VLAN name to be transmitted. *vlanid <vidlist>* –The vid of the VLAN to be configured. *enable* – Enable configuration of an individual port or group of ports *disable* - Disable configuration of an individual port or group of ports
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure dot1_tlv_protocol_vid on all ports:

```
DGS-2000-28:5# config lldp ports all dot1_tlv_protocol_vid vlan all enable
Command: config lldp ports all dot1_tlv_protocol_vid vlan all enable


Success.
```

config lldp ports	
Purpose	To define LLDP management basic TLVs advertisement on a port or ports.
Syntax	**config lldp ports {all | <portlist>} power_pse_tlv {enable | disable}**
Description	The **config lldp ports** power_pse TLVs command defines lldp power PSE admin status per port on the switch.
Parameters	*enable* – Enable configuration of an individual port or group of ports *disable* - Disable configuration of an individual port or group of ports
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To turn on LLDP power_pse_tlv on all ports:

```
DGS-2000-28MP:5# config lldp ports all power_pse_tlv enable
Command: config lldp ports all power_pse_tlv enable


Success.

DGS-2000-28MP:5#
```

show lldp mgt_addr	
Purpose	To display the *Link Layer Discovery Protocol* (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	*ipv4* <*ipaddr*> | *ipv6* <*ipv6addr*> **–** Specifies the lldp IPv4 or IPv6 address to be displayed.
Restrictions	None.

Example usage:

To show the LLDP management address advertisement:

```
DGS-2000-28MP: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)


Total Address : 1

DGS-2000-28MP:5#
```

show lldp statistics

Purpose	To display the *Link Layer Discovery Protocol* (LLDP) statistics for the specified ports.
Syntax	**show lldp statistics {ports <portlist>}**
Description	The **show lldp statistics** command displays the statistics of LLDP on the Switch.
Parameters	*ports <portlist>* **–** Specifies the ports to be displayed.
Restrictions	None.

Example usage:

To show the LLDP statistics for port 15:

```
DGS-2000-28MP:5# show lldp statistics ports 15
Command: show lldp statistics ports 15

Port ID : 15
------------------------------------------------------------------
lldpStatsTxPortFramesTotal              : 0
lldpStatsRxPortFramesDiscardedTotal  : 0
lldpStatsRxPortFramesErrors             : 0
lldpStatsRxPortFramesTotal              : 0
lldpStatsRxPortTLVsDiscardedTotal      : 0
lldpStatsRxPortTLVsUnrecognizedTotal : 0
lldpStatsRxPortAgeoutsTotal             : 0

DGS-2000-28MP:5#
```

show lldp power_pse_tlv

Purpose	To display the *Link Layer Discovery Protocol* (LLDP) powers.
Syntax	**show lldp power_pse_tlv**
Description	The **show lldp power_pse_tlv** command displays the power of LLDP on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To show the LLDP power PSE status:

```
DGS-2000-28MP:5# show lldp power_pse_tlv
Command: show lldp power_pse_tlv


Port         State
---------------------------------------
1            Disable
2            Disable
3            Disable
4            Disable
DGS-2000-28MP:5#
```

39

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 > forward_list [null | <portlist >]
show traffic_ segmentation	{<portlist >}

Each command is listed in detail, as follows:

config traffic_segmentation	
Purpose	To configure traffic segmentation on the Switch.
Syntax	**config traffic_segmentation <portlist > forward_list [null | <portlist >]**
Description	The **config traffic_segmentation** command configures traffic segmentation on the Switch.
Parameters	*<portlist >* – A port or a port channel for which the current traffic segmentation configuration on the Switch is to be displayed. *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-2000-28MP:5# config traffic_segmentation 1-3 forward_list 5
Command: config traffic_segmentation 1-3 forward_list 5

Success.
DGS-2000-28MP:5#
```

show traffic_segmentation	
Purpose	To display the current traffic segmentation configuration on the Switch.
Syntax	**show traffic_segmentation {<portlist >}**
Description	The **show traffic_segmentation** command displays the current traffic segmentation configuration on the Switch.
Parameters	*<portlist >* – A port or a port channel for which the current traffic segmentation configuration on the Switch is to be displayed.
Restrictions	None.

Example usage:

To display the current traffic segmentation configuration on the Switch:

```
DGS-2000-28MP:5#  show traffic_segmentation
Command: show traffic_segmentation


Traffic Segmentation Table

Port Forward Portlist
------ ----------------------
1
2
3
4
5
6
7
8
9
10

DGS-2000-28MP:5#
```

40

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 >] mode [active | passive]
config ethernet_oam ports (state)	[all | <portlist >] state [enable | disable]
config ethernet_oam ports (remote loopback)	[all | <portlist >] remote_loopback [start | stop]
config ethernet_oam ports (received remote loopback)	[all | <portlist >] received_remote_loopback [process | ignore]
config ethernet_oam ports (link monitor error symbol)	[all | <portlist >] 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 >] 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 >] 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 >] link_monitor error_frame_period {threshold < integer 1-4294967295> | window < integer 148810-100000000> | notify_state [enable | disable]}
config ethernet_oam remote-loopback port	<port> {test | count <integer1-1000> | packet <integer 64-1500> | pattern <hex_str> | wait-time <integer 1-10>}
config ethernet_oam ports	[<portlist> | all] critical_link_event critical_event notify_state [enable | disable]
show ethernet_oam port	<port> remote-loopback [current-session | last-session] {detail}
show ethernet_oam ports (status)	[all | <portlist >] status
show ethernet_oam ports (configuration)	[all | <portlist >] configuration
show ethernet_oam ports (statistics)	[all | <portlist >] statistics
show ethernet_oam	[all | <portlist >] event_log {index <value_list}

Command	Parameter
ports (event log)	
clear ethernet_oam ports	[all | <portlist >] [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 >] 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	The command is used to configure Ethernet OAM for ports to operate in active or passive mode. Port configured in *active* mode: (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. Port configured in *passive* mode: (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-2000-28MP:5#  config ethernet_oam ports 1 mode passive
Command: config ethernet_oam ports 1 mode passive

Success.
DGS-2000-28MP:5#
```

config ethernet_oam ports (state)	
Purpose	Used to enable or disable Ethernet OAM per port.
Syntax	**config ethernet_oam ports [all | <portlist >] state [enable | disable]**
Description	The **config ethernet_oam ports** command is used to enable or disable Ethernet OAM function on a per port basis. 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.
Parameters	*[all | <portlist >]* – Specifies a range of ports or all ports to be configured. *state [enable | disable]* – Specify to enable or disable the OAM function for the listed ports. The default state is disabled.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To enable Ethernet OAM on port 1:

```
DGS-2000-28MP:5#  config ethernet_oam ports 1 state enable
Command: config ethernet_oam ports 1 state enable

Success.
DGS-2000-28MP: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 >] 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	*[all | <portlist >]* – Specifies a range of ports or all ports to be configured. *remote_loopback [start | stop]* – 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-2000-28MP:5#  config ethernet_oam ports 1 remote_loopback start
Command: config ethernet_oam ports 1 remote_loopback start

Success.
DGS-2000-28MP: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 >] 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, thus it continues to process user traffic regardless.
Parameters	*[all* | *<portlist >]* – Specifies a range of ports or all ports to be configured. *received_remote_loopback [process* | *ignore]* – Specify 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-2000-28MP:5#  config ethernet_oam ports 1 received_remote_loopback process
Command: config ethernet_oam ports 1 received_remote_loopback process

Success.
DGS-2000-28MP: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 >] 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	*[all | <portlist >]* – Specifies a range of ports or all ports to be configured. *threshold <integer>* – 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. *window <integer 1000-60000>* –The range is 1000 to 60000 ms. The default value is 1000ms. *notify_state [enable | disable]* – 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-2000-28MP: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-2000-28MP: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 >] link_monitor error_frame {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 error frames for ports. 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.
Parameters	*[all | <portlist >]* – Specifies a range of ports or all ports to be configured. *threshold <integer>* – 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. *window <integer 1000-60000>* –The range is 1000 to 60000 ms. The default value is 1000ms. *notify_state [enable | disable]* – 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-2000-28MP: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-2000-28MP: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 >] link_monitor error_frame_seconds {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 error frame seconds for ports. An error frame second is one second interval wherein at least one frame error was detected. 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.
Parameters	*[all | <portlist >]* – Specifies a range of ports or all ports to be configured. *threshold <integer>* – 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. *window <integer 1000-60000>* –Specify the period of error frame seconds summary event. The range is 1000ms-60000ms and the default value is 60000 ms. *notify_state [enable | disable]* – 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 seconds threshold to 2 and period to 10000 ms for port 1:

```
DGS-2000-28MP: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-2000-28MP: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 >] 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	*[all | <portlist >]* – Specifies a range of ports or all ports to be configured. *threshold <integer>* – 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. *window <integer 148810-100000000>* – Specify the period of error frame period event. The period is specified by a number of received frames. The default value is 148810. *notify_state [enable | disable]* – 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-2000-28MP: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-2000-28MP: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 >] status**
Description	The **show ethernet_oam ports** command is used to show primary controls and status information for Ethernet OAM on specified ports. The information includes: (1) **OAM administration status**: enabled or disabled (2) **OAM operation status. It maybe the below value**: □**Disable**: OAM is disabled on this port □**LinkFault**: The link has detected a fault and is transmitting OAMPDUs with a link fault indication. □**PassiveWait**: The port is passive and is waiting to see if the peer device is OAM capable. **ActiveSendLocal**: The port is active and is sending local information □**SendLocalAndRemote**: The local port has discovered the peer but has not yet accepted or rejected the configuration of the peer. □**SendLocalAndRemoteOk**: The local device agrees the OAM peer entity. □**PeeringLocallyRejected**: The local OAM entity rejects the remote peer OAM entity. □**PeeringRemotelyRejected**: The remote OAM entity rejects the local device. □**Operational**: The local OAM entity learns that both it and the remote OAM entity have accepted the peering. □**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. (3) **OAM mode**: passive or active (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. (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. (6) **OAM Functions Supported**: The OAM functions supported on this port. These functions include: □**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). □**Loopback**: It indicates that the OAM entity can initiate and respond to loopback commands. □**Link Monitoring**: It indicates that the OAM entity can send and receive Event Notification OAMPDUs. □**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. (7) **Loopback Status**: The current status of the loopback function of the port: □**No Loopback** – The local and remote ports are not in loopback

	mode. ☐**Initiating Loopback** – The local port has sent the start remote loopback request to the peer and is waiting for response. ☐**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. ☐**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. ☐**Terminate Loopback** - The port is stopping loopback on the port.
Parameters	*[all | <portlist >]* – 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-2000-28MP: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 >] configuration**
Description	The **show ethernet_oam ports** command is used to view Ethernet OAM configurations for ports.
Parameters	*[all | <portlist >]* – Specifies a range of ports or all ports to display status.

Restrictions	None.

Example usage:

To show Ethernet OAM configuration on port 3:

```
DGS-2000-28MP: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 >] statistics**
Description	The **show ethernet_oam ports** command is used to display Ethernet OAM ports statistics information.
Parameters	*[all* | *<portlist >]* – Specifies a range of ports or all ports to display status.
Restrictions	None.

Example usage:

To show Ethernet OAM statistics on port 2:

```
DGS-2000-28MP: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 OAMPDUs Tx       : 0
  Organization Specific OAMPDUs Rx       : 0
  Unsupported OAMPDU Tx                  : 0
  Unsupported OAMPDU Rx                  : 0
  Frames Lost Due To OAM                 : 0

DGS-2000-28MP:5#
```

show ethernet_oam ports (event log)

Purpose	Used to display Ethernet OAM event log.
Syntax	**show ethernet_oam ports [all | <portlist >] event_log {index <value_list>}**
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	*[all | <portlist >]* – Specifies a range of ports or all ports to display status. *index <value_list>* – Specifies an index range to display.
Restrictions	None.

Example usage:

To show Ethernet OAM event log on port 1:

```
DGS-2000-28MP: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-2000-28MP:5#
```

clear ethernet_oam ports

Purpose	Used to clear Ethernet OAM port statistics or event log.
Syntax	**clear ethernet_oam ports [all | <portlist >] [event_log| statistics]**
Description	The **clear ethernet_oam ports** command is used to clear Ethernet OAM ports statistics or event log information.
Parameters	*[all* | *<portlist>]* – Specifies a range of ports or all ports to clear OAM statistics or event log. *[event_log* | *statistics]*> – Specifies an index range to display.
Restrictions	None.

Example usage:

To clear port 1 OAM statistics:

```
DGS-2000-28MP:5#  clear ethernet_oam ports 1 statistics
Command: clear ethernet_oam ports 1 statistics

Success.
DGS-2000-28MP:5#
```

41

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	*state [enable* | *disable]* – 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-2000-28MP:5# config safeguard_engine state enable
Command: config safeguard_engine state enable

Success.
DGS-2000-28MP: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-2000-28MP:5#  show safeguard_engine
Command: show safeguard_engine

Safeguard Engine State        :   Enable

DGS-2000-28MP:5#
```

42

LINK AGGREGATION COMMANDS

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

Command	Parameter
create link_aggregation group_id	<value> ports <portlist> [type {lacp | static}]
delete link_aggregation group_id	<value>
config link_aggregation	{algorithm { mac_source | mac_destination | mac_source_dest | ip_source | ip_destination | ip_source_dest } | group_id <value> ports <portlist> | state {disable | enable} }
show link_aggregation	{algorithm | [group_id <value>]}
config lacp port_priority	<portlist> <value (0-65535)> [timeout {long | short}]
config lacp_ports	<portlist> mode {active | passive}
show lacp	

Each command is listed in detail, as follows:

create link_aggregation	
Purpose	To create a link aggregation group on the Switch.
Syntax	**create link_aggregation group_id <value> ports <portlist> [type {lacp | static}]**
Description	The **create link_aggregation** command creates a link aggregation group with a unique identifier.
Parameters	*group_id* <*value*> − Specifies the group ID. The Switch allows up to 8 link aggregation groups to be configured. The group number identifies each of the groups. *type* – Specify the type of link aggregation used for the group. If the type is not specified the default type is *static*. • *lacp* – This DGSignates the port group as LACP compliant. LACP allows dynamic adjustment to the aggregated port group. LACP compliant ports may be further configured (see config lacp_ports). LACP compliant must be connected to LACP compliant devices. The maximum ports that can be configure in the same LACP are 16. • *static* – This DGSignates the aggregated port group as static. Static port groups can not be changed as easily as LACP compliant port groups since both linked devices must be manually configured if the configuration of the trunked group is changed. If static link aggregation is used, be sure that both ends of the connection are properly configured and that all ports have the same speed/duplex settings. The maximum ports that can be configure in the same static LAG are 8

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

Example usage:

To create a link aggregation group:

```
DGS-2000-28MP:5# create link_aggregation group_id 5 ports 9-10 type lacp
Command: create link_aggregation group_id 5 ports 9-10 type lacp


Success.

DGS-2000-28MP:5#
```

delete link_aggregation

Purpose	To delete a previously configured link aggregation group.
Syntax	**delete link_aggregation group_id <value>**
Description	The **delete link_aggregation group_id** command deletes a previously configured link aggregation group.
Parameters	*group_id* <*value*> − Specifies the group ID. The Switch allows up to 8 link aggregation groups to be configured. The group number identifies each of the groups.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To delete link aggregation group:

```
DGS-2000-28MP:5# delete link_aggregation group_id 1
Command: delete link_aggregation group_id 1


LA channel 1 delete successful
DGS-2000-28MP:5#
```

config link_aggregation group_id

Purpose	To configure a previously created link aggregation group.
Syntax	**config link_aggregation {algorithm { mac_source | mac_destination | mac_source_dest | ip_source | ip_destination | ip_source_dest } | group_id <value> ports <portlist> | state {disable | enable} }**
Description	The **config link_aggregation** command configures the parameters related link aggregation feature, like hash algorithm and port members.
Parameters	<*value 1-8*> − Specifies the group ID. The Switch allows up to 8 link aggregation groups to be configured. The group number identifies each of the groups. *ip_source* − Indicates that the Switch should examine the IP source address. *ip_destination* − Indicates that the Switch should examine the IP destination address.

	ip_source_dest − Indicates that the Switch should examine the IP source and destination addresses. *mac_source* − Indicates that the Switch should examine the MAC source address. *mac_destination* − Indicates that the Switch should examine the MAC destination address. *mac_source_dest* − Indicates that the Switch should examine the MAC source and destination addresses.
Restrictions	Only administrator or operator-level users can issue this command. Link aggregation groups may not overlap.

Example usage:

To change the hash algorithm for link aggregation:

```
DGS-2000-28MP:5# config link_aggregation algorithm ip_source
Command: config link_aggregation algorithm ip_source

Success.

DGS-2000-28MP:5
```

config lacp port_priority

Purpose	To set the priority value of a physical port in an LACP group.
Syntax	**config lacp port_priority <portlist> <value 0-65535> [timeout <long | short>]**
Description	The **config lacp port_priority** command sets the LACP priority value and administrative timeout of a physical port or range of ports in an LACP group.
Parameters	<*portlist*> - A port or range of ports to be configured. <*value 0-65535*> - Specifies the LACP priority value for a port or range of ports to be configured. The default is 1. <*timeout*> - Specifies the administrative LACP timeout. • *long* – Specifies the LACP timeout to be 90 seconds. This is the default. • *short* – Specifies the LACP timeout to be 3 seconds.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure the LACP priority of ports 1-3:

```
DGS-2000-28MP:5# config lacp port_priority 1-3 100 timeout long
Command: config lacp port_priority 1-3 100 timeout long

Success.
DGS-2000-28MP:5#
```

config lacp_ports	
Purpose	To configure settings for LACP compliant ports.
Syntax	**config lacp_ports <portlist> mode [active | passive]**
Description	The **config lacp_ports** command is used to configure ports that have been previously DGSignated as LACP ports.
Parameters	<*portlist*> − Specifies a port or range of ports to be configured. *mode* – Select the mode to determine if LACP ports will process LACP control frames. • *active* – Active LACP ports are capable of processing and sending LACP control frames. This allows LACP compliant devices to negotiate the aggregated link so the group may be changed dynamically as needs require. In order to utilize the ability to change an aggregated port group, that is, to add or subtract ports from the group, at least one of the participating devices must DGSignate LACP ports as active. Both devices must support LACP. • *passive* – LACP ports that are DGSignated as passive cannot process LACP control frames. In order to allow the linked port group to negotiate adjustments and make changes dynamically, at one end of the connection must have “active” LACP ports (see above).
Restrictions	Only Administrator, operator or power user–level users can issue this command.

Example usage:

To configure LACP port mode settings:

```
DGS-2000-28MP:5# config lacp_ports 1 mode active
Command: config lacp_ports 1 mode active



Success.
DGS-2000-28MP:5#
```

show lacp	
Purpose	To display current LACP port mode settings.
Syntax	**show lacp {<portlist>}**
Description	The **show lacp** command displays the current LACP mode settings.
Parameters	<*portlist*> - A port or range of ports whose LACP settings are to be displayed. If no parameter is specified, the system displays the current LACP status for all ports.
Restrictions	None.

Example usage:

To display LACP information for port1~3:

```
DGS-2000-28MP:5# show lacp 1-3
Command: show lacp 1-3

Port  Priority  Activity  Timeout
----- --------  --------  --------------
1     100       Active    Long (90 sec)
2     100       Active    Long (90 sec)
3     100       Active    Long (90 sec)
DGS-2000-28MP:5#
```

43

VOICE VLAN COMMANDS

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

Command	Parameter
enable voice_vlan	{ vlanid <vlanid (1-4094)> | < vlan_name (20) > }
disable voice_vlan	
config voice_vlan aging_time	<integer (1-120)>
config voice_vlan priority	<integer (0-7)>
config voice_vlan oui	{ add <macaddr> description <string (20)> [mask <macmask>] | delete <macaddr> }
config voice_vlan ports	<portlist> auto dectection { enable { tag | untag } | disable }
config voice_vlan log state	{ enable | disable }
show voice_vlan	[{ oui | ports <portlist> | { { lldp_med voice_device | voice_device } { all | ports <portlist> } } }]

Each command is listed in detail, as follows:

enable voice_vlan	
Purpose	To assign the particular VLAN as Voice VLAN.
Syntax	**enable voice_vlan [vlanid <vlanid (1-4094)> | < vlan_name (20) >]**
Description	Voice VLAN is a VLAN used to carry voice traffic from IP phone. The quality of service (QoS) for voice traffic shall be configured higner than normal traffic to ensure the quality of sound.
Parameters	*<vlanid (1-4094)>* - Specifies all VLANs or VLAN id to be displayed. *<vlan_name>* - Specifies the name of VLAN
Restrictions	Only Administrator, operator or power user–level users can issue this command.

Example usage:

To assign the particular VLAN as Voice VLAN:

```
DGS-2000-28:5# create vlan vlanid 5
Command: create vlan vlanid 5

Success.
DGS-2000-28:5# enable voice_vlan vlanid 5
Command: enable voice_vlan vlanid 5

Success.
```

```
DGS-2000-28:5# show voice_vlan
Command: show voice_vlan

Voice VLAN State     : Enabled
Voice VLAN           : 5
Priority             : 5
Aging Time           : 1 hours
Log State            : Disabled
Member Ports         :
Dynamic Member Ports :

DGS-2000-28:5#
```

disable voice_vlan

Purpose	To disable Voice VLAN function.
Syntax	**disable voice_vlan**
Description	To disable Voice VLAN function
Parameters	None
Restrictions	Only Administrator, operator or power user–level users can issue this command..

config voice_vlan aging_time

Purpose	To specify the aging time of dynamic Voice VLAN member port.
Syntax	**config voice_vlan aging_time <integer (1-120)>**
Description	To specify the aging time of dynamic Voice VLAN member port
Parameters	*<integer (1-120)>* - in range of 1-120 hours
Restrictions	Only Administrator, operator or power user–level users can issue this command..

Example usage:

To specify the aging time of dynamic Voice VLAN member port:

```
DGS-2000-28:5# config voice_vlan aging_time 2
Command: config voice_vlan aging_time 2

Success.
DGS-2000-28:5# show voice_vlan
Command: show voice_vlan

Voice VLAN State     : Enabled
Voice VLAN           : 5
Priority             : 5
Aging Time           : 2 hours
Log State            : Disabled
Member Ports         :
Dynamic Member Ports :
```

```
DGS-2000-28:5#
```

config voice_vlan priority

Purpose	To specify the 802.1p priority value used in voice traffic.
Syntax	**config voice_vlan priority <integer (0-7)>**
Description	To specify the 802.1p priority value used in voice traffic.
Parameters	*<integer (0-7)>* - in range of 0-7 of 802.1p priority value
Restrictions	Only Administrator, operator or power user–level users can issue this command.

Example usage:

To specify the 802.1p priority value used in voice traffic:

```
DGS-2000-28:5# config voice_vlan priority 7
Command: config voice_vlan priority 7



Success.

DGS-2000-28:5# show voice_vlan
Command: show voice_vlan

Voice VLAN State     : Enabled
Voice VLAN           : 5
Priority             : 7
Aging Time           : 2 hours
Log State            : Disabled
Member Ports         : 8
Dynamic Member Ports : 1

DGS-2000-28:5#
```

config voice_vlan oui

Purpose	To specifiy the particular OUI (Organization Unique Indentifier) values for Voice VLAN auto detection feature.
Syntax	**config voice_vlan oui [add <macaddr> description <string (20)> { mask <macmask> } | delete <macaddr>]**
Description	To specifiy the particular OUI (Organization Unique Indentifier) values for Voice VLAN auto detection feature. The OUI can be determined as range list by configuring MAC mask.
Parameters	*<macaddr>* - To specify the MAC address either by XX:XX:XX:XX:XX:XX or XX-XX-XX-XX-XX-XX format *<macmask>* - To specify the mask of MAC address indentified
Restrictions	Only Administrator, operator or power user–level users can issue this command.

Example usage:

To specifiy the particular OUI (Organization Unique Indentifier) values for Voice VLAN auto detection feature:

```
DGS-2000-28:5# config voice_vlan oui add 00-12-34-00-00-00 description DLINK_TEST
Command: config voice_vlan oui add 00-12-34-00-00-00 description DLINK_TEST

Success.
DGS-2000-28:5# config voice_vlan oui add 00:23:45:00:00:01 description DLINK_MASK mask ff:ff:ff:ff:ff:ff
Command: config voice_vlan oui add 00:23:45:00:00:01 description DLINK_MASK mask ff:ff:ff:ff:ff:ff

Success.
DGS-2000-28:5# show voice_vlan oui
Command: show voice_vlan oui

ID      Description       Telephony OUI       OUI Mask
--   -----------------   -----------------   -----------------
1    DLINK_TEST          00-12-34-00-00-00   FF-FF-FF-00-00-00
2    DLINK_MASK          00-23-45-00-00-01   FF-FF-FF-FF-FF-FF

Total Entries : 2

DGS-2000-28:5#
```

config voice_vlan ports

Purpose	To change the the state of auto detection feature in Voice VLAN.
Syntax	**config voice_vlan ports <portlist> auto dectection [enable { tag | untag } | disable]**
Description	To change the the state of auto detection feature in Voice VLAN.
Parameters	*<portlist>* − A port, range of ports which would configured for Voice VLAN auto detection state. *{ tag | untag }* – Determine the port rule once the MAC address (OUI) hits the value configured
Restrictions	Only Administrator, operator or power user–level users can issue this command.

Example usage:

To specifiy the particular OUI (Organization Unique Indentifier) values for Voice VLAN auto detection feature:

```
DGS-2000-28:5# config voice_vlan ports 1 auto dectection enable untag
Command: config voice_vlan ports 1 auto dectection enable untag

Success.

DGS-2000-28:5# config voice_vlan ports 8 auto dectection enable tag
Command: config voice_vlan ports 8 auto dectection enable tag
```

```
Success.

DGS-2000-28:5# show voice_vlan voice_device all
Command: show voice_vlan voice_device all

Ports   Voice Device
-----   -----------------
1       00-12-34-00-00-01
8       00-23-45-00-00-01

DGS-2000-28:5# show vlan vlanid 5
Command: show vlan vlanid 5

VID             : 5       VLAN NAME      : VLAN5
VLAN Type       : Voice VLAN
VLAN Advertisement : Disabled
Member Ports    : 1,8
Tagged Ports    : 8
Untagged Ports  : 1
Forbidden Ports : 1
```

config voice_vlan log state

Purpose	To change the the state of logging the event of Voice VLAN.
Syntax	**config voice_vlan log state [enable | disable]**
Description	To change the the state of logging the event of Voice VLAN.
Parameters	*enable* – Enable the logging machanism *disable* – Disable the logging mechanism
Restrictions	Only Administrator, operator or power user–level users can issue this command.

Example usage:

To specifiy the particular OUI (Organization Unique Indentifier) values for Voice VLAN auto detection feature:

```
DGS-2000-28:5# config voice_vlan log state enable
Command: config voice_vlan log state enable

Success.

DGS-2000-28:5# show log
Command: show log

Index  Time                Log Text
-----  ------------------- ----------------------------------------
```

```
 10    Mar  6 17:20:55:Voice Vlan-6: Port 8 add into voice VLAN 5
  9    Mar  6 17:20:55:Voice Vlan-6: New voice device detected (Port:8, MAC:0-23-45-
0-0-1)
  8    Mar  6 17:20:54:Voice Vlan-6: Port 1 add into voice VLAN 5
  7    Mar  6 17:20:54:Voice Vlan-6: New voice device detected (Port:1, MAC:0-12-34-
0-0-1)
  6    Mar  6 17:20:40:LinkStatus-6: Port 8 link up, 100Mbps FULL duplex
  5    Mar  6 17:20:38:Voice Vlan-6: Port 8 remove from voice VLAN 5
  4    Mar  6 17:20:38:LinkStatus-6: port 8 link down
  3    Mar  6 17:20:36:LinkStatus-6: Port 1 link up, 100Mbps FULL duplex
  2    Mar  6 17:20:33:Voice Vlan-6: Port 1 remove from voice VLAN 5
  1    Mar  6 17:20:33:LinkStatus-6: port 1 link down


DGS-2000-28:5#
```

show voice_vlan

Purpose	Used to show Voice VLAN global status, per port status, and dynamic learned device.
Syntax	**show voice_vlan [{ oui | ports <portlist> | { { lldp_med voice_device | voice_device } { all | ports <portlist> } } }]**
Description	To change the the state of logging the event of Voice VLAN.
Parameters	*oui* – Specify the Voice VLAN OUI parameters configured. *<portlist>* –A port, range of ports would be displaied *lldp_med voice_device* – Specify the dynamic device learned by LLDP-MED mechanism *voice_device* – Specify the dynamic devices learned by OUI.mechanism
Restrictions	None.

Example usage:

To show Voice VLAN global status, per port status, and dynamic learned device:

```
DGS-2000-28:5# show voice_vlan oui
Command: show voice_vlan oui

ID      Description       Telephony OUI       OUI Mask
--   -----------------   -----------------   -----------------
1    DLINK_TEST          00-12-34-00-00-00   FF-FF-FF-00-00-00
2    DLINK_MASK          00-23-45-00-00-01   FF-FF-FF-FF-FF-FF

Total Entries : 2
DGS-2000-28:5# show voice_vlan voice_device all
Command: show voice_vlan voice_device all



Ports   Voice Device
-----   -----------------
```

```
1       00-12-34-00-00-01
8       00-23-45-00-00-01

Total Entries : 2
```

44

AUTO SURVEILLANCE VLAN COMMANDS

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

Command	Parameter
enable surveillance_vlan	{ vlanid <vlanid (1-4094)> | < vlan_name (20) > }
disable surveillance_vlan	
config surveillance_vlan aging_time	<integer (1-65535)>
config surveillance_vlan priority	<integer (0-7)>
config surveillance_vlan oui	{add | delete} <macaddr> <macmask> [component_type {vms | vms_client | video_encoder | network_storage | other} description <desc (20)>]
config surveillance_vlan onvif_discover_port	{554 | <integer (1025-65535)>}
config surveillance_vlan onvif_ipc	<ip_addr> [mac <macaddr>] [description <desc (20)> | state {enable | disable}]
config surveillance_vlan onvif_nvr	<ip_addr> [mac <macaddr>] description <desc (20)>
config surveillance_vlan ports	{<portlist> | all} state {enable | disable}
config surveillance_vlan log state	{ enable | disable }
show surveillance_vlan	{ onvif_ipc_ports [<portlist>] {brief | detail} | onvif_nvr_ports [<portlist>] [ipc_list]}
show surveillance_vlan	[{ oui | ports [<portlist>] | device [ports <portlist>] }]

Each command is listed in detail, as follows:

enable surveillance_vlan	
Purpose	To assign the particular VLAN as surveillance VLAN.
Syntax	**enable surveillance_vlan [vlanid <vlanid (1-4094)> | < vlan_name (20) >]**
Description	Surveillance VLAN is a VLAN used to carry voice and video traffic from surveillance devices. The quality of service (QoS) for voice traffic shall be configured higner than normal traffic to ensure the

	quality of sound.
Parameters	*<vlanid (1-4094)>* - Specifies all VLANs or VLAN id to be displayed. *<vlan_name>* - Specifies the name of VLAN
Restrictions	Only Administrator, operator or power user–level users can issue this command.

Example usage:

To assign the particular VLAN as surveillance VLAN:

```
DGS-2000-28MP:5# enable surveillance_vlan vlanid 5
Command: enable surveillance_vlan vlanid 5

Success.

DGS-2000-28MP:5#
```

disable surveillance_vlan

Purpose	To disable Voice VLAN function.
Syntax	**disable surveillance_vlan**
Description	To disable Voice VLAN function
Parameters	None
Restrictions	Only Administrator, operator or power user–level users can issue this command.

xample usage:

To turn off surveillance VLAN:

```
DGS-2000-28MP:5# disable surveillance_vlan
Command: disable surveillance_vlan

Success.

DGS-2000-28MP:5#
```

config surveillance_vlan aging_time

Purpose	To specify the aging time of dynamic surveillance VLAN member port.
Syntax	**config surveillance_vlan aging_time <integer (1-65535)>**
Description	To specify the aging time of surveillance VLAN member port
Parameters	*<integer (1-65535)>* - Measurement unit in minute.
Restrictions	Only Administrator, operator or power user–level users can issue this command.

Example usage:

To specify the aging time of surveillance VLAN member port:

```
DGS-2000-28MP:5# config surveillance_vlan aging_time 20
Command: config surveillance_vlan aging_time 20
```

```
Success.

DGS-2000-28MP:5#
```

config surveillance_vlan priority

Purpose	To specify the 802.1p priority value used in surveillance traffic.
Syntax	**config surveillance_vlan priority <integer (0-7)>**
Description	To specify the 802.1p priority value used in voice traffic.
Parameters	*<integer (0-7)>* - in range of 0-7 of 802.1p priority value
Restrictions	None.

Example usage:

To specify the 802.1p priority value used in surveillance traffic:

```
DGS-2000-28MP:5# config surveillance_vlan priority 6
Command: config surveillance_vlan priority 6

Success.

DGS-2000-28MP:5#
```

config surveillance_vlan oui

Purpose	To specifiy the particular OUI (Organization Unique Indentifier) values for Voice VLAN auto detection feature.
Syntax	**config surveillance_vlan oui {add | delete} <macaddr> <macmask> [component_type {vms | vms_client | video_encoder | network_storage | other} description <desc (20)>]**
Description	To specifiy the particular OUI (Organization Unique Indentifier) values for Voice VLAN auto detection feature. The OUI can be determined as range list by configuring MAC mask.
Parameters	*<macaddr>* - To specify the MAC address either by XX:XX:XX:XX:XX:XX or XX-XX-XX-XX-XX-XX format *<macmask>* - To specify the mask of MAC address indentified. component_type: Idnetify the corresponding MAC address for the following types: vms (Video Management System), vms_client, video_encoder and network storage.
Restrictions	Only Administrator, operator or power user–level users can issue this command.

Example usage:

To specifiy the particular OUI (Organization Unique Indentifier) values for surveillance VLAN:

```
DGS-2000-28MP:5# config surveillance_vlan oui add 00:02:03:04:05:06 ff-ff-ff-ff-ff-ff
component_type vms
Command: config surveillance_vlan oui add 00:02:03:04:05:06 ff-ff-ff-ff-ff-ff co
mponent_type vms
```

```
Success.

DGS-2000-28MP:5#
```

config surveillance_vlan onvif_discover_port

Purpose	To configure the port for ONVIF discovery protocol.
Syntax	**config surveillance_vlan onvif_discover_port {554 | <integer (1025-65535)>}**
Description	ONVIF (Open Netork Video Inerface Forum) is an open industry forum to promote standardized interfaces for effective interoperability of IP-based physical security products.
Parameters	*554* | *<integer (1025-65535)>* − The port specified for ONVIF discovery protocol.
Restrictions	Only Administrator, operator or power user–level users can issue this command.

Example usage:

To specifiy the particular port for ONVIF discovery protocol

```
DGS-2000-28MP:5# config surveillance_vlan onvif_discover_port 1025
Command: config surveillance_vlan onvif_discover_port 1025

Success.

DGS-2000-28MP:5#
```

config surveillance_vlan onvif_ipc

Purpose	To identify the specific device as IPC (IP camera) device.
Syntax	**config surveillance_vlan onvif_ipc <ip_addr> [mac <macaddr>] [description <desc (20)> | state {enable | disable}]**
Description	To identify the specific device as IPC (IP camera) device.
Parameters	*<ip_addr>* − IP address of IPC. *mac<macaddr>*- IPC MAC address *description <desc (20)>* - Description string supports up to 32 characters.
Restrictions	Only Administrator, operator or power user–level users can issue this command.

Example usage:

To specifiy the particular device as IPC:

```
DGS-2000-28MP:5# config surveillance_vlan onvif_ipc 192.168.100.1 mac
00:02:03:04:05:06 description testing

Command: config surveillance_vlan onvif_ipc 192.168.100.1 mac 00:02:03:04:05:06 d
```

```
escription testing


Success.

DGS-2000-28MP:5#
```

config surveillance_vlan onvif_nvr

Purpose	To identify the specific device as NVR (Network Video Recorder) device.
Syntax	**config surveillance_vlan onvif_nvr <ip_addr> [mac <macaddr>] description <desc (20)>**
Description	To identify the specific device as IPC (IP camera) device.
Parameters	*<ip_addr>* − IP address of NVR. *mac<macaddr>*-NVR MAC address *description <desc (20)>* - Description string supports up to 32 characters.
Restrictions	Only Administrator, operator or power user–level users can issue this command..

Example usage:

To specifiy the particular device as NVR:

```
DGS-2000-28MP:5# config surveillance_vlan onvif_nvr 192.168.100.1 mac
00:02:03:04:05:06 description testing

Command: config surveillance_vlan onvif_nvr 192.168.100.1 mac 00:02:03:04:05:06 d
escription testing


Success.

DGS-2000-28MP:5#
```

config surveillance_vlan ports

Purpose	To change the the state of auto detection feature in surveillance VLAN.
Syntax	**config voice_vlan ports <portlist> | all} state {enable | disable}**
Description	To change the the state of auto detection feature in surveillance VLAN.
Parameters	*<portlist>* − A port, range of ports which would configured for Voice VLAN auto detection state.
Restrictions	Only Administrator, operator or power user–level users can issue this command.

Example usage:

To turn on surveillance VLAN on all ports:

```
DGS-2000-28MP:5# config surveillance_vlan ports all state enable
```

```
Command: config surveillance_vlan ports all state enable

Success.

DGS-2000-28MP:5#
```

config surveillance_vlan log state

Purpose	To change the the state of logging the event of surveillance VLAN.
Syntax	**config voice_vlan log state [enable | disable]**
Description	To change the the state of logging the event of surveillance VLAN.
Parameters	*enable* – Enable the logging machanism *disable* – Disable the logging mechanism
Restrictions	Only Administrator, operator or power user–level users can issue this command.

Example usage:

To turn on logging for surveillance VLAN events:

```
DGS-2000-28MP:5# config surveillance_vlan log state enable
Command: config surveillance_vlan log state enable

Success.

DGS-2000-28MP:5#
```

show surveillance_vlan

Purpose	Used to show Voice surveillance global status, per port status, and dynamic learned device.
Syntax	**show voice_vlan [{ oui | ports [<portlist>] | device [ports <portlist>] }]**
Description	To change the the state of logging the event of Voice VLAN.
Parameters	*oui* – Specify the Voice VLAN OUI parameters configured. <*portlist*> –A port, range of ports would be displaied *lldp_med voice_device* – Specify the dynamic device learned by LLDP-MED mechanism *voice_device* – Specify the dynamic devices learned by OUI.mechanism
Restrictions	None.

Example usage:

To show Voice VLAN global status, per port status, and dynamic learned device:

```
DGS-2000-28MP:5# show surveillance_vlan
Command: show surveillance_vlan
```

```
Surveillance VLAN State   Enabled
VLAN ID                   5
VLAN Name                 VLAN5
Priority                  6
Aging Time                20
ONVIF Discover Port       1025
Log State                 Enabled

DGS-2000-28MP:5#
```

45

D-LINK DISCOVER PROTOCOL COMMANDS

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

Command	Parameter
enable ddp	
disable ddp	
config ddp report state	[enable | diasble]
config ddp report_timer	[30 | 60 | 90 | 120 | never]
config ddp ports	[all | <portlist>] state [enable | disable]
show ddp	

Each command is listed in detail, as follows:

enable ddp	
Purpose	To enable the D-Link discover protocol function.
Syntax	**enable ddp**
Description	The **enable ddp** command is used to enable the D-Link discover protocol function.
Parameters	None.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To enable the D-Link discover protocol function:

```
DGS-2000-28MP:5# enable ddp
Command: enable ddp



Success.
DGS-2000-28MP:5#
```

disable ddp	
Purpose	To disable the D-Link discover protocol function.
Syntax	**disable ddp**
Description	The **disable ddp** command is used to disable the D-Link discover protocol function.
Parameters	None.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To disable the D-Link discover protocol function:

```
DGS-2000-28MP:5# disable ddp
Command: disable ddp



Success.
DGS-2000-28MP:5#
```

config ddp report state

Purpose	To enable or disable the D-Link discover protocol packet report function.
Syntax	**config ddp report state [enable | diasble]**
Description	The **config ddp report state** command is used to enable or disable the D-Link discover protocol packet report function.
Parameters	*[enable* | *disable]* – Specifies to enable or disable the D-Link discover protocol packet report function.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To enable the D-Link discover protocol packet report function:

```
DGS-2000-28MP:5# config ddp report state enable
Command: config ddp report state enable



Success.
DGS-2000-28MP:5#
```

config ddp report_timer

Purpose	To configure the D-Link discover protocol packet report timer.
Syntax	**config ddp report_timer [30 | 60 | 90 | 120 | never]**
Description	The **config ddp report timer** command is used configure the D-Link discover protocol packet report timer.
Parameters	*[30* | *60* | *90* | *120* | *never]* - Specifies the report timer of D-Link Discover Protocol in seconds.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To configure the D-Link discover protocol packet report timer:

```
DGS-2000-28MP:5# config ddp report timer 30
Command: config ddp report timer 30



Success.
DGS-2000-28MP:5#
```

config ddp ports

Purpose	To configure the ports of D-Link discover protocol packet report state.
Syntax	**config ddp ports [all | <portlist>] state [enable | disable]**
Description	The **config ddp ports** command is used configure the D-Link discover protocol packet report port state.
Parameters	*[all* | *<portlist>]* - Specifies the ports of D-Link Discover Protocol state to be enabled or disabled.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To enable the ports 6-8 of D-Link discover protocol state:

```
DGS-2000-28MP:5# config ddp ports 6-8 state enable
Command: config ddp ports 6-8 state enable



Success.
DGS-2000-28MP:5#
```

show ddp

Purpose	To display the ports of D-Link discover protocol packet information.
Syntax	**show ddp**
Description	The **show ddp** command is used to display the ports of D-Link discover protocol packet information.
Parameters	None.
Restrictions	None.

Example usage:

To display the D-Link discover protocol state:

```
DGS-2000-28MP:5# show ddp
Command: show ddp


DDP System Information
   DDP Global state            : Enable
   DDP Report Timer Period : Disable

DDP Port State

   Port  State
   ----  -----------
   1     Disable
   2     Disable
   3     Disable
   4     Disable
   5     Disable
   6     Enable
   7     Enable
   8     Enable
   9     Disable
   10    Disable
   11    Disable
   12    Disable
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a ALL
```

46

DIGITAL DIAGNOSTIC MONITORING COMMANDS

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

Command	Parameter
config ddm ports	<portlist> [bias_current_threshold [high_alarm | low_alarm] | rx_power_threshold | shutdown | state [enable | disable] | temperature_threshold | tx_power_threshold | voltage_threshold] ([high_alarm <signed_float>] [low_alarm <signed_float>] [high_warning <signed_float>] [low_warning <signed_float>])
config ddm power_unit	[mw | dbm]
show ddm ports	<portlist> [configuration | status | vendor_info]

Each command is listed in detail, as follows:

config ddm ports	
Purpose	To configure the DDM settings of the specified ports.
Syntax	**config ddm ports <portlist> [bias_current_threshold [high_alarm | low_alarm] | rx_power_threshold | shutdown | state [enable | disable] | temperature_threshold | tx_power_threshold | voltage_threshold]**
Description	The **config ddm ports** command is used to configure the DDM settings of the specified ports.
Parameters	*<portlist>* - Specifies the range of ports to be configured. *bias_current_threshold* - Specify the threshold of the optic module's bias current. *high_alarm* - Specify the high threshold for the alarm. When the operating parameter rises above this value, the action associated with the alarm is taken. *low_alarm* -Specify the low threshold for the alarm. When the operating parameter falls below this value, the action associated with the alarm is taken. *rx_power_threshold* - Specify the threshold of optic module's received power. *state* - Specify the DDM state to enable or disable. If the state is disabled, no DDM action will take effect. *temperature_threshold* - Specify the threshold of the optic module's temperature in centigrade. At least one parameter shall be specified for this threshold. *shutdown* - Specify whether or not to shutdown the port when the operating parameter exceeds the corresponding alarm threshold or warning threshold. The default value is none. *tx_power_threshold* - Specify the threshold of the optic module's output power. *voltage_threshold* - Specify the threshold of optic module's voltage.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure the port 21's voltage threshold:

```
DGS-2000-28MP:5# config ddm ports 1:21 temperature_threshold high_alarm 84.9555 low_alarm -10 high_warning 70 low_warning 2.25251
Command: config ddm ports 1:21 temperature_threshold high_alarm 84.9555 low_alarm -10 high_warning 70 low_warning 2.25251

Success.

DGS-2000-28MP:5#
```

config ddm power_unit

Purpose	To configure the unit of DDM TX and RX power.
Syntax	**config ddm power_unit [mw | dbm]**
Description	The **config ddm power_unit** command is used to configure the unit of DDM TX and RX power.
Parameters	*mw* - Specify the DDM TX and RX power unit as mW. *dbm* - Specify the DDM TX and RX power unit as dBm.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure the DDM TX and RX power unit as dBm:

```
DGS-2000-28MP:5# config ddm power_unit dbm
Command: config ddm power_unit dbm

Success.
DGS-2000-28MP:5#
```

show ddm ports

Purpose	To display the current operating DDM parameters and configuration values of the optic module of the specified ports.
Syntax	**show ddm ports <portlist> [configuration | status | vendor_info]**
Description	The **config ddm power_unit** command is used to display the current operating DDM parameters and configuration values of the optic module of the specified ports.
Parameters	<*portlist*> - Specify the ports of DDM to be displayed. *configuration* - Specifies that the configuration values will be displayed. *status* - Specifies that the operating parameter will be displayed. vendor_info - Specifies that the vender information will be displayed.
Restrictions	None.

Example usage:

To display ports 1-5's operating parameters:

```
DGS-2000-28MP:5# show ddm ports 1-5 vender_info
Command: show ddm ports 1-5 vender_info

Invalid DDM port list.

Failure!
DGS-2000-28MP:5#
```

47

IPV4/IPV6 ROUTING COMMANDS

The IPv4/IPv6 Routing commands commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameter
create iproute	[<network_address> | default] {metric <int 1-65535>} {primary | backup}
delete iproute	[<network_address> | default] <ipaddr>
show iproute	{static}
create ipv6route	[<ipv6networkaddr> | default] <ipv6addr> [metric <int 1-65535>] {primary | backup}
delete ipv6route	[<ipv6networkaddr> | default] default <ipv6addr>
show ipv6route	{static}

Each command is listed in detail, as follows:

create iproute	
Purpose	To create an IP route entry on the Switch.
Syntax	**create iproute [<network_address> | default] {metric <int 1-65535>} {primary | backup}**
Description	The **create iproute** command is used to create an IP route entry on the Switch. “Primary” and “backup” are mutually exclusive. Users can select only one when creating one new route. If a user sets neither of these, the system will try to set the new route first by primary and second by backup.
Parameters	*<network_address>* - The IP address and netmask of the IP interface that is the destination of the route. Specify the address and mask information using the traditional format (for example, 10.90.90.3/255.0.0.0 or in CIDR format, 10.90.90.3/8). *default* – To create a default IPv4 route entry. *<ipaddr>* – To specify the IPv4 address for the next hop route. · *metric <int 1-65535>* – To specify the hop cost, and the default is 1. The value ranges between 1 and 65535. · *primary* – To specify the route as the primary route to the destination. · *backup* – To specify the route as the backup route to the destination. If the route is not specified as the primary route or the backup route, then it will be auto-assigned by the system. The first created is the primary, the second created is the backup.
Restrictions	Only administrator, operator or power user-level users can issue this command.

Example usage:

To add a default route with a nexthop of 10.90.58.33 as primary route:

```
DGS-2000-28MP:5# create iproute default 10.90.58.33 primary
Command: create iproute default 10.90.58.33 primary

Success.
DGS-2000-28MP:5#
```

delete iproute	
Purpose	Used to delete an IP route entry from the Switch's IP routing table.
Syntax	**delete iproute [<network_address> | default] <ipaddr>**
Description	The **delete iproute** command will delete an existing IP route entry from the Switch's IP routing table.
Parameters	<*network_address*> - The IP address and netmask of the IP interface that is the destination of the route. Specify the address and mask information using the traditional format (for example, 10.90.90.3/255.0.0.0 or in CIDR format, 10.90.90.3/8). *default* – Specifies to delete a default IP route entry. <*ipaddr*> – To specify the IPv4 address for the next hop router to be configured.
Restrictions	Only Administrator, operator and power user-level users can issue this command.

Example usage:

To delete the default route from the routing table:

```
DGS-2000-28MP:5# delete iproute 10.90.58.33
Command: delete iproute 10.90.58.33


Success.
DGS-2000-28MP:5#
```

show iproute	
Purpose	Used to display the Switch's current IP routing table.
Syntax	**show iproute {static}**
Description	The **show iproute** command will display the Switch's current IP routing table.
Parameters	*{static}* – Specifies to display all the static route entries.
Restrictions	None.

Example usage:

To display the contents of the IP routing table:

```
DGS-2000-28MP:5# show iproute
Command: show iproute

Routing Table

IP Address/Netmask  Gateway    Interface    Hops    Protocol
--------------------------- --------------- ------------- ------- --------------
           10.0.0.0/8    0.0.0.0        System      1       Local

Total Entries  :1

DGS-2000-28MP:5#
```

create ipv6route

Purpose	Used to create an IPv6 static route in the Switch's IP routing table.
Syntax	**create ipv6route [<ipv6networkaddr> | default] <ipv6addr> [metric <int 1-65535>] {primary | backup}**
Description	This **create ipv6route** command is used to create a primary and backup IP route entry to the Switch's IP routing table.
Parameters	*<ipv6networkaddr>* - Specifies the destination network for the route. *default* – To create a default IPv6 route entry. *<ipaddr>* – To specify the IPv6 address for the next hop route. · *metric <int 1-65535>* – To specify the hop cost, and the default is 1. The value ranges between 1 and 65535. · *primary* – To specify the route as the primary route to the destination. · *backup* – To specify the route as the backup route to the destination. If the route is not specified as the primary route or the backup route, then it will be auto-assigned by the system. The first created is the primary, the second created is the backup.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To add a single static IPv6 entry in IPv6 format:

```
DGS-2000-28MP:5# create ipv6route default FEC0::5
Command: create ipv6route default FEC0::5


Success.
DGS-2000-28MP:5#
```

delete ipv6route

Purpose	Used to delete a static IPv6 route entry from the Switch's IP routing table.

Syntax	**delete ipv6route [<ipv6networkaddr> | default] <ipv6addr>**
Description	This **delete ipv6route** command will delete an existing static IPv6 entry from the Switch's IP routing table.
Parameters	*<ipv6networkaddr>* – To specify the IPv6 address that is the destination of the route to be deleted. *default* – Specifies to delete a default IP route entry. *<ipaddr>* – To specify the IPv6 address for the next hop router to be configured.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To delete a static IPv6 entry from the routing table:

```
DGS-2000-28MP:5# delete ipv6route default FEC0::5
Command: delete ipv6route default default FEC0::5


Success.
DGS-2000-28MP:5#
```

show ipv6route

Purpose	Used to display a static IPv6 route entry from the Switch's IP routing table.
Syntax	**show ipv6route {static}**
Description	This **show ipv6route** command will display an existing static IPv6 entry from the Switch's IP routing table.
Parameters	*{static}* – Specifies to display all the IPv6 static route entries.
Restrictions	None.

Example usage:

To show a static IPv6 entry from the routing table:

```
DGS-2000-28MP:5# show ipv6route
Command: show ipv6route

IPv6 Prefix: ::/0                       Protocol: Static Metric: 1
Next Hop   : FEC0::5                    IPIF    : System

Total Entries: 1
DGS-2000-28MP:5#
```

48

IP-MAC-PORT BINDING COMMANDS

The IP network layer uses a four-byte address. The Ethernet link layer uses a six-byte MAC address. Binding these two address types together allows the transmission of data between the layers. The primary purpose of IP-MAC-port binding is to restrict the access to a switch to a number of authorized users. Only the authorized client can access the Switch's port by checking the pair of IP-MAC addresses with the pre-configured database. If an unauthorized user tries to access an IP-MAC-port binding enabled port, the system will block the access by dropping its packet. The maximum number of IP-MAC-port binding entries is dependant on chip capability (e.g. the ARP table size) and storage size of the device. For the Switch, the maximum value for the IP-MAC-port binding ARP mode is 500. The creation of authorized users can be manually configured by CLI or Web. The function is port-based, meaning a user can enable or disable the function on the individual port.

The IP-MAC-Port Binding commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table:

Command	Parameter
create address_binding ip_mac	[ipaddress <ipaddr> | ipv6address <ipv6addr>] mac_address <macaddr> ports [<portlist> | all]
config address_binding ip_mac ports	[<portlist> | all] {state [disable | enable] | ip_inspection [disable | enable] | arp_inspection [loose | strict] | allow_zeroip [enable | disable] | forward_dhcppkt [enable | disable] | protocol [ipv4 | ipv6 | all]}
config address_binding auto_scan	from_ip <ipaddr> to_ip <ipaddr>
config address_binding auto_scan ipv6address	from_ip <ipv6addr> to_ip <ipv6addr>
delete address_binding	[ip_mac [ipaddress <ipaddr> | ipv6address <ipv6addr> | mac_address <macaddr> | all] | blocked [all | vlan_name <string 32> mac_address <macaddr> port <port 1-28>]]
show address_binding	{[ip_mac [all | {ipaddress <ipaddr> | ipv6address <ipv6addr> | mac_address <macaddr>}] }
show address_binding auto_scan list	
enable address_binding dhcp_snoop	ports {<portlist> | all} [vlan <vidlist>] [{ipv6 | all}]
disable address_binding dhcp_snoop	ports {<portlist> | all} [{ipv6 | all}]
config address_binding dhcp_snoop	{max_entry ports [<portlist> | all] limit [<int 1-10> | no_limit] {IPv6}} | {flush_on_port_down ports <portlist> | all] [enable | disable]}
show address_binding dhcp_snoop	[binding_entry | flust_status | max_entry | vlan_list] ports <portlist>

Each command is listed in detail, as follows:

create address_binding ip_mac	
Purpose	Used to create an IP-MAC-port binding entry.

Syntax	**create address_binding ip_mac [ipaddress <ipaddr> | ipv6address <ipv6addr>] mac_address <macaddr> ports [<portlist> | all]**
Description	The **create address_binding ip_mac ipaddress** command is used to create an IP-MAC-port binding entry.
Parameters	*ipaddress* <*ipaddr*> – The IPv4 address of the device where the IP-MAC-port binding is made. *Ipv6address* <*ipv6addr*> – The IPv4v6 address of the device where the IP-MAC-port binding is made. <*macaddr*> – The MAC address of the device where the IP-MAC-port binding is made. *[<portlist> | all]* – Specifies the ports to be configured for address binding.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To create address binding on the Switch:

DGS-2000-28MP:5# create address_binding ip_mac ipaddress 10.90.90.93 mac_address 00-11-11-22-33-44 ports 6

Command: create address_binding ip_mac ipaddress 10.90.90.93 mac_address 00-11-11-22-33-44 ports 6

Success.

DGS-2000-28MP:5#

config address_binding ip_mac ports

Purpose	Used to configure an IP-MAC-port binding state to enable or disable for specified ports.
Syntax	**config address_binding ip_mac ports [<portlist> | all] {state [disable | enable] | ip_inspection [disable | enable] | arp_inspection [loose | strict] | allow_zeroip [enable | disable] | forward_dhcppkt [enable | disable]}**
Description	The **config address_binding ip_mac ports** command is used to configure the IP-MAC-port binding state to enable or disable for specified ports.
Parameters	<*portlist*> − Specifies a port or range of ports. *all* – Specifies all ports on the switch. *[enable | disable]* – Enables or disables the specified range of ports for state, IP-inspection, allow_zeroip and forward_dhcppkt. *arp_inspection [loose | strict]* – Specifies to check the ARP inspection to be loose or stict for the specified ports.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To configure address binding on the Switch:

DGS-2000-28MP:5# config address_binding ip_mac ports 3 state disable arp_inspection loose ip_inspection disable

Command: config address_binding ip_mac ports 3 state disable arp_inspection loose ip_inspection disable

```
Success.
DGS-2000-28MP:5#
```

config address_binding auto_scan

Purpose	Used to configure an IP-MAC-port binding auto scan for specified IP addresses.
Syntax	**config address_binding auto_scan from_ip <ipaddr> to_ip <ipaddr>**
Description	The **config address_binding auto_scan** command is used to configure the IP-MAC-port binding auto scan for specified IP addresses.
Parameters	<*ipaddr*> − Specifies a range of IP addresses for address binding auto scan on the Switch.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To configure address binding auto scan on the Switch:

```
DGS-2000-28MP:5# config address_binding auto_scan from_ip 10.0.0.10 to_ip 10.0.0.12
Command: config address_binding auto_scan from_ip 10.0.0.10 to_ip 10.0.0.12

Success.
DGS-2000-28MP:5#
```

config address_binding auto_scan ipv6address

Purpose	Used to configure an IP-MAC-port binding auto scan for specified IPv6 addresses.
Syntax	**config address_binding auto_scan ipv6address from_ip <ipv6addr> to_ip <ipv6addr>**
Description	The **config address_binding auto_scan** command is used to configure the IP-MAC-port binding auto scan for specified IPv6 addresses.
Parameters	<*ipv6addr*> − Specifies a range of IPv6 addresses for address binding auto scan on the Switch.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To configure address binding auto scan on the Switch:

```
DGS-2000-28MP:5# config address_binding auto_scan ipv6address from_ip 3000::1 to_ip 3000::3
Command: config address_binding auto_scan ipv6address from_ip 3000::1 to_ip 3000::3

Success.
DGS-2000-28MP:5#
```

delete address_binding

Purpose	Used to delete IP-MAC-port binding entries.
Syntax	**delete address_binding [ip_mac [ipaddress <ipaddr> | ipv6address <ipv6addr> | mac_address <macaddr> | all] | blocked [all | vlan_name <string 32> mac_address <macaddr> port <port 1-28>]]**
Description	The **delete address_binding** command is used to delete IP-MAC-port binding entries. Two different kinds of information can be deleted. *ip_mac* – Individual address binding entries can be deleted by entering the physical and IP addresses of the device. Toggling to all will delete all the address binding entries. *blocked* – Blocked address binding entries (bindings between VLAN names and MAC addresses) can be deleted by entering the VLAN name and the physical address of the device. To delete all the blocked address binding entries, toggle all.
Parameters	*ipaddress* <*ipaddr*> – The IPv4 address of the device where the IP-MAC-port binding is made. *iv6paddress* <*ipv6addr*> – The IPv6 address of the device where the IP-MAC-port binding is made. <*macaddr*> – The MAC address of the device where the IP-MAC-port binding is made. *vlan_name* <*string 32*> – The VLAN name of the VLAN that is bound to a MAC address in order to block a specific device on a known VLAN. *all* – For IP-MAC-port binding all specifies all the IP-MAC-port binding entries; for blocked address binding entries all specifies all the blocked VLANs and their bound physical sddresses. <*port 1-28*> – Specifies a port to be deleted for address binding.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To delete all address binding entries on the Switch:

```
DGS-2000-28MP:5# delete address_binding ip_mac all
Command: delete address_binding ip_mac all

Success.
DGS-2000-28MP:5#
```

show address_binding

Purpose	Used to display IP-MAC-port binding entries.
Syntax	**show address_binding {[ip_mac [all | {ipaddress <ipaddr> | ipv6address <ipv6addr> | mac_address <macaddr>}] | blocked [all | vlan_name <string 32> mac_address <macaddr> port <portlist>]}**
Description	This **show address_binding** command is used to display IP-MAC-port binding entries. Four different kinds of information can be viewed. *ip_mac* – Address binding entries can be viewed by entering the physical and IP addresses of the device.

	blocked – Blocked address binding entries (bindings between VLAN names and MAC addresses) can be viewed by entering the VLAN name and the physical address of the device. *ports* – The number of enabled ports on the device.
Parameters	*ip_mac* – The database the user creates for address binding. *all* – For IP MAC binding all specifies all the IP-MAC-port binding entries; for blocked address binding entries all specifies all the blocked VLANs and their bound physical addresses. *blocked* – The address database that the system auto learns and blocks. *ipaddress* <*ipaddr*> – The IPv4 address of the device where the IP-MAC-port binding is made. *ipv6address* <*ipv6addr*> – The IPv6 address of the device where the IP-MAC-port binding is made. <*macaddr*> – The MAC address of the device where the IP-MAC-port binding is made. *vlan_name* <*string 32*> – The VLAN name of the VLAN that is bound to a MAC address in order to block a specific device on a known VLAN. *port* <*portlist*> – Specifies a port to be displayed for the address binding on the Switch.
Restrictions	None.

Example usage:

To display address binding entries on the Switch:

```
DGS-2000-28MP:5# show address_binding ip_mac all
Command: show address_binding ip_mac all

IP Address      MAC Address        Port
--------------  -----------------  ----
10.0.0.21       00-00-00-00-01-02  3

DGS-2000-28MP:5#
```

show address_binding auto_scan list

Purpose	Used to display IP-MAC-port binding entries.
Syntax	**show address_binding auto_scan list**
Description	This **show address_binding auto_scan list** command is used to display auto scan list of address binding on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display the auto scan list of address binding on the Switch:

```
DGS-2000-28MP:5# show address_binding auto_scan list
Command: show address_binding auto_scan list

VLAN IP Address                    MAC Address        Port  Bound
--------- -------------------------------- -----------------  ------  -----------
```

```
Total Entries : 0
DGS-2000-28MP:5#
```

enable address_binding dhcp_snoop

Purpose	Used to enable address binding DHCP Snooping.
Syntax	**enable address_binding dhcp_snoop ports [<portlist> | all]**
Description	This **enable address_binding dhcp_snoop** command is used to enable IP-MAC-port binding DHCP snooping entries.
Parameters	*[<portlist> | all]* – Specifies a port, a range of ports or all ports to be enabled of the address binding DHCP snooping on the Switch.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To enable the DHCP snooping of address binding for port 3~5 on the Switch:

```
DGS-2000-28MP:5# enable address_binding dhcp_snoop ports 3-5
Command: enable address_binding dhcp_snoop ports 3-5

Success.
DGS-2000-28MP:5#
```

disable address_binding dhcp_snoop

Purpose	Used to disable address binding DHCP Snooping.
Syntax	**disable address_binding dhcp_snoop ports [<portlist> | all]**
Description	This **disable address_binding dhcp_snoop** command is used to disable IP-MAC-port binding DHCP snooping entries.
Parameters	*[<portlist> | all]* – Specifies a port, a range of ports or all ports to be enabled of the address binding DHCP snooping on the Switch.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To disable the DHCP snooping of address binding for port 3~5 on the Switch:

```
DGS-2000-28MP:5# disable address_binding dhcp_snoop ports 4
Command: disable address_binding dhcp_snoop ports 4

Success.
DGS-2000-28MP:5#
```

config address_binding dhcp_snoop

Purpose	Used to configure the max entry and entry reflush mechanism of DHCP snooping function..
Syntax	**config address_binding dhcp_snoop {max_entry ports [<portlist> | all] limit [<int 1-10> | no_limit] {IPv6}} | {flush_on_port_down ports <portlist> | all] [enable | disable]}**
Description	The **config address_binding dhcp_snoop max_entry** command

	is used to specify the maximum number of DHCP snooping entries on specified ports. By default, the per-port maximum entry has no limit. The command **config address_binding dhcp_snooping flush_on_port_dow**n command forces to clear binded entry when port physical state is down.
Parameters	*max_entry* – The max binding entry of DHCP snooping *[<portlist> | all]* – Specifies a port, a range of ports or all ports to be configured of the address binding DHCP snooping on the Switch. *[<int 1-10> | no_limit]* – Specifies the limit for max entry number. *{IPv6}* – Specifies the IPv6 address used for this configuration. *Flush_on_port_down* – The mechanism to force clear binded entry when the specified port physically down. *[<portlist> | all]* – Specifies a port, a range of ports or all ports to be configured. *enable* | *disable* – Specified the state
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To configure the DHCP snooping of address binding for port 1 on the Switch:

```
DGS-2000-28MP:5# config address_binding dhcp_snoop max_entry ports 1 limit 1
Command: config address_binding dhcp_snoop max_entry ports 1 limit 1

Success.
DGS-2000-28MP:5#
DGS-2000-28MP:5# config address_binding dhcp_snoop flush_on_port_down
ports 1 enable
Command: config address_binding dhcp_snoop flush_on_port_down ports 1
enable

Success.
```

show address_binding dhcp_snoop

Purpose	Used to display DHCP snoop of IP-MAC-port binding.
Syntax	**show address_binding dhcp_snoop [binding_entry | flush_status | max_entry | vlan_list] {ports <portlist>}**
Description	This command is used show types information about DHCP snooping which includes binding entry, flush status, max entry a nd vlan list.
Parameters	*binding_entry* – Display the binding entry *flush_status* – Display the configured status of flush_on_port_down feature *max_entry* - Specifies ddress binding entries can be viewed. *vlan_list* – Display the list of VLAN group that configured to turn on DHCP snooping. *ports <portlist>* – Specifies the ports on the device to be displayed.
Restrictions	None.

Example usage:

To display DHCP snoop of address binding max entries of port 1~5 on the Switch:

```
DGS-2000-28MP:5# show address_binding dhcp_snoop max_entry ports 1-5
Command: show address_binding dhcp_snoop max_entry ports 1-5

Port  Max Entry  Max IPv6 Entry
----  ---------- ----------------------
1     No Limit   No Limit
2     No Limit   No Limit
3     No Limit   No Limit
4     No Limit   No Limit
5     No Limit   No Limit
DGS-2000-28MP:5#
```

49

DOS PREVENTION COMMANDS

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

Command	Parameter
config dos_prevention dos_type	[{land_attack | blat_attack | smurf_attack | tcp_null_scan | tcp_xmascan | tcp_synfin | tcp_syn_srcport_less_1024} | all] {action drop} | state [enable | disable]] }
show dos_prevention	{ land_attack | blat_attack | smurf_attack | tcp_null_scan | tcp_xmascan | tcp_synfin | tcp_syn_srcport_less_1024 }

Each command is listed in detail, as follows:

config dos_prevention dos_type

Purpose	Used to discard the L3 control packets sent to CPU from specific ports.
Syntax	**config dos_prevention dos_type [{land_attack | blat_attack | smurf_attack | tcp_null_scan | tcp_xmascan | tcp_synfin | tcp_syn_srcport_less_1024} | all] {action drop} | state [enable | disable]] }**
Description	The **config dos_prevention dos_type** command is used to configure the prevention of DoS attacks, and incluDGS state and action. The packets matching will be used by the hardware. For a specific type of attack, the content of the packet, regardless of the receipt port or destination port, will be matched against a specific pattern.
Parameters	The type of DoS attack. Possible values are as follows: land_attack, blat_attack, smurf_attack, tcp_null_scan, tcp_xmascan tcp_synfin and tcp_syn_srcport_less_1024. By default, prevention for all types of DoS are enabled except for tcp_syn_srcport_less_1024. *action [drop | mirror]* - When enabling DoS prevention, the following actions can be taken. · *drop* – Drop the attack packets. · *mirror* – Mirror the packet to other port for further process. *priority <value (0-7)>* – Change packet priority by the Switch from 0 to 7. If the priority is not specified, the original priority will be used. *rx_rate [no_limit | <value (64-1024000)>]* – controls the rate of the received DoS attack packets. If not specified, the default action is drop. *state [enable | disable]*- Enable or disable DoS prevention.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To configure a land attack and blat attack prevention:

```
DGS-2000-28MP:5# config dos_prevention dos_type blat_attack action drop
Command: config dos_prevention dos_type blat_attack action drop


Success.

DGS-2000-28MP:5#
```

show dos_prevention

Purpose	Used to display DoS prevention information.
Syntax	**show dos_prevention { land_attack | blat_attack | smurf_attack | tcp_null_scan | tcp_xmascan | tcp_synfin | tcp_syn_srcport_less_1024 }**
Description	The **show dos_prevention** command is used to display DoS prevention information, including the type of DoS attack, the prevention state, the corresponding action if the prevention is enabled, and the counter information of the DoS packet.
Parameters	The type of DoS attack. Possible values are as follows: land_attack, blat_attack, smurf_attack, tcp_null_scan, tcp_xmascan tcp_synfin and tcp_syn_srcport_less_1024.
Restrictions	None.

Example usage:

To display DoS prevention information:

```
DGS-2000-28MP:5# show dos_prevention
Command: show dos_prevention

Trap/Log   : Disabled
DosType                          State      Action       Frame Counts
-------------------------------- ---------- ------------ --------------------
Land Attack                      Enabled    Drop         -
Blat Attack                      Enabled    Drop         -
Tcp Null Scan                    Disabled   Drop         -
Tcp Xmascan                      Disabled   Drop         -
Tcp Synfin                       Enabled    Drop         -
Tcp Syn Srcport less 1024        Enabled    Drop         -
Ping Death Attack                Disabled   Drop         -
Tcp Tiny Fragment                Disabled   Drop         -
```

To display DoS prevention information for Land Attack:

```
DGS-2000-28MP:5# show dos_prevention land_attack
Command: show dos_prevention land_attack

DoS Type          : Land Attack
  State           : Enabled
  Action          : Drop
  Frame Counts    : -
```

```
DGS-2000-28MP:5#
```

50

TRUST HOST COMMANDS

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

Command	Parameter
enable trusted_host	
disable trusted_host	
create trusted_host	[<ipaddr> | <ipv6_addr> | network {<network_address> | <ipaddr>} | ipv6_prefix <ipv6networkaddr>]
show trusted_host	
delete trusted_host	[<ipaddr> | network <network_address> | <ip6_addr> | ipv6_prefix <ipv6networkaddr> | all]

Each command is listed in detail, as follows:

enable trusted_host	
Purpose	To enable the trusted host.
Syntax	**enable trusted_host**
Description	The **enable trusted_host** command enables the trusted host feature.
Parameters	None.
Restrictions	Only administrator or operator level users can issue this command.

Example usage:

To enable the trusted host on the Swtich:

```
DGS-2000-28MP:5# enable trusted_host
Command: enable trusted_host


Success.
DGS-2000-28MP:5#
```

disable trusted_host	
Purpose	To enable the trusted host.
Syntax	**disable trusted_host**
Description	The **disable trusted_host** command disables the trusted host feature.
Parameters	None.
Restrictions	Only administrator or operator level users can issue this command.

Example usage:

To disable the trusted host on the Swtich:

```
DGS-2000-28MP:5# disable trusted_host
Command: disable trusted_host


Success.
DGS-2000-28MP:5#
```

create trusted_host

Purpose	To create a trusted host.
Syntax	**create trusted_host [<ipaddr> | <ip6_addr> | network {<network_address> | <ipaddr> | ipv6_prefix <ipv6networkaddr>]**
Description	The **create trusted_host** command creates a trusted host. The Switch allows specifying up to 30 IPv4 or IPv6 addresses that are allowed to manage the Switch via in-band based management software. These IP addresses must be members of the Management VLAN. If no IP addresses are specified, then there is nothing to prevent any IP address from accessing the Switch, provided the user knows the Username and Password.
Parameters	<*ipaddr*> − The IPv4 address of the trusted host to be created. <*network_address*> − The subnet mask of the trusted host to be created. This parameter is optional. If not specified, the default subnet mask is 255.255.255.0. <*ip6_addr*> − The IPv6 address of the trusted host to be created. *ipv6_prefix* <*ipv6networkaddr*> − The IPv6 subnet prefix of the trusted network to be created. The network address of the trusted network. The form of network address is xxx.xxx.xxx.xxx/y.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To create the trusted host:

```
DGS-2000-28MP:5# create trusted_host 10.90.90.91
Command: create trusted_host 10.90.90.91

Success.
DGS-2000-28MP:5#
```

To create the IPv6 trusted host:

```
DGS-2000-28MP:5# create trusted_host 3000::1
Command: create trusted_host 3000::1


Success.
DGS-2000-28MP:5#
```

show trusted_host

Purpose	To display a list of trusted hosts entered on the Switch using the create trusted_host command above.
Syntax	**show trusted_host**
Description	The **show trusted_host** command displays a list of trusted hosts entered on the Switch using the **create trusted_host** command above.
Parameters	None.
Restrictions	None.

Example usage:

To display the list of trusted hosts:

```
DGS-2000-28MP:5# show trusted_host
Command: show trusted_host


Trusted Host Status : Disable

Management Stations

IP Address                  Subnet Mask
------------------------------ ------------------------------
10.90.90.91                 255.255.255.255
3000::1                     128

Total Entries: 2

DGS-2000-28MP:5#
```

delete trusted_host

Purpose	To delete a trusted host entry made using the **create trusted_host** command above.
Syntax	**delete trusted_host [<ipaddr> | network <network_address> | <ip6_addr> | ipv6_prefix <ipv6networkaddr> | all]**
Description	The **delete trusted_host** command deletes a trusted host entry made using the **create trusted_host** command above.
Parameters	*<ipaddr>* − The IP address of the trusted host. *network <network_address>* − The subnet mask of the trusted host to be deleted. This parameter is optional. *<ip6_addr>* − The IPv6 address of the trusted host to be removed. *ipv6_prefix <ipv6networkaddr>* − The IPv6 subnet prefix address of the trusted network to be removed. The network address of the trusted network. The form of network address is xxx.xxx.xxx.xxx/y. *all* − The all IP address of the trusted host.
Restrictions	Only administrator or operator level users can issue this command.

Example usage:

To delete a trusted host with an IPv4 address **10.90.90.91**:

```
DGS-2000-28MP:5# delete trusted_host 10.90.90.91
Command: delete trusted_host 10.90.90.91

Success.
DGS-2000-28MP:5#
```

51

POE COMMANDS

The PoE (Power over Ethernet) commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameter
config poe ports	[all | <portlist>] {clear_time_range | power_limit [auto | class_1 | class_2 | class_3 | class_4 | user_define <value 1-30>] | priority [high | normal | low] | state [enable | disable] | time_range <range_name 32>}
config por system	[legacy_pd [enable | disable] | power_disconnect_method [deny_low_priority_port | deny_next_port] | power_limit <sting>]
show poe ports	[all | <portlist>]
show poe system	

Each command is listed in detail, as follows:

config poe ports

Purpose	Used to configure the Power over Ethernet (PoE) functionality.
Syntax	**config poe ports [all | <portlist>] [state {enable | disable}] [time_range <range_name 32> | clear_time_range | priority {High | Normal | low} | power_limit {Auto | class_1 | class_2 | class_3 | class_4 | user_define <value 1-30>} | delay_power_detect {enable | disable}]**
Description	The config poe ports configures the Power over Ethernet (PoE) functionality of the Switch.
Parameters	*port* – Specify the port(s) for PoE parameters *all* – Specify all ports <*portlist*> − Specify the port, or a range of ports. *state* –Specifies whether power will be supplied to the powered device connected to this port or not *enable* - Specifies that PoE will be enabled of the specifies port(s). *disable* - Specifies that PoE will be disabled of the specifies port(s). *time_range <range_name 32>* - To configure the time-based PoE function on designated port(s). *clear_time_range* – Used to delete the time range for specified port(s). *priority* - Port priority determines the priority the system attempts to supply the power to the port. *High* –Specifies that the priority value will be set to high. *Normal* –Specifies that the priority value will be set to normal. *Low* - Specifies that the priority value will be set to low. *power_limit* - Specifies the power limit with different class *auto* –Automatic classification the PD's power consumption. *class_1* - Specifies that the power limit will be set to 4W

	class_2 - Specifies that the power limit will be set to 7W *class_3* - Specifies that the power limit will be set to 15.4W *class_4* –For 802.3at compliance PD devices. Supports up to 30W in this class. *user_define* <*value 1-30*> –Specifies the user defined power limit value here. Maximum capability for power output is 30W (802.3AT)
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure PoE with ports 8-10:

DGS-2000-28MP:5# config poe ports 8-10 power_limit Auto priority low state enable

Command: config poe ports 8-10 power_limit Auto priority low state enable

Success!

DGS-2000-28MP:5#

config poe system

Purpose	Used to configure the Power over Ethernet (PoE) parameter for entire system.
Syntax	**config poe system [legacy_pd [enable | disable] | power_disconnect_method [deny_low_priority_port | deny_next_port] | power_limit <string>]**
Description	The config poe system configures the Power over Ethernet (PoE) functionality of the Switch.
Parameters	*legacy_pd* - Specifies the legacy PDs detection status. *enable* - Specifies that the legacy PDs detection status will be enabled. *disable* − Specifies that the legacy PDs detection status will be disabled and can't detect the legacy PDs signal. *power_disconnect_method* - Specifies the disconnection method that will be used when the power budget is running out. *deny_low_priority_port* - The port with the lower priority will be shut down to allow the higher priority port to power up. *deny_next_port* - When the power budget is exceeded, the next port attempting to power up is denied, regardless of the port priority. *power_limit* <*string*> - Configure the system power budge.Different mdoel has different power limit. Please refer to hardware specification.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure PoE with ports 8-10:

```
DGS-2000-28MP:5# config poe system power_limit 193
Command: config poe system power_limit 193


Success!

DGS-2000-28MP:5#
```

show poe ports

Purpose	Used to display the ports of Power over Ethernet (PoE).
Syntax	**show poe ports [all | <portlist>]**
Description	The show poe ports displays the Power over Ethernet (PoE) ports of the Switch.
Parameters	*[all* | *<portlist>]* – Specifies the ports or all ports to be displayed.
Restrictions	None.

Example usage:

To display the PoE with ports 8:

```
DGS-2000-28MP:5# show poe ports 8
Command: show poe ports 8


Port: 8
State              : Enable
Priority           : Low
Power Limit        : Auto
Power(W)           : 0.0
Voltage(V)         : 0.0
Current(mA)        : 0.0
Status             : POWER OFF
Time Range         : N/A

Success!

DGS-2000-28MP:5#
```

show poe system

Purpose	Used to display the system information of Power over Ethernet (PoE).
Syntax	**show poe system**
Description	The show poe system displays the Power over Ethernet (PoE) system information of the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display the PoE system of Switch:

```
DGS-2000-28MP:5# show poe system
Command: show poe system

Power Limit                    : 193
Power Consumption              : 0
Power Remained                 : 0
Power Disconnection Method     : Deny Next Port
Detection Legacy PD            : Disable

Success!

DGS-2000-28MP:5#
```

52

DEBUG COMMANDS

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

Command	Parameter
debug	[http | https | module | snmp | ssh | system| telnet | trace]
show tech support	
clear tech support	

Each command is listed in detail, as follows:

debug config semaphore	
Purpose	To retrieve the debg for mudels.
Syntax	**debug** [http | https | module | snmp | ssh | system| telnet | trace]
Description	This command is used to retrieve the debg for mudels. Or running built-in debug process. Please consult with D-Link authorized technician or tech support team before proceed these commands.
Parameters	None.
Restrictions	None.

Example usage:

To proceed the debug command:

```
DGS-2000-28MP:5# debug system diag
Command: debug system diag

Diag Result:
Memory Pool : [Allocate fail]
================================================================================

Memory Pool Allocate fail:
Pool 23 Allocate Fail Count: 28
Pool 277 Allocate Fail Count: 6
Pool 278 Allocate Fail Count: 6
================================================================================

Cru Buf:Occupy 0.000000%  [ok]
ok      -- occupy bellow 20% , normal
busy    -- occupy between 21% to 50%,Need confirm buff is occuping by which task

warning -- occupy between 50% to 99%,MUST confirm buff is occuping by which task

error   -- occupy over 99%, buffer run out, fix it
================================================================================

Lock: [ok]
================================================================================

Reboot : [COLD]
cold       - power off and on
warm       - user reboot
watchdog   - watchdog reboot
DGS-2000-28MP:5#
```

show tech support

Purpose	To display system and configuration information. to provide to the Technical Assistance Center when reporting a problem, use the show tech-support command.
Syntax	**show tech support**
Description	The **show tech support** command displays system and configuration information to provide to the Technical Assistance Center when reporting a problem. By default, this command displays the output for technical-support-related show commands. Use keywords to specify the type of information to be displayed. If you do not specify any parameters, the system displays all configuration and memory data. The **show tech support** command may time out if the configuration file output takes longer to display than the configured session timeout time. If this happens, enter a set logout *timeout* value of 0 to disable automatic disconnection of idle sessions or enter a longer

	timeout value. The **show tech support** command output is continuous; it does not display one screen at a time. To interrupt the output, press Esc.
Parameters	None.
Restrictions	None.

Example usage:

To display technical support information on the Switch:

```
DGS-2000-28MP:5# show tech support
Command: show tech support

================================================================================

Error Trace Log
================================================================================

================================================================================

SLI TABLE
================================================================================

SOCKET STATE TYPE       ERROR QUE NUM
------ ----- ----------- ----- -------
3     1    SOCK_DGRAM  0    0
4     1    SOCK_DGRAM  -39   0
5     1    SOCK_DGRAM  0    0
6     1    SOCK_DGRAM  0    0
7     1    SOCK_DGRAM  0    0
8     1    SOCK_DGRAM  0    0
9     1    SOCK_DGRAM  0    0
10    1     SOCK_DGRAM  0    0
11    1     SOCK_DGRAM  0    0
12    1     SOCK_DGRAM  0    0
13    1     SOCK_DGRAM  0    0
14    1     SOCK_DGRAM  0    0
15    1     SOCK_DGRAM  0    0
16    1     SOCK_DGRAM  0    0
17    1     SOCK_DGRAM  0    0
18    3     SOCK_STREAM 0    0
19    3     SOCK_STREAM 0    0
20    3     SOCK_STREAM 0    0
21    3     SOCK_STREAM 0    0
22    3     SOCK_STREAM 0    0
23    1     SOCK_DGRAM  0    0
24    3     SOCK_STREAM 0    0
25    1     SOCK_DGRAM  0    0
26    1     SOCK_RAW    0    0
27    1     SOCK_RAW    0    0
```

```
28    1    SOCK_DGRAM  0    0
29    1    SOCK_DGRAM  0    0
30    1    SOCK_DGRAM  0    0
================================================================================

TCP TABLE
================================================================================

INDEX TYPE STATE SOCKET RX/TX BUFF SIZE RX/TX BUFF Cnt REMOTE IP:PORT/LOCAL IP:P
ORT
----- ---- ----- ------ --------------  -------------- -------------------------
-----
1    0   2    18     9216 ~ 0         0 ~ 0     0.0.0.0:0~0.0.0.0:80
2    0   2    19       0 ~ 0         0 ~ 0     0.0.0.0:0~0.0.0.0:80
3    0   2    20       0 ~ 0         0 ~ 0     0.0.0.0:0~0.0.0.0:23
4    0   2    21       0 ~ 0         0 ~ 0     0.0.0.0:0~0.0.0.0:23
5    0   2    22     9216 ~ 0         0 ~ 0     0.0.0.0:0~0.0.0.0:22
6    0   2    24    65535 ~ 0         0 ~ 0     0.0.0.0:0~0.0.0.0:22

- Stacktrace Log -

No stacktrace information.

- System Info. -

Device Type            : DGS-2000-28MP
MAC Address            : F4-8C-EB-E9-EE-00
IP Address             : 10.90.90.90
VLAN Name              : default
Subnet Mask            : 255.0.0.0
Default Gateway        : 0.0.0.0
System Boot Version    : 1.00.001
System Firmware Version  : 1.00.009
System Hardware Version  : A1
System Serial Number   : TM1C1JA000043
System Name            :
System Location        :
System Up Time         : 0 days, 2 hrs, 47 min, 10 secs
System Contact         :
System Time            : 02:46:38 01 01 2019
IGMP Snooping          : Disabled
802.1X Status          : Disabled
Telnet                 : Enabled  <TCP  23>
SSH                    : Enabled  <TCP  22>
Web                    : Enabled  <TCP  80>
RMON                   : Disabled
Syslog Global State    : Disabled
CLI Paging             : Enabled
```

```
- Memory Info. -
        total      used      free     shared    buffers
Mem:     255572    151600    103972         0      9008
Swap:         0         0         0
Total:   255572    151600    103972
DGS-2000-28MP:5#
```

clear tech support

Purpose	To clear system and configuration information.
Syntax	**clear tech support**
Description	The **clear tech support** command is used to clear system and configuration information.
Parameters	None.
Restrictions	None.

Example usage:

To clear technical support information on the Switch:

```
DGS-2000-28MP:5# clear tech support
Command: clear tech support


Success.

DGS-2000-28MP:5#
```

53

DEVICE SPECIFICATIONS

This appendix contains the device specifications, and contains the following topics:

- **Technical Specifications**
- **Supported Transceivers**

Technical Specifications

Performance	
Transmission Method	Store-and-forward
Packet Buffer memory	DGS-2000-10: 4.1 Mbits DGS-2000-10P: 4.1 Mbits DGS-2000-10MP: 4.1 Mbits DGS-2000-20: 4.1 Mbits DGS-2000-26: 4.1 Mbitss DGS-2000-28: 4.1 Mbits DGS-2000-28P: 4.1 Mbits DGS-2000-28MP: 4.1 Mbits DGS-2000-52: 12 Mbits DGS-2000-52MP: 12 Mbits
64 Bytes Max. Packet Forwarding Rate	Full-wire speed for all connections. DGS-2000-10: 14.88 Mpps DGS-2000-10P: 14.88 Mpps DGS-2000-10MP: 14.88 Mpps DGS-2000-20: 29.8 Mpps DGS-2000-26: 38.7 Mpps DGS-2000-28: 41.7 Mpps DGS-2000-28P: 41.7 Mpps DGS-2000-28MP: 41.7 Mpps DGS-2000-52: 77.4 Mpps DGS-2000-52MP: 77.4 Mpps
MAC Address Learning	Automatic update. Supports 8K MAC address.
DRAM	256 MB – DDR3
Flash Memory	32 MB – SPI flash
Priority Queues	8 Priority Queues per port.
Forwarding Table Age Time	Max age: 10–600 seconds. Default = 300.

Physical and Environmental	
Power Consumption	DGS-2000-10: Standby power consumption: 2.03 Watts DGS-2000-10P:

Physical and Environmental	
	Maximum power consumption: 81.9 Watts (PoE On),7.6 Watts (PoE Off) Standby power consumption: 2.5 Watts DGS-2000-10MP: Maximum power consumption: 152.3 Watts (PoE On), 9.4 Watts (PoE Off) Standby power consumption: 5.2 Watts DGS-2000-20: Standby power consumption: 5.47 Watts DGS-2000-26: Standby power consumption: 5.01 Watts DGS-2000-28: Standby power consumption: 6.49 Watts DGS-2000-28P: Maximum power consumption: 263.9 Watts (PoE On), 30.6 Watts (PoE Off) Standby power consumption: 19.6 Watts DGS-2000-28MP: Maximum power consumption: 446.1 Watts (PoE On), 29.8 Watts (PoE Off) Standby power consumption: 18.5 Watts DGS-2000-52: Standby power consumption: 13.7 Watts DGS-2000-52MP: Maximum power consumption: 478.9 Watts (PoE On), 54.4 Watts (PoE Off) Standby power consumption: 32 Watts
Fans	DGS-2000-28P: 2pcs Smart Fan DGS-2000-28MP: 2pcs Smart Fan DGS-2000-52: 2pcs Smart Fan DGS-2000-52MP: 2pcs Smart Fan
Operating Temperature	-5 to 50 degrees Celsius
Storage Temperature	-40 to 70 degrees Celsius
Humidity	Storage: 5% to 95% non-condensing
Dimensions	DGS-2000-10: 280 x 126 x 44 mm DGS-2000-10P: 280 x 126 x 44 mm DGS-2000-10MP: 330 x 180 x 44 mm DGS-2000-20: 280 x 180 x 44 mm DGS-2000-26: 440 x 140 x 44 mm DGS-2000-28: 440 x 140 x 44 mm DGS-2000-28P: 440 x 250 x 44 mm DGS-2000-28MP: 440 x 250 x 44 mm DGS-2000-52:440 x 210 x 44 mm DGS-2000-52MP: 440 x 430 x 44 mm

Physical and Environmental	
Weight	DGS-2000-10: 0.98 kg DGS-2000-10P: 0.95 kg DGS-2000-10MP: 1.77 kg DGS-2000-20: 1.75 kg DGS-2000-26: 2.06 kg DGS-2000-28: 2.15 kg DGS-2000-28P: 3.75 kg DGS-2000-28MP: 3.94 kg DGS-2000-52: 3.46 kg DGS-2000-52MP: 6.26 kg
EMI	CE, FCC, VCCI, BSMI
Safety	UL, CB, LVD, BSMI

General	
10/100/1000BASE-TX Ethernet ports	8 x 10/100/1000BaseT ports for DGS-2000-10, DGS-2000-10P and DGS-2000-10MP 20 x 10/100/1000BaseT ports for DGS-2000-20 24 x 10/100/1000BaseT ports for DGS-2000-26 28 x 10/100/1000BaseT ports for DGS-2000-28, DGS-2000-28P, DGS-2000-28MP 52 x 10/100/1000BaseT ports for DGS-2000-52, DGS-2000-52MP
SFP ports	Port 9 ~ 10 for DGS-2000-10, DGS-2000-10P and DGS-2000-10MP Port 17 ~ 20 for DGS-2000-20 Port 25 ~ 26 for DGS-2000-26 Port 25 ~ 28 for DGS-2000-28, DGS-2000-28P, DGS-2000-28MP Port 49 ~ 52 for DGS-2000-52 and DGS-2000-52MP
Standards	• IEEE 802.3 10BASE-T Ethernet • IEEE 802.3u 100BASE-TX Fast Ethernet • IEEE 802.3ab 1000BASE-T Gigabit Ethernet • IEEE 802.3ah • IEEE 802.3x Flow Control for full-duplex mode, auto-negotiation
Protocols	CSMA/CD
Duplex Mode	Full/half-duplex for 10/100Mbps and full-duplex for 1000Mbps speed
Topology	Star

Network Cables
• UTP Cat. 3, Cat. 4, Cat. 5, Cat. 5e (100m max.) • EIA/TIA-568 150-ohm STP (100m max.)

Supported Transceivers

Optional SFP Transceivers	
DEM-310GT	1000BASE-LX, Single-mode, 10 km
DEM-311GT	1000BASE-SX, Multi-mode, 500 m
DEM-312GT2	1000BASE-SX, Multi-mode, 2 km
DEM-312GT2	1000BASE-LHX, Single-mode, 50 km
DEM-315GT	1000BASE-ZX, Single-mode, 80 km
DGS-712	1000BASE-T 100 m (only supports 1000 Mbps mode) (no flow control)
DEM-302S-LX	1000BASE-LX, Single-mode, 2 km

Optional WDM SFP Transceivers	
DEM-330T	1000BASE-LX, Single-mode, 10 km, Tx: 1550, Rx:1310 nm
DEM-330R	1000BASE-LX, Single-mode, 10 km, Tx: 1310, Rx: 1550 nm
DEM-331T	1000BASE-LX, Single-mode, 40 km, Tx: 1550, Rx: 1310 nm
DEM-331R	1000BASE-LX, Single-mode, 40 km, Tx: 1310, Rx: 1550 nm
DEM-302S-BXD	1000BASE-LX, Single-mode, 2 km, Tx: 1550, Rx: 1310 nm
DEM-302S-BXU	1000BASE-LX, Single-mode, 2 km, Tx: 1310, Rx: 1550 nm