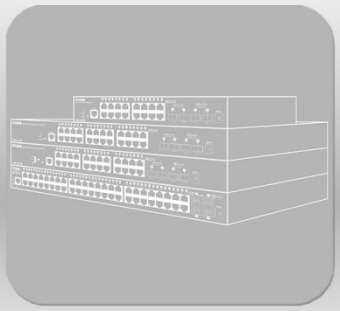
D-Link®
Building Networks for People



CLI Reference Guide

Product Model: DGS-3000 Series

Gigabit Ethernet Switch

Release 4.00

Table of Contents

Chapter 1 Using Command Line Interface 1
Chapter 2 Basic Command List 8
Chapter 3 802.1Q VLAN Command List 27
Chapter 4 802.1X Command List 43
Chapter 5 AAA Accounting Command List 58
Chapter 6 Access Authentication Control Command List 76
Chapter 7 Access Control List (ACL) Command List 97
Chapter 8 Address Resolution Protocol (ARP) Command List 116
Chapter 9 ARP Spoofing Prevention Command List 121
Chapter 10 Auto-Backup Command List 124
Chapter 11 Auto-Configuration Command List 134
Chapter 12 Auto-Image Command List 137
Chapter 13 Basic Commands Command List 140
Chapter 14 BPDU Attack Protection Command List 159
Chapter 15 Cable Diagnostics Command List 164
Chapter 16 Command Logging Command List 166
Chapter 17 Compound Authentication Command List 168
Chapter 18 Configuration Command List 176
Chapter 19 Connectivity Fault Management (CFM) Command List 181
Chapter 20 Connectivity Fault Management (CFM) Extension Command List 204
Chapter 21 CPU Interface Filtering Command List 212
Chapter 22 Debug Software Command List 221
Chapter 23 DHCP Local Relay Command List 228
Chapter 24 DHCP Relay Command List 234
Chapter 25 DHCP Server Command List 249
Chapter 26 DHCP Server Screening Command List 268
Chapter 27 DHCPv6 Relay Command List 280
Chapter 28 Digital Diagnostic Monitoring (DDM) Commands 297
Chapter 29 D-Link Discovery Protocol (DDP) Client Command List 303
Chapter 30 D-Link Unidirectional Link Detection (DULD) Command List 307
Chapter 31 Domain Name System (DNS) Resolver Command List 310
Chapter 32 DoS Attack Prevention Command List 317
Chapter 33 Energy Efficient Ethernet (EEE) Command List 321
Chapter 34 Ethernet Ring Protection Switching (ERPS) Command List 323
Chapter 35 Filter Command List 344
Chapter 36 Filter Database (FDB) Command List 347
Chapter 37 Flash File System (FFS) Command List 357
Chapter 38 Flex Link Command List 366
Chapter 39 Gratuitous ARP Command List 369

Chapter 40 IGMP Snooping Command List 374
Chapter 41 IP-MAC-Port Binding (IMPB) Command List 400
Chapter 42 IPv6 Neighbor Discover Command List 428
Chapter 43 Jumbo Frame Command List 432
Chapter 44 Layer 2 Protocol Tunneling (L2PT) Command List 434
Chapter 45 Link Aggregation Command List 438
Chapter 46 Link Layer Discovery Protocol (LLDP) Command List 445
Chapter 47 LLDP-MED Command List 463
Chapter 48 Loop Back Detection (LBD) Command List 471
Chapter 49 MAC Notification Command List 477
Chapter 50 MAC-based Access Control Command List 482
Chapter 51 MAC-based VLAN Command List 497
Chapter 52 Mirror Command List 500
Chapter 53 MLD Snooping Command List 503
Chapter 54 MSTP debug enhancement Command List 525
Chapter 55 Multicast Filter Command List 531
Chapter 56 Multicast VLAN Command List 542
Chapter 57 Multiple Spanning Tree Protocol (MSTP) Command List 563
Chapter 58 Network Load Balancing (NLB) Command List 575
Chapter 59 Network Monitoring Command List 580
Chapter 60 Network Time Protocol (NTP) Command List 586
Chapter 61 OAM Commands 603
Chapter 62 Password Recovery Command List 610
Chapter 63 Peripherals Command List 612
Chapter 64 Ping Command List 615
Chapter 65 Port Security Command List 618
Chapter 66 Power over Ethernet (PoE) Command List (DGS-3000-28LP and DGS-3000-28XMP Only) 626
Chapter 67 Power Saving Command List 633
Chapter 68 PPPoE Circuit ID Insertions Command List 640
Chapter 69 Protocol VLAN Command List 643
Chapter 70 QinQ Command List 649
Chapter 71 Quality of Service (QoS) Command List 657
Chapter 72 RADIUS Client Command List 676
Chapter 73 RSPAN Command List 685
Chapter 74 Safeguard Engine Command List 691
Chapter 75 Secure Shell (SSH) Command List 693
Chapter 76 Secure Sockets Layer (SSL) Command List 701
Chapter 77 sFlow Command List 708
Chapter 78 Show Technical Support Command List 720
Chapter 79 Simple Mail Transfer Protocol (SMTP) Command List 723
Chapter 80 Simple Network Management Protocol (SNMP) Command List 728
Chapter 81 Single IP Management Command List 754

Chapter 82 Static Route Command List 765
Chapter 83 Syslog and Trap Source-interface Command List 771
Chapter 84 System Log Command List 775
Chapter 85 System Severity Command List 795
Chapter 86 Telnet Client Command List 797
Chapter 87 TFTP/FTP Client Command List 798
Chapter 88 Time and SNTP Command List 808
Chapter 89 Trace Route Command List 815
Chapter 90 Traffic Control Command List 818
Chapter 91 Traffic Segmentation Command List 823
Chapter 92 Trusted Host Command List 825
Chapter 93 UDP Helper Command List 829
Chapter 94 VLAN Trunking Command List 835
Chapter 95 Voice VLAN Command List 840
Chapter 96 Web-based Access Control (WAC) Command List 850
Chapter 97 Zero Touch Provisioning (ZTP) Command List 865
Appendix A Password Recovery Procedure 868
Appendix B System Log Entries 869
Appendix C Trap Log Entries 878
Appendix D RADIUS Attributes Assignment 883
Appendix E IETF RADIUS Attributes Support 885
Appendix F ERPS Information 887

Chapter 1 Using Command Line Interface

The Switch can be managed through the Switch's serial port, Telnet, SNMP 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. Every command will be introduced in terms of purpose, format, description, parameters, and examples. Configuration and management of the Switch via the Web-based management agent are discussed in the Web UI Reference Guide. For detailed information on installing hardware please also refer to the Hardware Installation Guide.

1-1 Accessing the Switch via the Serial Port

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

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

A computer running a terminal emulation program capable of emulating a VT-100 terminal and a serial port configured as above are then connected to the Switch's Console port via an included RS-232 to RJ-45 convertor cable.

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

```
                        DGS-3000-28XMP Gigabit Ethernet Switch
                                Command Line Interface

                                Firmware: Build 4.00.010
                Copyright(C) 2018 D-Link Corporation. All rights reserved.
UserName:
PassWord:

DGS-3000-28XMP:admin#
```

There is no initial username or password. Just press the **Enter** key twice to display the CLI input cursor – **DGS-3000-28XMP:admin#**. This is the command line where all commands are input.

1-2 Setting the Switch's IP Address

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

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

```
  Boot Procedure                                          V4.00.001
-------------------------------------------------------------------------------

  Power On Self Test ....................................  100 %

  MAC Address   : F0-7D-68-15-10-00
  H/W Version   : B1

  Please Wait, Loading V4.00.010 Runtime Image ..............  100 %
  UART init .................................................  100 %
  Starting runtime image
  Device Discovery ..........................................  100 %
  Configuration init ........................................      |
```

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

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

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

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

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

```
DGS-3000-28XMP:admin# config ipif System ipaddress 10.24.22.100/255.0.0.0
Command: config ipif System ipaddress 10.24.22.100/8

Success.

DGS-3000-28XMP:admin#
```

In the above example, the Switch was assigned an IP address of 10.24.22.100 with a subnet mask of 255.0.0.0. The system message **Success** indicates that the command was executed successfully. The Switch can now be configured and managed via Telnet, SNMP MIB browser and the CLI or via the Web-based management agent using the above IP address to connect to the Switch.

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

```
..
?
cable_diag ports
cd
cfm linktrace
cfm lock md
cfm loopback
clear
clear address_binding dhcp_snoop binding_entry ports
clear address_binding nd_snoop binding_entry ports
clear arptable
clear attack_log
clear cfm pkt_cnt
clear counters
clear dhcp binding
clear dhcp conflict_ip
clear ethernet_oam ports
clear fdb
clear igmp_snooping data_driven_group
clear igmp_snooping statistics counter
clear log
clear mac_based_access_control auth_state
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

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

```
DGS-3000-28XMP:admin#config account
Command: config account
Next possible completions:
<username>

DGS-3000-28XMP:admin#
```

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

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

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

```
DGS-3000-28XMP:admin#config account
Command: config account
Next possible completions:
<username>

DGS-3000-28XMP:admin#config account
```

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

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

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

```
DGS-3000-28XMP:admin#the
Available commands:
..                  ?                   cable_diag          cd
cfm                 clear               config              copy
create              debug               del                 delete
dir                 disable             download            enable
erase               erps                login               logout
md                  move                no                  ping
ping6               rd                  reboot              reconfig
rename              reset               save                show
smtp                telnet              traceroute          traceroute6
upload

DGS-3000-28XMP:admin#
```

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-3000-28XMP:admin#show
Command: show
Next possible completions:
802.1p              802.1x              aaa                 access_profile
account             accounting          acct_client         address_binding
arp_spoofing_prevention                 arpentry            attack_log
auth_client         auth_diagnostics    auth_session_statistics
auth_statistics     authen              authen_enable       authen_login
authen_policy       authentication      authorization       autobackup
autoconfig          autoimage           bandwidth_control   boot_file
bpdu_protection     cfm                 command             command_history
config              cpu                 cpu_filter          current_config
ddm                 ddp                 device_status       dhcp
dhcp_local_relay    dhcp_relay          dhcp_server
dhcpv6_local_relay                      dhcpv6_relay        dos_prevention
dot1v_protocol_group                    dscp                duld
eee                 environment         erps                error
ethernet_oam        exec_banner         fdb                 filter
flex_link           flow_meter          gratuitous_arp      greeting_message
gvrp                hol_prevention      host_name           igmp
igmp_snooping       ip_tcp_pmtu_discovery                   ipif
ipif_ipv6_link_local_auto               iproute             ipv6
ipv6route           jumbo_frame         l2protocol_tunnel   lacp_port
led                 limited_multicast_addr                  link_aggregation
lldp                lldp_med            log                 log_console
log_discriminator   log_monitor         log_save_timing
log_software_module                     loopdetect
mac_based_access_control                mac_based_access_control_local
mac_based_vlan      mac_notification    max_mcast_group
mcast_filter_profile                    mirror              mld_snooping
multicast           multicast_fdb       name_server         nlb
ntp                 outgoing_session_timeout                packet
password_recovery   per_queue           poe                 port
port_security       port_security_entry                     port_vlan
ports               power_saving        pppoe               private_vlan
pvid                qinq                radius              reset_button
rmon                router_ports        rspan               safeguard_engine
scheduling          scheduling_mechanism                    serial_port
session             sflow               sim                 smtp
snmp                sntp                ssh                 ssl
storage_media_info                      stp                 switch
syslog              system_severity     tech_support        terminal
tftp                time                time_range          traffic
traffic_segmentation                    trap                trusted_host
udp_helper          utilization         vlan                vlan_translation
vlan_trunk          voice_vlan          wac

DGS-3000-28XMP:admin#
```

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

1-3 Command Syntax Symbols

Each CLI command available on this switch contains certain syntax symbols that might be unfamiliar to the inexperienced user. Each syntax symbol carries a meaning and by knowing that meaning we can better understand how the command is used. All commands are case-sensitive. Be sure to disable the **Caps Lock** key or any other unwanted function that changes text case.

Syntax	Description
angle brackets < >	This syntax is used to enclose a variable or a value. Users must enter the variable or value. For example, in the **config command_prompt [<string 16> | username | default]** command, users must enter the command prompt string value and NOT the parameter <string 16>.
square brackets [ ]	This syntax is used to enclose a required value or list of required arguments. Only one value or argument must be specified. For example, in the **config command_prompt [<string 16> | username | default]** command, users must enter either the command prompt string, select the username, or select the default option. Do not type the square brackets.
vertical bar |	This syntax is used to separate mutually exclusive items in a list. For example, in the **reset {[config | system]} {force_agree}** command, users may choose **config** or **system** in the command. Do not type the vertical bar.
braces { }	This syntax is used to enclose an optional value or a list of optional arguments. One or more values or arguments can be specified. For example, in the **reset {[config | system]} {force_agree}** command, users may choose config or system in the command. Do not type the braces.
parentheses ( )	This syntax is used to indicate that at least one or more of the values or arguments in the preceding syntax enclosed by braces must be specified. For example, in the **config dhcp_relay {hops <int 1-16> | time <sec 0-65535>}(1)** command, users have the option to specify hops or time or both of them. The "(1)" following the set of braces indicates at least one argument or value within the braces must be specified. Do not type the parentheses.
ipif <ipif_name 12>	In this syntax example, the value **12** means that the IP interface name can be up to 12 characters long.
metric <value 1-31>	In this syntax example, the values **1-31** means that the metric value must be between 1 and 31.

1-4 Line Editing Keys

Keys	Description
Delete	This key is used to delete the character under the cursor and to shift the remainder of the line to the left.
Backspace	This key is used to delete the character to the left of cursor and shift the remainder of the line to the left.
CTRL+R	This key is used to replace text characters with newly typed text or to insert newly typed text within the existing sentence. This is similar to the **Insert** key.
Up Arrow	This key is used to repeat 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	This key is used to display the next command in the command history entered in the current session. This displays each command sequentially as it was entered. Use the up arrow to review previous commands.

Left Arrow	This key is used to move the cursor to the left.
Right Arrow	This key is used to move the cursor to the right.
Tab	This key is used to help users to select the appropriate token.

1-5 Multiple Page Display Control Keys

When CLI paging is enabled, the screen display will pause when the show command output reaches the end of the page, as shown below.

```
DGS-3000-28XMP:admin#show stp ports
Command: show stp ports

 MSTP Port Information
 ----------------------
 Port Index     : 1     , Hello Time: 2 /2 , Port STP : Enabled  ,
 External PathCost : Auto/200000   , Edge Port : True /No , P2P : Auto /Yes
 Port RestrictedRole : False,  Port RestrictedTCN : False
 Port Forward BPDU : Disabled
 MSTI   Designated Bridge   Internal PathCost  Prio  Status      Role
 -----  ------------------  -----------------  ----  ----------  ----------
 0      N/A                 200000             128   Forwarding  NonStp


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

The following control keys will then be available:

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

Chapter 2 Basic Command List

show session
show serial_port
config serial_port {baud_rate [9600 | 19200 | 38400 | 115200] | auto_logout [never | 2_minutes | 5_minutes | 10_minutes | 15_minutes]}
enable clipaging
disable clipaging
login
logout
?
clear
show command_history
config command_history <value 1-40>
config greeting_message {default}
show greeting_message
config command_prompt [<string 16> | username | default]
config terminal width [default | <value 80-200>]
show terminal width
config ports [<portlist> | all] {medium_type [fiber | copper]} {speed [auto | 10_half | 10_full | 100_half | 100_full | 1000_full {[master | slave]} | 10g_full] | flow_control [enable | disable] | learning [enable | disable] | state [enable | disable] | mdix [auto | normal | cross] | [description <desc 1-100> | clear_description]}(1)
show ports {<portlist>} {[description | err_disabled | details | media_type]}
config exec_banner {default}
show exec_banner
config outgoing_session_timeout <value 0-1439> [console | telnet | ssh]
show outgoing_session_timeout
enable monitor
disable monitor

2-1 show session

Description

This command is used to display a list of all users currently logged into the Switch.

Format

show session

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To display the session entries:

```
DGS-3000-28XMP:admin#show session
Command: show session

 ID  Live Time    From                                    Level Name
 --- ------------ --------------------------------------- ----- ---------------
 8   00:03:29.400 Serial Port                             admin Anonymous

Total Entries: 1




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

2-2 show serial_port

Description

This command is used to display the current serial port settings.

Format

show serial_port

Parameters

None.

Restrictions

None.

Example

To display the serial port setting:

```
DGS-3000-28XMP:admin#show serial_port
Command: show serial_port

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

DGS-3000-28XMP:admin#
```

2-3 config serial_port

Description

This command is used to configure the serial bit rate that will be used to communicate with the management host and the automatic logout time for idle connections.

Format

config serial_port {baud_rate [9600 | 19200 | 38400 | 115200] | auto_logout [never | 2_minutes | 5_minutes | 10_minutes | 15_minutes]}

Parameters

baud_rate - (Optional) Specifies the serial bit rate that will be used to communicate with the management host. The default baud rate is 115200.

9600 - Specifies the serial bit rate to be 9600.

19200 - Specifies the serial bit rate to be 19200.

38400 - Specifies the serial bit rate to be 38400.

115200 - Specifies the serial bit rate to be 115200.

auto_logout - (Optional) Specifies the automatic logout time.

never - Never time out.

2_minutes - Specifies that the device will automatically log out after being idle for longer than 2 minutes.

5_minutes - Specifies that the device will automatically log out after being idle for longer than 5 minutes.

10_minutes - Specifies that the device will automatically log out after being idle for longer than 10 minutes.

15_minutes - Specifies that the device will automatically log out after being idle for longer than 15 minutes.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure baud rate:

```
DGS-3000-28XMP:admin# config serial_port baud_rate 9600
Command: config serial_port baud_rate 9600

Success.

DGS-3000-28XMP:admin#
```

2-4 enable clipaging

Description

This command is used to enable the pausing of the screen display when the show command output reaches the end of the page. The default setting is enabled.

Format

enable clipaging

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

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

```
DGS-3000-28XMP:admin# enable clipaging
Command: enable clipaging

Success.

DGS-3000-28XMP:admin#
```

2-5 disable clipaging

Description

This command is used to disable the pausing of the screen display when the show command output reaches the end of the page. The default setting is enabled.

Format

disable clipaging

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

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

```
DGS-3000-28XMP:admin# disable clipaging
Command: disable clipaging

Success.

DGS-3000-28XMP:admin#
```

2-6 login

Description

This command is used to log in the Switch.

Format

login

Parameters

None.

Restrictions

None.

Example

To log in the Switch with a user name dlink:

```
DGS-3000-28XMP:admin# login
Command: login

UserName:dlink
PassWord:****

DGS-3000-28XMP:admin#
```

2-7 logout

Description

This command is used to log out the Switch.

Format

logout

Parameters

None.

Restrictions

None.

Example

To log out the current user:

```
DGS-3000-28XMP:admin# logout
Command: logout


**********
* Logout *
**********

                              DGS-3000-28XMP Gigabit Ethernet Switch
                                     Command Line Interface

                                    Firmware: Build 4.00.010
                  Copyright(C) 2018 D-Link Corporation. All rights reserved.
UserName:
```

2-8 ?

Description

This command is used to display the description for all commands or the specified command.

Format

?

Parameters

None.

Restrictions

None.

Example

To get “ping” command usage, descriptions:

```
DGS-3000-28XMP:admin#? ping
Command: ? ping

Command: ping
Usage:  [<ipaddr> | <domain_name 255>] { times <value 1-255> | timeout <sec 1-99>}
Description: Used to test the connectivity between network devices.

DGS-3000-28XMP:admin#
```

2-9 clear

Description

This command is used to clear the screen.

Format

clear

Parameters

None.

Restrictions

None.

Example

To clear screen:

```
DGS-3000-28XMP:admin# clear
Command: clear



DGS-3000-28XMP:admin#
```

2-10 show command_history

Description

This command is used to display command history.

Format

show command_history

Parameters

None.

Restrictions

None.

Example

To display command history:

```
DGS-3000-28XMP:admin# show command_history
Command: show command_history

? ping
login
show serial_port
show session
? config bpdu_protection ports
? reset
? create account
? create ipif
show
the
?

DGS-3000-28XMP:admin#
```

2-11 config command_history

Description

This command is used to configure the number of commands that the Switch can recall. The Switch “remembers” up to the last 40 commands you entered.

Format

config command_history <value 1-40>

Parameters

<value 1-40> - Enter the number of commands that the Switch can recall. This value must be between 1 and 40.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the number of command history:

```
DGS-3000-28XMP:admin# config command_history 25
Command: config command_history 25

Success.

DGS-3000-28XMP:admin#
```

2-12 config greeting_message

Description

This command is used to configure the greeting message (or banner).

Format

config greeting_message {default}

Parameters

default - (Optional) Specifies to return the greeting message (banner) to its original factory default entry.

Restrictions

Only Administrators and Operators can issue this command.

Example

To edit the banner:

```
DGS-3000-28XMP:admin#config greeting_message
Command: config greeting_message

Greeting Messages Editor
================================================================================

                    DGS-3000-28XMP Gigabit Ethernet Switch
                             Command Line Interface

                            Firmware: Build 4.00.010
           Copyright(C) 2018 D-Link Corporation. All rights reserved.
================================================================================

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

2-13 show greeting_message

Description

This command is used to display the greeting message.

Format

show greeting_message

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To display greeting message:

```
DGS-3000-28XMP:admin#show greeting_message
Command: show greeting_message

================================================================================

                    DGS-3000-28XMP Gigabit Ethernet Switch
                             Command Line Interface

                           Firmware: Build 4.00.010
          Copyright(C) 2018 D-Link Corporation. All rights reserved.
================================================================================

DGS-3000-28XMP:admin#
```

2-14 config command_prompt

Description

This command is used to modify the command prompt.

The current command prompt consists of four parts: “product name” + “:” + ”user level” + ”#” (e.g. “DGS-3000-28XMP:admin# ”). This command is used to modify the first part (1. “product name”) with a string consisting of a maximum of 16 characters, or to be replaced with the login user name.

When issuing the **reset** command, the current command prompt will remain the same. However, when issuing the **reset system** command, the command prompt will return to its original factory default value.

Format

config command_prompt [<string 16> | username | default]

Parameters

<string 16> - Enter the new command prompt string of no more than 16 characters.
username - Specifies to set the login username as the command prompt.
default - Specifies to return the command prompt to its original factory default value.

Restrictions

Only Administrators and Operators can issue this command.

Example

To edit the command prompt:

```
DGS-3000-28XMP:admin# config command_prompt Prompt#
Command: config command_prompt Prompt#

Success.

Prompt#:admin#
```

2-15 config terminal width

Description

This command is used to set the current terminal width.

The usage is described as below:

1. When a user logs in and configure the terminal width to 120, this configuration will take effect for this login section. If the user enters the “save” command, the configuration is saved. After the user logs out and logs in again, the terminal width is 120.
2. If the user did not save the configuration and another user logs in, the default value is used for the terminal width.
3. If two CLI sessions are running at the same time and the terminal width is changed in one of the sessions and saved, the other section will not be effected until the next login.

Format

config terminal width [default | <value 80-200>]

Parameters

default - Specifies to use the default value of the terminal width. The default value is 80.
<value 80-200> - Enter the terminal width. The width is between 80 and 200 characters.

Restrictions

None.

Example

To configure the current terminal width:

```
DGS-3000-28XMP:admin# config terminal width 120
Command: config terminal width 120

Success.

DGS-3000-28XMP:admin#
```

2-16 show terminal width

Description

This command is used to display the configuration of the current terminal width.

Format

show terminal width

Parameters

None.

Restrictions

None.

Example

To display the configuration of current terminal width:

```
DGS-3000-28XMP:admin# show terminal width
Command: show terminal width

Global terminal width     : 80
Current terminal width    : 80

DGS-3000-28XMP:admin#
```

2-17 config ports

Description

This command is used to configure the Switch's port settings.

NOTE: A standard MIB limits the length of the port description to 64 characters.

Format

config ports [<portlist> | all] {medium_type [fiber | copper]} {speed [auto | 10_half | 10_full | 100_half | 100_full | 1000_full {[master | slave]} | 10g_full] | flow_control [enable | disable] | learning [enable | disable] | state [enable | disable] | mdix [auto | normal | cross] | [description <desc 1-100> | clear_description]}(1)

Parameters

<portlist> - Enter a list of ports used here.
all - Specifies that all the ports will be used for this configuration.
medium_type - (Optional) Specifies which medium type will be used on the combo port. **fiber** - Specifies that the medium type will be set to fiber. **copper** - Specifies that the medium type will be set to copper.
speed - (Optional) Specifies the port speed of the specified ports. **auto** - Specifies the port speed to auto-negotiation. **10_half** - Specifies the port speed to 10_half. **10_full** - Specifies the port speed to 10_full.

100_half - Specifies the port speed to 100_half.

100_full - Specifies the port speed to 100_full.

1000_full - Specifies the port speed to 1000_full. While setting the port speed to 1000_full, the master or slave mode should be specified for the 1000BASE-TX ports, and leave the 1000_full without any master or slave setting for other ports.

master - Specifies that the port(s) will be set to master.

slave - Specifies that the port(s) will be set to slave.

10g_full - Specifies the port speed to 10g_full.

flow_control - (Optional) Specifies to turn on or turn off flow control on one or more ports.

enable - Specifies that the flow control option will be enabled.

disable - Specifies that the flow control option will be disabled.

learning - (Optional) Specifies to turn on or turn off MAC address learning on one or more ports.

enable - Specifies that the learning option will be enabled.

disable - Specifies that the learning option will be disabled.

state - (Optional) Specifies to enable or disable the specified port. If the specified ports are in the error-disabled status, setting their state to enable will recover these ports from disabled to enable state.

enable - Specifies that the port state will be enabled.

disable - Specifies that the port state will be disabled.

mdix - (Optional) Specifies the MDIX mode.

auto - Specifies the MDIX mode for the port to be auto.

normal - Specifies the MDIX mode for the port to be normal. If set to normal state, the port is in the MDIX mode and can be connected to a PC's NIC using a straight-through cable or a port (in the MDIX mode) on another switch through a cross-over cable.

cross - Specifies the MDIX mode for the port to be cross. If set to cross state, the port is in the MDI mode and can be connected to a port (in the MDIX mode) on another switch through a straight cable.

description - (Optional) Specifies the description of the port interface.

<desc 1-100> - Enter the port interface description. This value can be up to 100 characters long.

clear_description - (Optional) Specifies that the description field will be cleared.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the ports:

```
DGS-3000-28XMP:admin# config ports all medium_type copper speed auto
Command: config ports all medium_type copper speed auto

Success.

DGS-3000-28XMP:admin#
```

2-18 show ports

Description

This command is used to display the current configuration of all ports or the specified ports.

Format

show ports {<portlist>} {[description | err_disabled | details | media_type]}

Parameters

ports - Specifies a range of ports to be displayed. **<portlist>** - (Optional) Enter the range of ports to be displayed.
description - (Optional) Specifies if port description will be included in the display. **err_disabled** - (Optional) Specifies to display error-disabled ports. **details** - (Optional) Specifies to display the port details. **media_type** - (Optional) Specifies to display the port media type and SFP/SFP+ information.

Restrictions

None.

Example

To display the port details:

```
DGS-3000-28XMP:admin#show ports details
Command: show ports details

Port : 1
--------------------
Port Status                 : Link Up
Description                 :
HardWare Type               : Gigabits Ethernet
MAC Address                 : F0-7D-68-15-10-01
Bandwidth                   : 100000Kbit
Auto-Negotiation            : Enabled
Duplex Mode                 : Full Duplex
Flow Control                : Disabled
MDI                         : Cross
Address Learning            : Enabled
Last Clear of Counter       : 2 hours 34 mins ago
BPDU Hardware Filtering Mode: Disabled
Queuing Strategy            : FIFO
TX Load                     :   0/100,          0 bits/sec,        0 packets/sec
RX Load                     :   0/100,          0 bits/sec,        0 packets/sec


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

To display the media type and SFP/SFP+ information of ports 24 to 28:

```
DGS-3000-28XMP:admin#show ports 24-28 media_type
Command: show ports 24-28 media_type

 Port     Type           Vendor name/       PN/                SN/
                         OUI                Rev                Date Code
 ------  --------------  -----------------  -----------------  -----------------
 24      1000Base-T             -                  -                  -
                                -                  -                  -
 25      SFP LC          FINISAR CORP./     FTLF8519P2BCL-EX/  PGK3CVJ/
                         0 :90:65           A                  091106
         Compatibility: Multi-Mode,1300Mbd, 850nm
 26      SFP LC          FINISAR CORP./     FTLX8571D3BCL/     ARK1CC0/
                         0 :90:65           A                  140507
         Compatibility: Single Mode (SM),10300Mbd, 850nm
 27      10GBase-R              -                  -                  -
                                -                  -                  -
 28      10GBase-R              -                  -                  -
                                -                  -                  -

DGS-3000-28XMP:admin#
```

2-19 config exec_banner

Description

This command is used toconfigure the EXEC banner. The modified banner will be only saved in DRAM by pressing CTRL+W. Enter the **save** command to save the banner in NV-RAM.

Format

config exec_banner {default}

Parameters

default - (Optional) Specifies to revert to the default value.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the EXEC banner:

```
DGS-3000-28XMP:admin#config exec_banner
Command: config exec_banner

Exec Banner Editor
================================================================================
This is D-Link switch.




================================================================================

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

Success.

DGS-3000-28XMP:admin#
```

2-20 show exec_banner

Description

This command is used to display the EXEC banner.

Format

show exec_banner

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To display the EXEC banner:

```
DGS-3000-28XMP:admin#show exec_banner
Command: show exec_banner

================================================================================
This is D-Link switch.
================================================================================

DGS-3000-28XMP:admin#
```

2-21 config outgoing_session_timeout

Description

This command is used to configure the timeout value to close specified sessions that is established for logging into another device.

Format

config outgoing_session_timeout <value 0-1439> [console | telnet | ssh]

Parameters

<value 0-1439> - Specifies the outgoing session timeout value. The value is between 0 and 1439. 0 represents never timeout.
console - Specifies that the timeout occurs through the Console connection to the Switch.
telnet - Specifies that the timeout occurs through a Telnet connection to the Switch.
ssh - Specifies that the timeout occurs through an SSH connection to the Switch.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the timeout value of the SSH outgoing session:

```
DGS-3000-28XMP:admin#config outgoing_session_timeout 200 ssh
Command: config outgoing_session_timeout 200 ssh

Success.

DGS-3000-28XMP:admin#
```

2-22 show outgoing_session_timeout

Description

This command is used to display timeout values of outgoing sessions.

Format

show outgoing_session_timeout

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To display timeout values of outgoing sessions:

```
DGS-3000-28XMP:admin#show outgoing_session_timeout
Command: show outgoing_session_timeout

 Outgoing session timeout:
 From       Timeout
 ---------  ---------------
 Console    0(Never)
 Telnet     0(Never)
 SSH        200 minutes

DGS-3000-28XMP:admin#
```

2-23 enable monitor

Description

This command is used to enable debugging and system log messages for current Telnet/SSH sessions.

Format

enable monitor

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable the monitor mode:

```
DGS-3000-28XMP:admin#enable monitor
Command: enable monitor

Success.

DGS-3000-28XMP:admin#
```

2-24 disable monitor

Description

This command is used to disable debugging and system log messages for current Telnet/SSH sessions.

Format

disable monitor

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To disable the monitor mode:

```
DGS-3000-28XMP:admin#disable monitor
Command: disable monitor

Success.

DGS-3000-28XMP:admin#
```

Chapter 3 802.1Q VLAN Command List

create vlan <vlan_name 32> tag <vlanid 2-4094> {type [1q_vlan | private_vlan]} {advertisement}
create vlan vlanid <vidlist> {type [1q_vlan | private_vlan]} {advertisement}
delete vlan <vlan_name 32>
delete vlan vlanid <vidlist>
config vlan <vlan_name 32> {[add [tagged | untagged | forbidden] | delete] <portlist> | advertisement [enable | disable]}(1)
config vlan vlanid <vidlist> {[add [tagged | untagged | forbidden] | delete] <portlist> | advertisement [enable | disable] | name <vlan_name 32>}(1)
config port_vlan [<portlist> | all] {gvrp_state [enable | disable] | ingress_checking [enable | disable] | acceptable_frame [tagged_only | admit_all] | pvid <vlanid 1-4094>}(1)
show vlan {<vlan_name 32>}
show vlan ports {<portlist>}
show vlan vlanid <vidlist>
show port_vlan {<portlist>}
enable pvid auto_assign
disable pvid auto_assign
show pvid auto_assign
config gvrp [timer {join < value 100-100000> | leave < value 100-100000> | leaveall <value 100-100000>} | nni_bpdu_addr [dot1d | dot1ad]]
show gvrp
enable gvrp
disable gvrp
config private_vlan [<vlan_name 32> | vid <vlanid 2-4094>] [add [isolated | community] | remove] [<vlan_name 32> | vlanid <vidlist>]
show private_vlan {[<vlan_name 32> | vlanid<vidlist>]}

3-1 create vlan

Description

This command is used to create a VLAN on the Switch. The VLAN ID must be always specified when creating a VLAN.

Format

create vlan <vlan_name 32> tag <vlanid 2-4094> {type [1q_vlan | private_vlan]} {advertisement}

Parameters

<vlan_name 32> - Enter the VLAN name to be created. The VLAN name can be up to 32 characters long.
tag - Specifies the VLAN ID of the VLAN to be created. **<vlanid 2-4094>** - Enter the VLAN ID here. The VLAN ID value must be between 2 and 4094.

type - (Optional) Specifies the type of VLAN here.
1q_vlan - Specifies that the type of VLAN used is based on the 802.1Q standard.
private_vlan - Specifies that the private VLAN type will be used.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To create a VLAN with name “v2” and VLAN ID 2:

```
DGS-3000-28XMP:admin# create vlan v2 tag 2 type 1q_vlan advertisement
Command: create vlan v2 tag 2 type 1q_vlan advertisement

Success.

DGS-3000-28XMP:admin#
```

3-2 create vlan vlanid

Description

This command is used to create more than one VLAN at a time. A unique VLAN name (e.g. VLAN10) will be automatically assigned by the system. The automatic assignment of a VLAN name is based on the following rule: “VLAN”+ID. For example, for VLAN ID 100, the VLAN name will be VLAN100. If this VLAN name is conflicting with the name of an existing VLAN, then it will be renamed based on the following rule: “VLAN”+ID+”ALT”+ collision count. For example, if this conflict is the second collision, then the name will be VLAN100ALT2.

Format

create vlan vlanid <vidlist> {type [1q_vlan | private_vlan]} {advertisement}

Parameters

<vidlist> - Enter the VLAN ID list to be created.

type - (Optional) Specifies the type of VLAN to be created.
1q_vlan - Specifies that the VLAN created will be a 802.1Q VLAN.
private_vlan - Specifies that the private VLAN type will be used.

advertisement - (Optional) Specifies the VLAN as being able to be advertised.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To create some VLANs using VLAN ID:

```
DGS-3000-28XMP:admin# create vlan vlanid 10-30
Command: create vlan vlanid 10-30

Success.

DGS-3000-28XMP:admin#
```

3-3 delete vlan

Description

This command is used to delete a previously configured VLAN by its name on the Switch.

Format

delete vlan <vlan_name 32>

Parameters

<vlan_name 32> - Enter the name of the VLAN to be deleted. This name can be up to 32 characters long.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To remove the VLAN called “v1”:

```
DGS-3000-28XMP:admin# delete vlan v1
Command: delete vlan v1

Success.

DGS-3000-28XMP:admin#
```

3-4 delete vlan vlanid

Description

This command is used to delete one or more previously configured VLAN by VID list.

Format

delete vlan vlanid <vidlist>

Parameters

<vidlist> - Enter the VLAN ID list to be deleted.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To remove VLANs from 10-30:

```
DGS-3000-28XMP:admin# delete vlan vlanid 10-30
Command: delete vlan vlanid 10-30

Success.

DGS-3000-28XMP:admin#
```

3-5 config vlan

Description

This command is used to configure a VLAN based on the name.

Format

config vlan <vlan_name 32> {[add [tagged | untagged | forbidden] | delete] <portlist> | advertisement [enable | disable]}(1)

Parameters

<vlan_name 32> - Enter the VLAN name. This name can be up to 32 characters long.
add - Specifies to add tagged, untagged or forbidden ports to the VLAN. **tagged** - Specifies the additional ports as tagged. **untagged** - Specifies the additional ports as untagged. **forbidden** - Specifies the additional ports as forbidden.
delete - Specifies to delete ports from the VLAN.
<portlist> - Enter the list of ports used for the configuration here.
advertisement - Specifies the Generic VLAN Registration Protocol (GVRP) state of this VLAN. **enable** - Specifies to enable advertisement for this VLAN. **disable** - Specifies to disable advertisement for this VLAN.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To add ports 4 to 8 as tagged ports to the VLAN v2:

```
DGS-3000-28XMP:admin# config vlan v2 add tagged 4-8
Command: config vlan v2 add tagged 4-8

Success.

DGS-3000-28XMP:admin#
```

3-6 config vlan vlanid

Description

This command is used to configure multiple VLANs at the same time. Conflicts will be generated if you configure the name of multiple VLANs at the same time.

Format

config vlan vlanid <vidlist> {[add [tagged | untagged | forbidden] | delete] <portlist> | advertisement [enable | disable] | name <vlan_name 32>}(1)

Parameters

<vidlist> - Enter a list of VLAN IDs to configure.
add - Specifies to add tagged, untagged or forbidden ports to the VLAN. **tagged** - Specifies the additional ports as tagged. **untagged** - Specifies the additional ports as untagged. **forbidden** - Specifies the additional ports as forbidden.
delete - Specifies to delete ports from the VLAN.
<portlist> - Enter the list of ports used for the configuration here.
advertisement - Specifies the GVRP state of this VLAN. **enable** - Specifies to enable advertisement for this VLAN. **disable** - Specifies to disable advertisement for this VLAN.
name - Specifies the new name of the VLAN. **<vlan_name 32>** - Enter the VLAN name here. This name can be up to 32 characters long.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To add ports 4 to 8 as tagged ports to the VLAN ID from 10-20:

```
DGS-3000-28XMP:admin# config vlan vlanid 10-20 add tagged 4-8
Command: config vlan vlanid 10-20 add tagged 4-8

Success.

DGS-3000-28XMP:admin#
```

3-7 config port_vlan

Description

This command is used to set the ingress checking status, the sending and receiving GVRP information.

Format

config port_vlan [<portlist> | all] {gvrp_state [enable | disable] | ingress_checking [enable | disable] | acceptable_frame [tagged_only | admit_all] | pvid <vlanid 1-4094>}(1)

Parameters

<portlist> - Enter a range of ports for which you want ingress checking. The port list is specified by listing the beginning port number on the Switch, separated by a colon. Then highest port number of the range (also separated by a colon) is specified. The beginning and end of the port list range are separated by a dash. **all** - Specifies all ports for ingress checking.
gvrp_state - Specifies to enable or disable GVRP for the ports specified in the port list. **enable** - Specifies that GVRP for the specified ports will be enabled. **disable** - Specifies that GVRP for the specified ports will be disabled.
ingress_checking - Specifies to enable or disable ingress checking for the specified port list. **enable** - Specifies that ingress checking will be enabled for the specified port list. **disable** - Specifies that ingress checking will be disabled for the specified port list.
acceptable_frame - Specifies the type of frame that will be accepted by the port. There are two types: **tagged_only** - Specifies that only tagged packets will be accepted by this port. **admit_all** - Specifies that all packets will be accepted.
pvid - Specifies the Port VLAN ID (PVID) of the ports. **<vlanid 1-4094>** - Enter the VLAN ID here. The VLAN ID value must be between 1 and 4094.

Restrictions

Only Administrators and Operators can issue this command.

Example

To set the ingress checking status, the sending and receiving GVRP information:

```
DGS-3000-28XMP:admin# config port_vlan 1-5 gvrp_state enable ingress_checking enable
acceptable_frame tagged_only pvid 2
Command: config port_vlan 1-5 gvrp_state enable ingress_checking enable acceptable_frame
tagged_only pvid 2


Success.


DGS-3000-28XMP:admin#
```

3-8 show vlan

Description

This command is used to display the VLAN information , including parameter settings and operational values.

Format

show vlan {<vlan_name 32>}

Parameters

<vlan_name 32> - (Optional) Enter the VLAN name to be displayed. The VLAN name can be up to 32 characters long.

Restrictions

None.

Example

To display VLAN settings:

```
DGS-3000-28XMP:admin# show vlan
Command: show vlan


VLAN Trunk State        : Enabled
VLAN Trunk Member Ports : 1-5


VID             : 1               VLAN Name     : default
VLAN Type       : Static          Advertisement : Enabled
Member Ports    : 1-28
Static Ports    : 1-28
Current Tagged Ports  :
Current Untagged Ports: 1-28
Static Tagged Ports   :
Static Untagged Ports : 1-28
Forbidden Ports       :

VID             : 2               VLAN Name     : v2
VLAN Type       : Static          Advertisement : Enabled
Member Ports    : 4-8
Static Ports    : 4-8
Current Tagged Ports  : 4-8
Current Untagged Ports:
Static Tagged Ports   : 4-8
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

3-9 show vlan ports

Description

This command is used to display the VLAN information per port.

Format

show vlan ports {<portlist>}

Parameters

<portlist> - (Optional) Enter the list of ports for which the VLAN information will be displayed.

Restrictions

None.

Example

To display the VLAN configuration for port 6:

```
DGS-3000-28XMP:admin# show vlan ports 6
Command: show vlan ports 6

 Port   VID   Untagged  Tagged  Dynamic  Forbidden
-----   ----  --------  ------  -------  ---------
 6      1       X         -       -        -
 6      2       -         X       -        -

DGS-3000-28XMP:admin#
```

3-10 show vlan vlanid

Description

This command is used to display the VLAN information using the VLAN ID.

Format

show vlan vlanid <vidlist>

Parameters

<vidlist> - Enter the VLAN ID to be displayed.

Restrictions

None.

Example

To display the VLAN configuration for VLAN ID 1:

```
DGS-3000-28XMP:admin# show vlan vlanid 1
Command: show vlan vlanid 1


VID             : 1               VLAN Name     : default
VLAN Type       : Static          Advertisement : Enabled
Member Ports    : 1-28
Static Ports    : 1-28
Current Tagged Ports  :
Current Untagged Ports: 1-28
Static Tagged Ports   :
Static Untagged Ports : 1-28
Forbidden Ports       :

 Total Entries : 1


DGS-3000-28XMP:admin#
```

3-11 show port_vlan

Description

This command is used to display the ports' VLAN attributes on the Switch. If no parameter is specified, the system will display the GVRP information of all ports.

Format

show port_vlan {<portlist>}

Parameters

<portlist> - (Optional) Enter a range of ports to be displayed.

Restrictions

None.

Example

To display 802.1Q port setting:

```
DGS-3000-28XMP:admin# show port_vlan
Command: show port_vlan

Port     PVID  GVRP      Ingress Checking  Acceptable Frame Type
-------  ----  --------  ----------------  --------------------------
 1       2     Enabled   Enabled           Only VLAN-tagged Frames
 2       2     Enabled   Enabled           Only VLAN-tagged Frames
 3       2     Enabled   Enabled           Only VLAN-tagged Frames
 4       2     Enabled   Enabled           Only VLAN-tagged Frames
 5       2     Enabled   Enabled           Only VLAN-tagged Frames
 6       1     Disabled  Enabled           All Frames
 7       1     Disabled  Enabled           All Frames
 8       1     Disabled  Enabled           All Frames
 9       1     Disabled  Enabled           All Frames
 10      1     Disabled  Enabled           All Frames
 11      1     Disabled  Enabled           All Frames
 12      1     Disabled  Enabled           All Frames
 13      1     Disabled  Enabled           All Frames
 14      1     Disabled  Enabled           All Frames
 15      1     Disabled  Enabled           All Frames
 16      1     Disabled  Enabled           All Frames
 17      1     Disabled  Enabled           All Frames
 18      1     Disabled  Enabled           All Frames
 19      1     Disabled  Enabled           All Frames
 20      1     Disabled  Enabled           All Frames
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

3-12 enable pvid auto assign

Description

This command is used to enable the auto-assignment of PVID.

If “Auto-assign PVID” is enabled, PVID will be possibly changed by PVID or VLAN configuration. When the user configures a port to VLAN X’s untagged membership, this port’s PVID will be updated with VLAN X. In the form of VLAN list command, PVID is updated with the last item of the VLAN list. When the user removes a port from the untagged membership of the PVID’s VLAN, the port’s PVID will be assigned with “default VLAN”.

The default setting is enabled.

Format

enable pvid auto_assign

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable auto-assign PVID:

```
DGS-3000-28XMP:admin# enable pvid auto_assign
Command: enable pvid auto_assign

Success.

DGS-3000-28XMP:admin#
```

3-13 disable pvid auto assign

Description

This command is used to disable auto-assignment of PVID.

Format

disable pvid auto_assign

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To disable the auto-assign PVID:

```
DGS-3000-28XMP:admin# disable pvid auto_assign
Command: disable pvid auto_assign

Success.

DGS-3000-28XMP:admin#
```

3-14 show pvid auto_assign

Description

This command is used to display the PVID auto-assignment state.

Format

show pvid auto_assign

Parameters

None.

Restrictions

None.

Example

To display PVID auto-assignment state:

```
DGS-3000-28XMP:admin# show pvid auto_assign
Command: show pvid auto_assign

PVID Auto-assignment: Enabled

DGS-3000-28XMP:admin#
```

3-15 config gvrp

Description

This command is used to configure the GVRP timer's value.

Format

config gvrp [timer {join < value 100-100000> | leave < value 100-100000> | leaveall <value 100-100000>} | nni_bpdu_addr [dot1d | dot1ad]]

Parameters

timer - Specifies that the GVRP timer parameter will be configured.
join - (Optional) Specifies that the Join time will be set. **<value 100-100000>** - Enter the time in milliseconds here. This value must be between 100 and 100000. The default value is 200.
leave - (Optional) Specifies that the Leave time will be set. **<value 100-100000>** - Enter the time in milliseconds here. This value must be between 100 and 100000. The default value is 600.
leaveall - (Optional) Specifies that the Leave All time will be set. **<value 100-100000>** - Enter the time in milliseconds here. This value must be between 100 and 100000. The default value is 10000.
nni_bpdu_addr - Specifies to determine the BPDU protocol address for GVRP at the service provider's site. It can use 802.1d GVRP address, 802.1ad service provider GVRP address or a user-defined multicast address. The range of the user-defined address is 0180C2000000 - 0180C2FFFFFF. **dot1d** - Specifies that the NNI BPDU protocol address value will be set to Dot1d. **dot1ad** - Specifies that the NNI BPDU protocol address value will be set to Dot1ad.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To set the Join time to 200 milliseconds:

```
DGS-3000-28XMP:admin# config gvrp timer join 200
Command: config gvrp timer join 200

Success.

DGS-3000-28XMP:admin#
```

3-16 show gvrp

Description

This command is used to display the GVRP global setting.

Format

show gvrp

Parameters

None.

Restrictions

None.

Example

To display the global setting of GVRP:

```
DGS-3000-28XMP:admin# show gvrp
Command: show gvrp

 Global GVRP   : Disabled
 Join Time     : 200 Milliseconds
 Leave Time    : 600 Milliseconds
 LeaveAll Time : 10000 Milliseconds
 NNI BPDU Address: dot1d

DGS-3000-28XMP:admin#
```

3-17 enable gvrp

Description

This command is used to enable the Generic VLAN Registration Protocol (GVRP).

Format

enable gvrp

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable the generic VLAN Registration Protocol (GVRP):

```
DGS-3000-28XMP:admin# enable gvrp
Command: enable gvrp

Success.

DGS-3000-28XMP:admin#
```

3-18 disable gvrp

Description

This command is used to disable the Generic VLAN Registration Protocol (GVRP).

Format

disable gvrp

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To disable the Generic VLAN Registration Protocol (GVRP):

```
DGS-3000-28XMP:admin# disable gvrp
Command: disable gvrp

Success.

DGS-3000-28XMP:admin#
```

3-19 config private_vlan

Description

This command is used to add or remove a secondary VLAN from a private VLAN.

Use the **create vlan <vlan_name 32> tag <vlanid 2-4094> type private_vlan** command to create a primary private VLAN.

A private VLAN is comprised by a primary VLAN, an optional isolated VLAN, and a number of community VLANs.

A secondary VLAN cannot be associated with multiple primary VLANs.

The untagged member port of the primary VLAN is called the promiscuous port. The tagged member port of the primary VLAN is called the trunk port.

A promiscuous port of a private VLAN cannot be a promiscuous port of other private VLANs.

The primary VLAN member port cannot be a secondary VLAN member port at the same time.

The untagged member port of the secondary VLAN must be an isolated port or a community port.

When a VLAN is associated with a primary VLAN as the secondary VLAN, the promiscuous port of the primary VLAN will function as the untagged member of the secondary VLAN and the trunk port of the primary VLAN will function as the tagged member of the secondary VLAN.

A secondary VLAN cannot have the advertisement feature enabled.

Only the primary VLAN can be configured as a Layer 3 interface.

The private VLAN member port cannot be included in the traffic segmentation function.

Format

config private_vlan [<vlan_name 32> | vid <vlanid 2-4094>] [add [isolated | community] | remove] [<vlan_name 32> | vlanid <vidlist>]

Parameters

<vlan_name 32> - Enter the name of the private VLAN.
vid - Specifies the VLAN ID of the private VLAN. **<vlanid 2-4094>** - Enter the VLAN ID. This value must be between 2 and 4094.
add - Specifies that a secondary VLAN will be added to the private VLAN. **isolated** - Specifies the secondary VLAN as an isolated VLAN. **community** - Specifies the secondary VLAN as a community VLAN.
remove - Specifies that a secondary VLAN will be removed from the private VLAN.
<vlan_name 32> - Enter the secondary VLAN name used. This name can be up to 32 characters long.
vlanid - A range of secondary VLANs to add or remove to the private VLAN. **<vidlist>** - Enter the secondary VLAN ID used here.

Restrictions

Only Administrators and Operators can issue this command.

Example

To associate secondary vlan to private vlan p1:

```
DGS-3000-28XMP:admin#config private_vlan p1 add community vlanid 3
Command: config private_vlan p1 add community vlanid 3

Success.

DGS-3000-28XMP:admin#
```

3-20 show private_vlan

Description

This command is used to show the private VLAN information.

Format

show private_vlan {[<vlan_name 32> | vlanid <vidlist>]}

Parameters

<vlan_name 32> - (Optional) Enter the name of the private VLAN or its secondary VLAN. This name can be up to 32 characters long.
vlanid - (Optional) Specifies the VLAN ID of the private VLAN or its secondary VLAN. **<vidlist>** - Enter the VLAN ID used here.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To display private VLAN settings:

```
DGS-3000-28XMP:admin#show private_vlan
Command: show private_vlan

Primary VLAN    2
----------------------------------------
 Promiscuous Ports   :
 Trunk Ports         :
 Isolated Ports      :                     Isolated VLAN    : 3
 Community Ports     :                     Community VLAN   : 4


 Total Entries: 1


DGS-3000-28XMP:admin#
```

Chapter 4 802.1X Command List

enable 802.1x
disable 802.1x
create 802.1x user <username 15>
delete 802.1x user <username 15>
show 802.1x user
config 802.1x auth_protocol [local | radius_eap]
config 802.1x fwd_pdu system [enable | disable]
config 802.1x fwd_pdu ports [<portlist> | all] [enable | disable]
config 802.1x authorization attributes radius [enable | disable]
show 802.1x {[auth_state | auth_configuration] ports {<portlist>}}
config 802.1x capability ports [<portlist> | all] [authenticator | none]
config 802.1x max_users [<value 1–448> | no_limit]
config 802.1x auth_parameter ports [<portlist> | all] [default | {direction [both | in] | port_control [force_unauth | auto | force_auth] | quiet_period <sec 0-65535> | tx_period <sec 1-65535> | supp_timeout <sec 1-65535> | server_timeout <sec 1-65535> | max_req <value 1-10> | reauth_period <sec 1-65535> | max_users [<value 1-448> | no_limit] | enable_reauth [enable | disable]}(1)]
config 802.1x auth_mode [port_based | mac_based]
config 802.1x init [port_based ports [<portlist> | all] | mac_based ports [<portlist> | all] {mac_address <macaddr>}]
config 802.1x reauth [port_based ports [<portlist> | all] | mac_based ports [<portlist> | all] {mac_address <macaddr>}]
create 802.1x guest_vlan {<vlan_name 32>}
delete 802.1x guest_vlan {<vlan_name 32>}
config 802.1x guest_vlan ports [<portlist> | all] state [enable | disable]
show 802.1x guest_vlan

4-1 enable 802.1x

Description

This command is used to enable the 802.1X function.

Format

enable 802.1x

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable the 802.1X function:

```
DGS-3000-28XMP:admin# enable 802.1x
Command: enable 802.1x

Success.

DGS-3000-28XMP:admin#
```

4-2 disable 802.1x

Description

This command is used to disable the 802.1X function.

Format

disable 802.1x

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To disable the 802.1X function:

```
DGS-3000-28XMP:admin# disable 802.1x
Command: disable 802.1x

Success.

DGS-3000-28XMP:admin#
```

4-3 create 802.1x user

Description

This command is used to create an 802.1X user.

Format

create 802.1x user <username 15>

Parameters

<username 15> - Enter the username to be added. This value can be up to 15 characters long.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To create an 802.1x user “test”:

```
DGS-3000-28XMP:admin# create 802.1x user test
Command: create 802.1x user test

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

DGS-3000-28XMP:admin#
```

4-4 delete 802.1x user

Description

This command is used to delete an 802.1X user.

Format

delete 802.1x user <username 15>

Parameters

<username 15> - Enter the username to be deleted. This value can be up to 15 characters long.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete user “test”:

```
DGS-3000-28XMP:admin# delete 802.1x user test
Command: delete 802.1x user test

Success.

DGS-3000-28XMP:admin#
```

4-5 show 802.1x user

Description

This command is used to display the 802.1X user.

Format

show 802.1x user

Parameters

None.

Restrictions

None.

Example

To display the 802.1X user information:

```
DGS-3000-28XMP:admin# show 802.1x user
Command: show 802.1x user

 Current Accounts:
 Username         Password
 ---------------  ---------------
 test             test

 Total Entries:1


DGS-3000-28XMP:admin#
```

4-6 config 802.1x auth_protocol

Description

This command is used to configure the 802.1X authentication protocol.

Format

config 802.1x auth_protocol [local | radius_eap]

Parameters

local - Specifies the authentication protocol as local.
radius_eap - Specifies the authentication protocol as RADIUS EAP.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the 802.1X authentication protocol to RADIUS EAP:

```
DGS-3000-28XMP:admin# config 802.1x auth_protocol radius_eap
Command: config 802.1x auth_protocol radius_eap

Success.

DGS-3000-28XMP:admin#
```

4-7 config 802.1x fwd_pdu system

Description

This command is used to globally control the forwarding of EAPOL PDU. When 802.1X functionality is disabled globally or for a port, and if 802.1X fwd_pdu is enabled both globally and for the port, a received EAPOL packet on the port will be flooded in the same VLAN to those ports for which 802.1X fwd_pdu is enabled and 802.1X is disabled (globally or just for the port). The default state is disabled.

Format

config 802.1x fwd_pdu system [enable | disable]

Parameters

enable - Specifies to enable the forwarding of EAPOL PDU.
disable - Specifies to disable the forwarding of EAPOL PDU.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure forwarding of EAPOL PDU system state enable:

```
DGS-3000-28XMP:admin# config 802.1x fwd_pdu system enable
Command: config 802.1x fwd_pdu system enable

Success.

DGS-3000-28XMP:admin#
```

4-8 config 802.1x fwd_pdu ports

Description

This command is used to control the forwarding of EAPOL PDU. When 802.1X functionality is disabled globally or for a port, and if 802.1X fwd_pdu is enabled both globally and for the port, a received EAPOL packet on the port will be flooded in the same VLAN to those ports for which 802.1X fwd_pdu is enabled and 802.1X is disabled (globally or just for the port). The default state is disabled.

Format

config 802.1x fwd_pdu ports [<portlist> | all] [enable | disable]

Parameters

<portlist> - Enter the list of ports used for the configuration.
all - Specifies that all the ports will be used.
enable - Specifies to enable forwarding EAPOL PDU receive on the ports.
disable - Specifies to disable forwarding EAPOL PDU receive on the ports.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure 802.1X fwd_pdu for ports:

```
DGS-3000-28XMP:admin# config 802.1x fwd_pdu ports 1-2 enable
Command: config 802.1x fwd_pdu ports 1-2 enable

Success.

DGS-3000-28XMP:admin#
```

4-9 config 802.1x authorization attributes radius

Description

This command is used to enable or disable acceptance of authorized configuration.

When the authorization is enabled for 802.1X's RADIUS authentication, the authorized attributes (for example VLAN, 802.1p default priority, and ACL) assigned by the RADUIS server will be accepted.

Format

config 802.1x authorization attributes radius [enable | disable]

Parameters

enable - Specifies to enable the authorization attributes. When enabled, the authorization attributes (for example VLAN, 802.1p default priority, and ACL) assigned by the RADUIS server will be accepted. This is the default.
disable - Specifies to disable the authorization attributes.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To disable the acceptance of authorized data assigned from the RADIUS server:

```
DGS-3000-28XMP:admin# config 802.1x authorization attributes radius disable
Command: config 802.1x authorization attributes radius disable

Success.

DGS-3000-28XMP:admin#
```

4-10 show 802.1x

Description

This command is used to display the 802.1X state or configurations. If no parameter is specified, the 802.1X system configurations will be displayed.

Format

show 802.1x {[auth_state | auth_configuration] ports {<portlist>}}

Parameters

auth_state - (Optional) Specifies to display 802.1X authentication state machine of some or all ports
auth_configuration - (Optional) Specifies to display 802.1X configurations of some or all ports.
port - (Optional) Specifies a range of ports to be displayed. If no port is specified, all ports will be displayed. **<portlist>** - Enter the list of ports used for the configuration here.

Restrictions

None.

Example

To display the 802.1X port level configurations:

```
DGS-3000-28XMP:admin# show 802.1x auth_configuration ports 1
Command: show 802.1x auth_configuration ports 1


Port Number    : 1
Capability     : None
AdminCrlDir    : Both
OpenCrlDir     : Both
Port Control   : Auto
QuietPeriod    : 60    sec
TxPeriod       : 30    sec
SuppTimeout    : 30    sec
ServerTimeout  : 30    sec
MaxReq         : 2     times
ReAuthPeriod   : 3600  sec
ReAuthenticate : Disabled
Forward EAPOL PDU On Port : Enabled
Max User On Port : 16









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

4-11 config 802.1x capability ports

Description

This command is used to configure the port capability.

Format

config 802.1x capability ports [<portlist> | all] [authenticator | none]

Parameters

<portlist> - Enter the list of ports used for the configuration here.
all - Specifies all ports to be configured.
authenticator - Specifies the port(s) to act as authenticator which enforces authentication before allowing access to services through that port.
none - Specifies to disable authentication on the specified ports.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the port capability:

```
DGS-3000-28XMP:admin# config 802.1x capability ports 1-10 authenticator
Command: config 802.1x capability ports 1-10 authenticator

Success.

DGS-3000-28XMP:admin#
```

4-12 config 802.1x max_users

Description

This command is used to limit the maximum number of users that can be learned via 802.1X authentication. In addition to the global limitation, the maximum users per port is also limited. It is specified by the **config 802.1x auth_parameter** command.

Format

config 802.1x max_users [<value 1–448> | no_limit]

Parameters

<value 1-448> - Enter the maximum number of users. This value must be between 1 and 448.
no_limit – Specifies that the user limit will be set to the maximum of 448.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

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

```
DGS-3000-28XMP:admin# config 802.1x max_users 200
Command: config 802.1x max_users 200

Success.

DGS-3000-28XMP:admin#
```

4-13 config 802.1x auth_parameter ports

Description

This command is used to configure the parameters that control the operation of the authenticator associated with a port.

Format

config 802.1x auth_parameter ports [<portlist> | all] [default | {direction [both | in] | port_control [force_unauth | auto | force_auth] | quiet_period <sec 0-65535> | tx_period <sec 1-65535> | supp_timeout <sec 1-65535> | server_timeout <sec 1-65535> | max_req <value 1-10> | reauth_period <sec 1-65535> | max_users [<value 1-448> | no_limit] | enable_reauth [enable | disable]}(1)]

Parameters

<portlist> - Enter the list of ports used for the configuration here.
all - Specifies that all the ports will be used.
default - Specifies that all parameters will be set to their default value.
direction - Specifies the direction of access control. **both** - Specifies bidirectional access control. **in** - Specifies unidirectional access control.
port_control - Specifies to force a specific port to be unconditionally authorized or unauthorized by setting the parameter of port_control to be force_authorized or force_unauthorized. Besides, the controlled port will reflect the outcome of authentication if port_control is auto. **force_unauth** - Specifies to force a specific port to be unconditionally unauthorized. **auto** - Specifies that the controlled port will reflect the outcome of authentication. **force_auth** - Specifies to force a specific port to be unconditionally authorized.
quiet_period - Specifies the initialization value of the quietWhile timer. **<sec 0-65535>** - Enter the quiet period value here. This value must be between 0 and 65535 seconds. The default value is 60 seconds.
tx_period - Specifies the initialization value of the transmit timer period. **<sec 1-65535>** - Enter the TX period value here. This value must be between 1 and 65535 seconds. The default value is 30 seconds.
supp_timeout - Specifies the initialization value of the aWhile timer when timing out the supplicant. **<sec 1-65535>** - Enter the supplicant timeout value here. This value must be between 1 and 65535 seconds. The default value is 30 seconds.
server_timeout - Specifies the initialization value of the aWhile timer when timing out the authentication server. **<sec 1-65535>** - Enter the server timeout value here. This value must be between 1 and 65535 seconds. The default value is 30.
max_req - Specifies the maximum number of times that the authentication PAE state machine will retransmit an EAP Request packet to the supplicant. **<value 1-10>** - Enter the maximum required value here. This value must be between 1 and 10. The default value is 2.
reauth_period - Specifies the re-authentication timer in seconds. **<sec 1-65535>** - Enter the re-authentication period value here. This value must be between 1 and 65535 seconds. The default value is 3600.
max_users - Specifies the maximum number of users per port. The default value is 16. **<value 1-448>** - Enter the maximum users value here. This value must be between 1 and 448. **no_limit** - Specifies that no limit is enforced on the maximum users.
enable_reauth - Specifies to enable or disable the re-authentication mechanism for a specific port. **enable** - Specifies to enable the re-authentication mechanism for a specific port. **disable** - Specifies to disable the re-authentication mechanism for a specific port.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

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

```
DGS-3000-28XMP:admin# config 802.1x auth_parameter ports 1-20 direction both
Command: config 802.1x auth_parameter ports 1-20 direction both

Success.

DGS-3000-28XMP:admin#
```

4-14 config 802.1x auth_mode

Description

This command is used to configure the 802.1X authentication mode.

Format

config 802.1x auth_mode [port_based | mac_based]

Parameters

port_based - Specifies to configure the authentication mode as port-based.
mac_based - Specifies to configure the authentication mode as MAC-based.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the authentication mode:

```
DGS-3000-28XMP:admin# config 802.1x auth_mode port_based
Command: config 802.1x auth_mode port_based

Success.

DGS-3000-28XMP:admin#
```

4-15 config 802.1x init

Description

This command is used to initialize the authentication state of some or all ports.

Format

config 802.1x init [port_based ports [<portlist> | all] | mac_based ports [<portlist> | all] {mac_address <macaddr>}]

Parameters

port_based ports- Specifies to configure the authentication mode as port-based.

<portlist> - Enter the list of ports used for the configuration here. **all** - Specifies that all ports will be used.
mac_based ports - Specifies to configure the authentication mode as MAC-based. **<portlist>** - Enter the list of ports used for the configuration here. **all** - Specifies that all ports will be used.
mac_address - (Optional) Specifies the MAC address of the client. **<macaddr>** - Enter the MAC address used here.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To initialize the authentication state of all ports:

```
DGS-3000-28XMP:admin# config 802.1x init port_based ports all
Command: config 802.1x init port_based ports all

Success.

DGS-3000-28XMP:admin#
```

4-16 config 802.1x reauth

Description

This command is used to re-authenticate a device connected to the port. During the re-authentication period, the port status remains authorized until re-authentication has failed.

Format

config 802.1x reauth [port_based ports [<portlist> | all] | mac_based ports [<portlist> | all] {mac_address <macaddr>}]

Parameters

port_based ports - Specifies to configure the authentication mode as port-based. **<portlist>** - Enter the list of ports used for the configuration here. **all** - Specifies that all ports will be used.
mac_based ports - Specifies to configure the authentication mode as MAC-based. **<portlist>** - Enter the list of ports used for the configuration here. **all** - Specifies that all ports will be used.
mac_address - (Optional) Specifies the MAC address of the client. **<macaddr>** - Enter the MAC address used here.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To re-authenticate the device connected to the port:

```
DGS-3000-28XMP:admin# config 802.1x reauth port_based ports all
Command: config 802.1x reauth port_based ports all

Success.

DGS-3000-28XMP:admin#
```

4-17 create 802.1x guest_vlan

Description

This command is used to assign a static VLAN as a guest VLAN. The specific VLAN which will be assigned as the guest VLAN must be pre-existing. The specific VLAN , assigned as a guest VLAN, cannot be deleted.

Format

create 802.1x guest_vlan {<vlan_name 32>}

Parameters

<vlan_name 32> - (Optional) Specifies the VLAN to be a guest VLAN. The VLAN name can be up to 32 characters long.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To create a VLAN named “guestVLAN” as an 802.1X guest VLAN:

```
DGS-3000-28XMP:admin# create 802.1x guest_vlan guestVLAN
Command: create 802.1x guest_vlan guestVLAN

Success.

DGS-3000-28XMP:admin#
```

4-18 delete 802.1x guest_vlan

Description

This command is used to delete a guest VLAN setting, but not the static VLAN assigned to the guest VLAN. All ports assigned to the guest VLAN will be reassigned to the original VLAN when the guest VLAN is deleted.

Format

delete 802.1x guest_vlan {<vlan_name 32>}

Parameters

<vlan_name 32> - (Optional) Enter the guest VLAN name here. The VLAN name can be up to 32 characters long.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete the guest VLAN named “guestVLAN”:

```
DGS-3000-28XMP:admin# delete 802.1x guest_vlan guestVLAN
Command: delete 802.1x guest_vlan guestVLAN

Success.

DGS-3000-28XMP:admin#
```

4-19 config 802.1x guest_vlan

Description

This command is used to configure guest VLAN settings. If the specific port state is changed from enabled to disabled, this port will be moved back to its original VLAN.

Format

config 802.1x guest_vlan ports [<portlist> | all] state [enable | disable]

Parameters

ports - Specifies a range of ports for which to enable or disable guest VLAN function.
- **<portlist>** - Enter the list of ports used for the configuration here.
- **all** - Specifies that all the ports will be included in this configuration.

state - Specifies the guest VLAN port state of the configured ports.
- **enable** - Specifies to join the guest VLAN.
- **disable** - Specifies to be removed from the guest VLAN.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable ports 2 to 8 for the 802.1X guest VLAN:

```
DGS-3000-28XMP:admin# config 802.1x guest_vlan ports 2-8 state enable
Command: config 802.1x guest_vlan ports 2-8 state enable

Warning, The ports are moved to Guest VLAN.

Success.

DGS-3000-28XMP:admin#
```

4-20 show 802.1x guest_vlan

Description

This command is used to show the information of guest VLANs.

Format

show 802.1x guest_vlan

Parameters

None.

Restrictions

None.

Example

To show 802.1X guest VLAN on the Switch:

```
DGS-3000-28XMP:admin# show 802.1x guest_vlan
Command: show 802.1x guest_vlan

Guest VLAN Setting
-----------------------------------------------------------
Guest VLAN : guestVLAN
Enabled Guest VLAN Ports : 2-8

DGS-3000-28XMP:admin#
```

Chapter 5 AAA Accounting Command List

create accounting method_list_name <string 15>
config accounting [default | method_list_name <string 15>] method {tacacs+ | radius | server_group <string 15> | none}(1)
delete accounting method_list_name <string 15>
show accounting [default | method_list_name <string 15> | all]
config accounting service [network | shell | system] state [enable {[radius_only | method_list_name <string 15> | default_method_list]} | disable]
config accounting service command {administrator | operator | power_user | user} [method_list_name <string 15> | none]
show accounting service
create tacacs server_host [<ipaddr> | <ipv6addr>] {port <int 1-65535> | timeout <int 1-255> | retransmit <int 1-20>}
config tacacs server_host [<ipaddr> | <ipv6addr>] {port <int 1-65535> | timeout <int 1-255> | retransmit <int 1-20>}
create xtacacs server_host [<ipaddr> | <ipv6addr>] {port <int 1-65535> | timeout <int 1-255> | retransmit <int 1-20>}
config xtacacs server_host [<ipaddr> | <ipv6addr>] {port <int 1-65535> | timeout <int 1-255> | retransmit <int 1-20>}
create tacacs+ server_host [<ipaddr> | <ipv6addr>] {port <int 1-65535> | key [<key_string 254> | none] | timeout <int 1-255> }
config tacacs+ server_host [<ipaddr> | <ipv6addr>] {port <int 1-65535> | key [<key_string 254> | none] | timeout <int 1-255>}
create radius server_host [<ipaddr> | <ipv6addr>] {auth_port <int 1-65535> | acct_port <int 1-65535> | key [<key_string 254> | none] | timeout <int 1-255> | retransmit <int 1-20>}
config radius server_host [<ipaddr> | <ipv6addr>] {auth_port <int 1-65535> | acct_port <int 1-65535> | key [<key_string 254> | none] | timeout <int 1-255> | retransmit <int 1-20>}
delete aaa server_host [<ipaddr> | <ipv6addr>] protocol [tacacs | xtacacs | tacacs+ | radius]
show aaa server_host
create aaa server_group <string 15>
config aaa server_group [tacacs | xtacacs | tacacs+ | radius | group_name <string 15>] [add | delete] server_host [<ipaddr> | <ipv6addr>] protocol [tacacs | xtacacs | tacacs+ | radius]
delete aaa server_group <string 15>
show aaa server_group {<string 15>}
show aaa

5-1 create accounting method_list_name

Description

This command is used to create a user-defined method list of accounting methods. The maximum number of method lists is 8.

Format

create accounting method_list_name <string 15>

Parameters

<string 15> - Enter the name of the user-defined method list.

Restrictions

Only Administrators can issue this command.

Example

To create a user-defined method list called “shell_acct”:

```
DGS-3000-28XMP:admin#create accounting method_list_name shell_acct
Command: create accounting method_list_name shell_acct

Success.

DGS-3000-28XMP:admin#
```

5-2 config accounting

Description

This command is used to configure a user-defined or the default method list for accounting services on the Switch.

Format

config accounting [default | method_list_name <string 15>] method {tacacs+ | radius | server_group <string 15> | none}(1)

Parameters

default - Specifies the default method list of accounting methods.

method_list_name - Specifies the user-defined method list of accounting methods.
- **<string 15>** - Enter the name of the method list.

method - Specifies the accounting method.
- **tacacs+** - Specifies to use TACACS+ built-in server group.
- **radius** - Specifies to use RADIUS built-in server group.
- **server_group** - Specifies to use the user-defined server group.
  - **<string 15>** - Enter the name of the server group
- **none** - Specifies to disable accounting.

Restrictions

Only Administrators can issue this command.

Example

To configure a user-defined method list called “shell_acct” to use TACAS+ built-in server group followed by RADIUS built-in server group:

```
DGS-3000-28XMP:admin#config accounting method_list_name shell_acct method tacacs+ radius
Command: config accounting method_list_name shell_acct method tacacs+ radius

Success.

DGS-3000-28XMP:admin#
```

5-3 delete accounting method_list_name

Description

This command is used to delete a user-defined method list of accounting methods.

Format

delete accounting method_list_name <string 15>

Parameters

<string 15> - Enter the name of the method list.

Restrictions

Only Administrators can issue this command.

Example

To delete the user-defined method list called “shell_acct”:

```
DGS-3000-28XMP:admin#delete accounting method_list_name shell_acct
Command: delete accounting method_list_name shell_acct

Success.

DGS-3000-28XMP:admin#
```

5-4 show accounting

Description

This command is used to display method lists of accounting methods.

Format

show accounting [default | method_list_name <string 15> | all]

Parameters

default - Specifies the default method list of accounting methods.
method_list_name - Specifies the user-defined method list of accounting methods. **<string 15>** - Enter the name of the method list.
all - Specifies to display all method lists

Restrictions

Only Administrators can issue this command.

Example

To display the user-defined method list called “shell_acct”:

```
DGS-3000-28XMP:admin#show accounting method_list_name shell_acct
Command: show accounting method_list_name shell_acct

Method List Name  Priority  Method Name      Comment
----------------  --------  ---------------  ------------------
shell_acct        1         tacacs+          Built-in Group
                  2         radius           Built-in Group

DGS-3000-28XMP:admin#
```

5-5 config accounting service

Description

This command is used to configure the state of the specified accounting service.

Format

config accounting service [network | shell | system] state [enable {[radius_only | method_list_name <string 15> | default_method_list]} | disable]

Parameters

network - Specifies the accounting service for 802.1X port access control. By default, the service is disabled.
shell - Specifies the accounting service for shell events. When the user logs in or out the Switch (via the console, Telnet, or SSH) and a timeout occurs, accounting information will be collected and sent to RADIUS server. By default, the service is disabled.
system - Specifies the accounting service for system events: reset and reboot. By default, the service is disabled.
state - Specifies the state of the specified service. **enable** - Specifies to enable the specified accounting service. **radius_only** - (Optional) Specifies to only use the RADIUS server created in the **config radius add** command. **method_list_name** - (Optional) Specifies to only use the user-defined method list of accounting methods created in the **create accounting method_list_name** command. **<string 15>** - Enter the name of the method list. **default_method_list** - (Optional) Specifies to use the default method list. **disable** - Specifies to disable the specified accounting service.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable the AAA accounting method list called “shell_acct” for shell events:

```
DGS-3000-28XMP:admin#config accounting service shell state enable method_list_name shell_acct
Command: config accounting service shell state enable method_list_name shell_acct

Success.

DGS-3000-28XMP:admin#
```

5-6 config accounting service command

Description

This command is used to configure the accounting service to be able to issue the commands at the specified level. If no command level is specified, all levels is chosen.

Format

config accounting service command {administrator | operator | power_user | user} [method_list_name <string 15> | none]

Parameters

administrator - (Optional) Specifies to use administrator-level commands.
operator - (Optional) Specifies to use operator-level commands.
power_user - (Optional) Specifies to use power-user-level commands.
user - (Optional) Specifies to use user-level commands.
method_list_name - Specifies to only use the user-defined method list of accounting methods created in the **create accounting method_list_name** command. **<string 15>** - Enter the name of the method list. **none** - Specifies to disable this feature.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the AAA accounting method list called “shell_acct” to use the administrator-level commands:

```
DGS-3000-28XMP:admin#config accounting service command administrator method_list_name
shell_acct
Command: config accounting service command administrator method_list_name shell_acct

Success.

DGS-3000-28XMP:admin#
```

5-7 show accounting service

Description

This command is used to show the status of accounting services.

Format

show accounting service

Parameters

None.

Restrictions

None.

Example

To show information of RADIUS accounting services:

```
DGS-3000-28XMP:admin#show accounting service
Command: show accounting service

Accounting State    Method
------------------- ---------------
Network : Disabled
Shell   : Enabled   shell_acct
System  : Enabled

DGS-3000-28XMP:admin#
```

5-8 create tacacs server_host

Description

This command is used to create a TACACS server host. When an AAA server host is created, its IP address and protocol are the index. More than one protocol service can be run on the same physical host. The maximum number of supported server hosts is 16.

Format

create tacacs server_host [<ipaddr> | <ipv6addr>] {port <int 1-65535> | timeout <int 1-255> | retransmit <int 1-20>}

Parameters

<ipaddr> - Enter the IP address of the server host.
<ipv6addr> - Enter the IPv6 address of the server host.
port - (Optional) Specifies the port number of the TACACS server host. **<int 1-65535>** - Enter the port number. The default value is 49.
timeout - (Optional) Specifies the time to wait for the server to reply. **<int 1-255>** - Enter the time in seconds. The default value is 5 seconds.
retransmit - (Optional) Specifies the count for re-transmitting. **<int 1-20>** - Enter the re-transmit value here. The default value is 2.

Restrictions

Only Administrators can issue this command.

Example

To create a TACACS server host:

```
DGS-3000-28XMP:admin#create tacacs server_host 10.1.1.222 port 15555 timeout 10
Command: create tacacs server_host 10.1.1.222 port 15555 timeout 10

Success.

DGS-3000-28XMP:admin#
```

5-9 config tacacs server_host

Description

This command is used to configure the TACACS server host.

Format

config tacacs server_host [<ipaddr> | <ipv6addr>] {port <int 1-65535> | timeout <int 1-255> | retransmit <int 1-20>}

Parameters

<ipaddr> - Enter the IP address of the server host.
<ipv6addr> - Enter the IPv6 address of the server host.
port - (Optional) Specifies the port number of the TACACS server host. **<int 1-65535>** - Enter the port number. The default value is 49.
timeout - (Optional) Specifies the time to wait for the server to reply. **<int 1-255>** - Enter the time in seconds. The default value is 5 seconds.
retransmit - (Optional) Specifies the count for re-transmitting. **<int 1-20>** - Enter the re-transmit value here. The default value is 2.

Restrictions

Only Administrators can issue this command.

Example

To configure the count for re-transmitting of the TACACS server host to 5:

```
DGS-3000-28XMP:admin#config tacacs server_host 10.1.1.222 retransmit 5
Command: config tacacs server_host 10.1.1.222 retransmit 5

Success.

DGS-3000-28XMP:admin#
```

5-10 create xtacacs server_host

Description

This command is used to create a XTACACS server host. When an AAA server host is created, its IP address and protocol are the index. More than one protocol service can be run on the same physical host. The maximum number of supported server hosts is 16.

Format

create xtacacs server_host [<ipaddr> | <ipv6addr>] {port <int 1-65535> | timeout <int 1-255> | retransmit <int 1-20>}

Parameters

<ipaddr> - Enter the IP address of the server host.
<ipv6addr> - Enter the IPv6 address of the server host.
port - (Optional) Specifies the port number of the XTACACS server host. **<int 1-65535>** - Enter the port number. The default value is 49.
timeout - (Optional) Specifies the time to wait for the server to reply. **<int 1-255>** - Enter the time in seconds. The default value is 5 seconds.
retransmit - (Optional) Specifies the count for re-transmitting. **<int 1-20>** - Enter the re-transmit value here. The default value is 2.

Restrictions

Only Administrators can issue this command.

Example

To create a XTACACS server host:

```
DGS-3000-28XMP:admin#create xtacacs server_host 10.1.1.222 port 15555 timeout 10

Command: create xtacacs server_host 10.1.1.222 port 15555 timeout 10

Success.

DGS-3000-28XMP:admin#
```

5-11 config xtacacs server_host

Description

This command is used to configure the XTACACS server host.

Format

config xtacacs server_host [<ipaddr> | <ipv6addr>] {port <int 1-65535> | timeout <int 1-255> | retransmit <int 1-20>}

Parameters

<ipaddr> - Enter the IP address of the server host.
<ipv6addr> - Enter the IPv6 address of the server host.
port - (Optional) Specifies the port number of the XTACACS server host. **<int 1-65535>** - Enter the port number. The default value is 49.
timeout - (Optional) Specifies the time to wait for the server to reply. **<int 1-255>** - Enter the time in seconds. The default value is 5 seconds.
retransmit - (Optional) Specifies the count for re-transmitting. **<int 1-20>** - Enter the re-transmit value here. The default value is 2.

Restrictions

Only Administrators can issue this command.

Example

To configure the count for re-transmitting of the XTACACS server host to 5:

```
DGS-3000-28XMP:admin#config xtacacs server_host 10.1.1.222 retransmit 5
Command: config xtacacs server_host 10.1.1.222 retransmit 5

Success.

DGS-3000-28XMP:admin#
```

5-12 create tacacs+ server_host

Description

This command is used to create a TACACS+ server host. When an AAA server host is created, its IP address and protocol are the index. More than one protocol service can be run on the same physical host. The maximum number of supported server hosts is 16.

Format

create tacacs+ server_host [<ipaddr> | <ipv6addr>] {port <int 1-65535> | key [<key_string 254> | none] | timeout <int 1-255>}

Parameters

<ipaddr> - Enter the IP address of the server host.
<ipv6addr> - Enter the IPv6 address of the server host.
port - (Optional) Specifies the port number of the TACACS+ server host. **<int 1-65535>** - Enter the port number. The default value is 49.
key - (Optional) Specifies the key string in plain text format. **<key_string 254>** - Enter the string of the key. **none** - Specifies to have no encryption for TACACS+.
timeout - (Optional) Specifies the time to wait for the server to reply. **<int 1-255>** - Enter the time in seconds. The default value is 5 seconds.

Restrictions

Only Administrators can issue this command.

Example

To create a TACACS+ server host:

```
DGS-3000-28XMP:admin#create tacacs+ server_host 10.1.1.222 port 15555 timeout 10
Command: create tacacs+ server_host 10.1.1.222 port 15555 timeout 10

Success.

DGS-3000-28XMP:admin#
```

5-13 config tacacs+ server_host

Description

This command is used to configure the TACACS+ server host.

Format

config tacacs+ server_host [<ipaddr> | <ipv6addr>] {port <int 1-65535> | key [<key_string 254> | none] | timeout <int 1-255>}

Parameters

<ipaddr> - Enter the IP address of the server host.
<ipv6addr> - Enter the IPv6 address of the server host.
port - (Optional) Specifies the port number of the TACACS+ server host. **<int 1-65535>** - Enter the port number. The default value is 49.
key - (Optional) Specifies the key string in plain text format. **<key_string 254>** - Enter the string of the key. **none** - Specifies to have no encryption for TACACS+.
timeout - (Optional) Specifies the time to wait for the server to reply. **<int 1-255>** - Enter the time in seconds. The default value is 5 seconds.

Restrictions

Only Administrators can issue this command.

Example

To configure the TACACS+ server host with the key value “abc123”:

```
DGS-3000-28XMP:admin#config tacacs+ server_host 10.1.1.222 key "abc123"
Command: config tacacs+ server_host 10.1.1.222 key "abc123"

Success.

DGS-3000-28XMP:admin#
```

5-14 create radius server_host

Description

This command is used to create a RADIUS server host. When an AAA server host is created, its IP address and protocol are the index. More than one protocol service can be run on the same physical host. The maximum number of supported server hosts is 16.

Format

create radius server_host [<ipaddr> | <ipv6addr>] {auth_port <int 1-65535> | acct_port <int 1-65535> | key [<key_string 254> | none] | timeout <int 1-255> | retransmit <int 1-20>}

Parameters

<ipaddr> - Enter the IP address of the server host.
<ipv6addr> - Enter the IPv6 address of the server host.
auth_port - (Optional) Specifies the port number for RADIUS authentication. **<int 1-65535>** - Enter the port number. The default value is 1812.
acct_port - (Optional) Specifies the port number for RADIUS accounting. **<int 1-65535>** - Enter the port number. The default value is 1813.
key - (Optional) Specifies the key string in plain text format. **<key_string 254>** - Enter the string of the key.

none - Specifies to have no encryption for TACACS+.
timeout - (Optional) Specifies the time to wait for the server to reply. **<int 1-255>** - Enter the time in seconds. The default value is 5 seconds.
retransmit - (Optional) Specifies the count for re-transmitting. **<int 1-20>** - Enter the re-transmit value here. The default value is 2.

Restrictions

Only Administrators can issue this command.

Example

To create a RADIUS server host:

```
DGS-3000-28XMP:admin#create radius server_host 10.1.1.222 auth_port 15555 timeout 110
Command: create radius server_host 10.1.1.222 auth_port 15555 timeout 110

Success.

DGS-3000-28XMP:admin#
```

5-15 config radius server_host

Description

This command is used to configure the RADIUS server host.

Format

config radius server_host [<ipaddr> | <ipv6addr>] {auth_port <int 1-65535> | acct_port <int 1-65535> | key [<key_string 254> | none] | timeout <int 1-255> | retransmit <int 1-20>}

Parameters

<ipaddr> - Enter the IP address of the server host.
<ipv6addr> - Enter the IPv6 address of the server host.
auth_port - (Optional) Specifies the port number for RADIUS authentication. **<int 1-65535>** - Enter the port number. The default value is 1812.
acct_port - (Optional) Specifies the port number for RADIUS accounting. **<int 1-65535>** - Enter the port number. The default value is 1813.
key - (Optional) Specifies the key string in plain text format. **<key_string 254>** - Enter the string of the key. **none** - Specifies to have no encryption for TACACS+.
timeout - (Optional) Specifies the time to wait for the server to reply. **<int 1-255>** - Enter the time in seconds. The default value is 5 seconds.
retransmit - (Optional) Specifies the count for re-transmitting. **<int 1-20>** - Enter the re-transmit value here. The default value is 2.

Restrictions

Only Administrators can issue this command.

Example

To configure the RADIUS server host with the key value “abc123”:

```
DGS-3000-28XMP:admin#config radius server_host 10.1.1.222 key "abc123"
Command: config radius server_host 10.1.1.222 key "abc123"

Success.

DGS-3000-28XMP:admin#
```

5-16 delete aaa server_host

Description

This command is used to delete the specified AAA server host.

Format

delete aaa server_host [<ipaddr> | <ipv6addr>] protocol [tacacs | xtacacs | tacacs+ | radius]

Parameters

<ipaddr> - Enter the IP address of the server host.
<ipv6addr> - Enter the IPv6 address of the server host.
protocol - Specifies the protocol used with the AAA. **tacacs** - Specifies the protocol as TACACS. **xtacacs** - Specifies the protocol as XTACACS. **tacacs+** - Specifies the protocol as TACACS+. **radius** - Specifies the protocol as RADIUS.

Restrictions

Only Administrators can issue this command.

Example

To delete the TACACS+ protocol used with the AAA server host with the IP address of 10.1.1.222:

```
DGS-3000-28XMP:admin#delete aaa server_host 10.1.1.222 protocol tacacs+
Command: delete aaa server_host 10.1.1.222 protocol tacacs+

Success.

DGS-3000-28XMP:admin#
```

5-17 show aaa server_host

Description

This command is used to display the information of AAA server hosts.

Format

show aaa server_host

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To display the information of AAA server hosts:

```
DGS-3000-28XMP:admin#show aaa server_host
Command: show aaa server_host

IP Address           Protocl Port  Acct  Time Retry Key
                             Port  out
-------------------- ------- ----- ----- ---- ----- --------------------------
10.1.1.222           RADIUS  15555 1813  110  2     abc123
10.1.1.222           TACACS  15555 -     5    2     -
10.1.1.222           TACACS+ 15555 -     5    -     abc123
10.1.1.222           XTACACS 15555 -     5    2     -


Total Entries : 4

DGS-3000-28XMP:admin#
```

5-18 create aaa server_group

Description

This command is used to create a group of user-defined AAA servers. The maximum number of server groups, including the built-in server groups, is 8. Each server group can have up to 8 server hosts.

Format

create aaa server_group <string 15>

Parameters

<string 15> - Enter the name of the server group.

Restrictions

Only Administrators can issue this command.

Example

To create a user-defined AAA server group called “group_1”:

```
DGS-3000-28XMP:admin#create aaa server_group group_1
Command: create aaa server_group group_1

Success.

DGS-3000-28XMP:admin#
```

5-19 config aaa server_group

Description

This command is used to add or remove an AAA server host to or from the specified server group.

Format

config aaa server_group [tacacs | xtacacs | tacacs+ | radius | group_name <string 15>] [add | delete] server_host [<ipaddr> | <ipv6addr>] protocol [tacacs | xtacacs | tacacs+ | radius]

Parameters

tacacs - Specifies to use the built-in TACACS server group.
xtacacs - Specifies to use the built-in XTACACS server group.
tacacs+ - Specifies to use the built-in TACACS+ server group.
radius - Specifies to use the built-in RADIUS server group.
group_name - Specifies the user-defined group name **<string 15>** - Enter the name of the server group.
add - Specifies to add the server host to the server group.
delete - Specifies to remove the server host from the server group.
server_host - Specifies the server host. **<ipaddr>** - Enter the IP address of the server host. **<ipv6addr>** - Enter the IPv6 address of the server host.
protocol - Specifies the protocol used with the AAA. **tacacs** - Specifies the protocol as TACACS. **xtacacs** - Specifies the protocol as XTACACS. **tacacs+** - Specifies the protocol as TACACS+. **radius** - Specifies the protocol as RADIUS.

Restrictions

Only Administrators can issue this command.

Example

To add the AAA server host with the IP address of 10.1.1.222 to the server group called “group_1”:

```
DGS-3000-28XMP:admin# config aaa server_group group_name group_1 add server_host 10.1.1.222
protocol tacacs+
Command: config aaa server_group group_name group_1 add server_host 10.1.1.222 protocol
tacacs+


Success.


DGS-3000-28XMP:admin#
```

5-20 delete aaa server_group

Description

This command is used to delete a group of user-defined AAA servers..

Format

delete aaa server_group <string 15>

Parameters

<string 15> - Enter the name of the server group.

Restrictions

Only Administrators can issue this command.

Example

To delete a user-defined AAA server group called “group_1”:

```
DGS-3000-28XMP:admin#delete aaa server_group group_1
Command: delete aaa server_group group_1

Success.

DGS-3000-28XMP:admin#
```

5-21 show aaa server_group

Description

This command is used to display AAA server groups.

Format

show aaa server_group {<string 15>}

Parameters

<string 15> - (Optional) Enter the name of the server group.

Restrictions

Only Administrators can issue this command.

Example

To display all AAA server groups:

```
DGS-3000-28XMP:admin#show aaa server_group
Command: show aaa server_group

Group Name      IP Address                              Protocol
--------------- --------------------------------------- --------
group_1         10.1.1.222                              TACACS+

radius          10.1.1.222                              RADIUS

tacacs          10.1.1.222                              TACACS

tacacs+         10.1.1.222                              TACACS+

xtacacs         10.1.1.222                              XTACACS

Total Entries : 5

DGS-3000-28XMP:admin#
```

5-22 show aaa

Description

This command is used to display the AAA global configuration.

Format

show aaa

Parameters

None.

Restrictions

None.

Example

To display the AAA global configuration:

```
DGS-3000-28XMP:admin#show aaa
Command: show aaa

Authentication Policy: Disabled
Accounting Network Service State: Disabled
Accounting Network Service Method:
Accounting Shell Service State: Disabled
Accounting Shell Service Method:
Accounting System Service State: Disabled
Accounting System Service Method:
Accounting Admin Command Service Method:
Accounting Operator Command Service Method:
Accounting PowerUser Command Service Method:
Accounting User Command Service Method:

DGS-3000-28XMP:admin#
```

Chapter 6 Access Authentication Control Command List

enable password encryption
disable password encryption
enable authen_policy
disable authen_policy
show authen_policy
create authen_login method_list_name <string 15>
config authen_login [default | method_list_name <string 15>] method {tacacs | xtacacs | tacacs+ | radius | server_group <string 15> | local | none}
delete authen_login method_list_name <string 15>
show authen_login [default | method_list_name <string 15> | all]
create authen_enable method_list_name <string 15>
config authen_enable [default | method_list_name <string 15>] method {tacacs | xtacacs | tacacs+ | radius | server_group <string 15> | local _enable | none}
delete authen_enable method_list_name <string 15>
show authen_enable [default | method_list_name <string 15> | all]
config authen application [console | telnet | ssh | http | all] [login | enable] [default | method_list_name <string 15>]
show authen application
create authen server_group <string 15>
config authen server_group [tacacs | xtacacs | tacacs+ | radius | <string 15>] [add | delete] server_host [<ipaddr> | <ipv6addr>] protocol [tacacs | xtacacs | tacacs+ | radius]
delete authen server_group <string 15>
show authen server_group {<string 15>}
create authen server_host [<ipaddr> | <ipv6addr>] protocol [tacacs | xtacacs | tacacs+ | radius] {port <int 1-65535> | key [<key_string 254> | none] | timeout <int 1-255> | retransmit <int 1-20>}
config authen server_host [<ipaddr> | <ipv6addr>] protocol [tacacs | xtacacs | tacacs+ | radius] {port <int 1-65535> | key [<key_string 254> | none] | timeout <int 1-255> | retransmit <int 1-20>}
delete authen server_host [<ipaddr> | <ipv6addr>] protocol [tacacs | xtacacs | tacacs+| radius]
show authen server_host
config authen parameter response_timeout <int 0-255>
config authen parameter attempt <int 1-255>
show authen parameter
enable admin
config admin local_enable {encrypt [plain_text | sha_1] <password>}

6-1 enable password encryption

Description

This command is used to enable password encryption. The user account configuration information will be stored in the configuration file, and can be applied to the system later.

If password encryption is enabled, the password will be in encrypted form.

Format

enable password encryption

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To enable the password encryption:

```
DGS-3000-28XMP:admin# enable password encryption
Command: enable password encryption

Success.

DGS-3000-28XMP:admin#
```

6-2 disable password encryption

Description

This command is used to disable password encryption. The user account configuration information will be stored in the configuration file, and can be applied to the system later.

When password encryption is disabled, if the user specifies the password in the plaintext form, the password will be in the plaintext form. However, if the user specifies the password in the encrypted form, or if the password has been converted to the encrypted form by the last **enable password encryption** command, the password will still be in the encrypted form. It cannot be reverted back to the plaintext form.

Format

disable password encryption

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To disable password encryption:

```
DGS-3000-28XMP:admin# disable password encryption
Command: disable password encryption

Success.

DGS-3000-28XMP:admin#
```

6-3 enable authen_policy

Description

This command is used to enable system access authentication policy. When authentication is enabled, the device will adopt the login authentication method list to authenticate the user for login, and adopt the enable authentication method list to authenticate the enable password for promoting the user‘s privilege to Admin level.

Format

enable authen_policy

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To enable system access authentication policy:

```
DGS-3000-28XMP:admin# enable authen_policy
Command: enable authen_policy

Success.

DGS-3000-28XMP:admin#
```

6-4 disable authen_policy

Description

This command is used to disable system access authentication policy. When authentication is disabled, the device will adopt the local user account database to authenticate the user for login, and adopt the local enable password to authenticate the enable password for promoting the user‘s privilege to Admin level.

Format

disable authen_policy

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To disable system access authentication policy:

```
DGS-3000-28XMP:admin# disable authen_policy
Command: disable authen_policy

Success.

DGS-3000-28XMP:admin#
```

6-5 show authen_policy

Description

This command is used to display the status of the system access authentication policy.

Format

show authen_policy

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To display system access authentication policy:

```
DGS-3000-28XMP:admin# show authen_policy
Command: show authen_policy

Authentication Policy : Enabled

DGS-3000-28XMP:admin#
```

6-6 create authen_login method_list_name

Description

This command is used to create a user-defined authentication method list. The maximum supported number of the login method lists is 8.

Format

create authen_login method_list_name <string 15>

Parameters

<string 15> - Enter the user-defined method list name. This value can be up to 15 characters long.

Restrictions

Only Administrators can issue this command.

Example

To create a user-defined method list for user login:

```
DGS-3000-28XMP:admin# create authen_login method_list_name login_list_1
Command: create authen_login method_list_name login_list_1

Success.

DGS-3000-28XMP:admin#
```

6-7 config authen_login

Description

This command is used to configure a user-defined or default method list for user login. The sequence of methods will affect the result. For example, if the sequence is TACACS+ first, then TACACS and local, when the user tries to log in, the authentication request will be sent to the first server host in TACACS+ built-in server group. If the first server host in TACACS+ group is missing, the authentication request will be sent to the second server host in TACACS+ group, and so on. If all server hosts in TACACS+ group are missing, the authentication request will be sent to the first server host in TACACS group and so on. If all server hosts in TACACS group are missing, the local account database in the device is used to authenticate this user. When the user logs into the device successfully while using methods like TACACS/XTACACS/TACACS+/RADIUS built-in or user-defined server groups or none, the “user” privilege level is assigned. If the user wants to get admin privilege level, user must use the **enable admin** command to promote the user’s privilege level. But when local method is used, the privilege level will depend on the account privilege level stored in the local device.

Format

config authen_login [default | method_list_name <string 15>] method {tacacs | xtacacs | tacacs+ | radius | server_group <string 15> | local | none}

Parameters

default - Specifies to use the default method list.

method_list_name - Specifies to use a user-defined method list.
- **<string 15>** - Enter the method list name here. This value can be up to 15 characters long.

method - Specifies the authentication method used.
- **tacacs** - (Optional) Specifies authentication through the built-in server group TACACS.
- **xtacacs** - (Optional) Specifies authentication through the built-in server group XTACACS.

tacacs+ - (Optional) Specifies authentication through the built-in server group TACACS+.
radius - (Optional) Specifies authentication through the built-in server group RADIUS.
server_group - (Optional) Specifies authentication through the user-defined server group.
<string 15> - Enter the server group value here. This value can be up 15 characters long.
local - (Optional) Specifies authentication through the local user account database of the Switch.
none - (Optional) Specifies that there is no authentication.

Restrictions

Only Administrators can issue this command.

Example

To configure a user-defined method list for user login:

```
DGS-3000-28XMP:admin# config authen_login method_list_name login_list_1 method tacacs+ tacacs
local
Command: config authen_login method_list_name login_list_1 method tacacs+ tacacs local

Success.

DGS-3000-28XMP:admin#
```

6-8 delete authen_login method_list_name

Description

This command is used to delete a user-defined method list for user login.

Format

delete authen_login method_list_name <string 15>

Parameters

<string 15> - Enter the user-defined method list name. This value can be up to 15 characters long.

Restrictions

Only Administrators can issue this command.

Example

To delete a user-defined method list for user login:

```
DGS-3000-28XMP:admin# delete authen_login method_list_name login_list_1
Command: delete authen_login method_list_name login_list_1

Success.

DGS-3000-28XMP:admin#
```

6-9 show authen_login

Description

This command is used to display the method list for user login.

Format

show authen_login [default | method_list_name <string 15> | all]

Parameters

default - Specifies to display default user-defined method list for user login.
method_list_name - Specifies to display the specific user-defined method list for user login. **<string 15>** - Enter the method list name here. This value can be up to 15 characters long.
all - Specifies to display all method lists for user login.

Restrictions

Only Administrators can issue this command.

Example

To display a user-defined method list for user login:

```
DGS-3000-28XMP:admin# show authen_login method_list_name login_list_1
Command: show authen_login method_list_name login_list_1

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

DGS-3000-28XMP:admin#
```

6-10 create authen_enable method_list_name

Description

This command is used to create a user-defined method list for promoting a user's privilege to Admin level.

Format

create authen_enable method_list_name <string 15>

Parameters

<string 15> - Enter the user-defined method list name. This value can be up to 15 characters long.

Restrictions

Only Administrators can issue this command.

Example

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

```
DGS-3000-28XMP:admin# create authen_enable method_list_name enable_list_1
Command: create authen_enable method_list_name enable_list_1

Success.

DGS-3000-28XMP:admin#
```

6-11 config authen_enable

Description

This command is used to configure a user-defined or default method list for promoting a user's privilege to Admin level. The sequence of methods will affect the result. For example, if the sequence is TACACS+ first, then TACACS and local_enable, when the user tries to promote the privilege to Admin level, the authentication request will be sent to the first server host in TACACS+ built-in server group. If the first server host in TACACS+ group is missing, the authentication request will be sent to the second server host in TACACS+ group, and so on. If all server hosts in TACACS+ group are missing, the authentication request will be sent to the first server host in TACACS group and so on. If all server hosts in TACACS group are missing, the local enable password in the device is used to authenticate this user's password.

Format

config authen_enable [default | method_list_name <string 15>] method {tacacs | xtacacs | tacacs+ | radius | server_group <string 15> | local _enable | none}

Parameters

default - Specifies to use the default method list.

method_list_name - Specifies to use a user-defined method list.
- **<string 15>** Enter the method list name here. This value can be up to 15 characters long.

method - Specifies the authentication method used.
- **tacacs** - (Optional) Specifies authentication through the built-in server group TACACS.
- **xtacacs** - (Optional) Specifies authentication through the built-in server group XTACACS.
- **tacacs+** - (Optional) Specifies authentication through the built-in server group TACACS+.
- **radius** - (Optional) Specifies authentication through the built-in server group RADIUS.
- **server_group** - (Optional) Specifies authentication through the user-defined server group.
  - **<string 15>** - Enter the server group name here. This value can be up to 15 characters long.
- **local_enable** - (Optional) Specifies authentication through the local enable password in the device.
- **none** - (Optional) Specifies that there is no authentication.

Restrictions

Only Administrators can issue this command.

Example

To configure a user-defined method list for promoting a user's privilege to Admin level:

```
DGS-3000-28XMP:admin# config authen_enable method_list_name enable_list_1 method tacacs+
tacacs local_enable
Command: config authen_ enable method_list_name enable_list_1 method tacacs+ tacacs
local_enable

Success.

DGS-3000-28XMP:admin#
```

6-12 delete authen_enable method_list_name

Description

This command is used to delete a user-defined method list for promoting a user's privilege to Admin level.

Format

delete authen_enable method_list_name <string 15>

Parameters

<string 15> - Enter the user-defined method list name. This value can be up to 15 characters long.

Restrictions

Only Administrators can issue this command.

Example

To delete a user-defined method list for promoting a user's privilege to Admin level:

```
DGS-3000-28XMP:admin# delete authen_enable method_list_name enable_list_1
Command: delete authen_enable method_list_name enable_list_1

Success.

DGS-3000-28XMP:admin#
```

6-13 show authen_enable

Description

This command is used to display the method list for promoting a user's privilege to Admin level.

Format

show authen_enable [default | method_list_name <string 15> | all]

Parameters

default - Specifies to display the default user-defined method list for promoting a user's privilege to Admin level.
method_list_name - Specifies to display the user-defined method list for promoting a user's privilege to Admin level. **<string 15>** - Enter the method list name here. This value can be up to 15 characters long.
all - Specifies to display all method lists for promoting a user's privilege to Admin level.

Restrictions

Only Administrators can issue this command.

Example

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

```
DGS-3000-28XMP:admin# show authen_enable method_list_name enable_list_1
Command: show authen_enable method_list_name enable_list_1

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

DGS-3000-28XMP:admin#
```

6-14 config authen application

Description

This command is used to configure the login or enable method list for all or the specified application.

Format

config authen application [console | telnet | ssh | http | all] [login | enable] [default | method_list_name <string 15>]

Parameters

console - Specifies the application as console.
telnet - Specifies the application as telnet.
ssh - Specifies the application as SSH.
http - Specifies the application as web.
all - Specifies the application as console, telnet, SSH, and web.
login - Specifies the method list for user login.
enable - Specifies the method list for promoting a user's privilege to Admin level.
default - Specifies the default method list.
method_list_name - Specifies the user-defined method list name.

<string> - Enter the method list name here. This value can be up to 15 characters long.

Restrictions

Only Administrators can issue this command.

Example

To configure the login method list for telnet:

```
DGS-3000-28XMP:admin# config authen application telnet login method_list_name login_list_1
Command: config authen application telnet login method_list_name login_list_1

Success.

DGS-3000-28XMP:admin#
```

6-15 show authen application

Description

This command is used to display the login/enable method list for all applications.

Format

show authen application

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

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

```
DGS-3000-28XMP:admin# show authen application
Command: show authen application

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

DGS-3000-28XMP:admin#
```

6-16 create authen server_group

Description

This command is used to create a user-defined authentication server group. The maximum supported number of server groups including built-in server groups is 8. Each server group supports a maximum of 8 server hosts.

Format

create authen server_group <string 15>

Parameters

<string 15> - Enter the user-defined server group name. This value can be up to 15 characters long.

Restrictions

Only Administrators can issue this command.

Example

To create a user-defined authentication server group:

```
DGS-3000-28XMP:admin# create authen server_group mix_1
Command: create authen server_group mix_1

Success.

DGS-3000-28XMP:admin#
```

6-17 config authen server_group

Description

This command is used to add or remove an authentication server host to or from the specified server group. Built-in TACACS, XTACACS, TACACS+, or RADIUS server groups only accept server hosts that use the same protocol. For example, a RADIUS server group only supports RADIUS server hosts. User-defined server groups can accept server hosts with different protocols.

Format

config authen server_group [tacacs | xtacacs | tacacs+ | radius | <string 15>] [add | delete] server_host [<ipaddr> | <ipv6addr>] protocol [tacacs | xtacacs | tacacs+ | radius]

Parameters

tacacs - Specifies to configure the built-in server group TACACS.
xtacacs - Specifies to configure the built-in server group XTACACS.
tacacs+ - Specifies to configure the built-in server group TACACS+.
radius - Specifies to configure the built-in server group RADIUS.
<string 15> - Enter the server group name here. This value can be up to 15 characters long.
add - Specifies to add a server host to a server group.

delete - Specifies to remove a server host from a server group.
server_host - Specifies the server host. **<ipaddr>** - Enter the server host IP address here. **<ipv6addr>** - Enter the server host IPv6 address here.
protocol - Specifies the authentication protocol used. **tacacs** - Specifies that the TACACS authentication protocol will be used. **xtacacs** - Specifies that the XTACACS authentication protocol will be used. **tacacs+** - Specifies that the TACACS+ authentication protocol will be used. **radius** - Specifies that the RADIUS authentication protocol will be used.

Restrictions

Only Administrators can issue this command.

Example

To add an authentication server host to a server group:

```
DGS-3000-28XMP:admin# config authen server_group mix_1 add server_host 10.1.1.222 protocol
tacacs+
Command: config authen server_group mix_1 add server_host 10.1.1.222 protocol ta
cacs+

Success.

DGS-3000-28XMP:admin#
```

6-18 delete authen server_group

Description

This command is used to delete a user-defined authentication server group.

Format

delete authen server_group <string 15>

Parameters

<string 15> - Enter the user-defined server group name. This value can be up to 15 characters long.

Restrictions

Only Administrators can issue this command.

Example

To delete a user-defined authentication server group:

```
DGS-3000-28XMP:admin# delete authen server_group mix_1
Command: delete authen server_group mix_1

Success.

DGS-3000-28XMP:admin#
```

6-19 show authen server_group

Description

This command is used to display the authentication server groups.

Format

show authen server_group {<string 15>}

Parameters

<string 15> - (Optional) Enter the built-in or user-defined server group name. This value can be up to 15 characters long.

Restrictions

Only Administrators can issue this command.

Example

To display all authentication server groups:

```
DGS-3000-28XMP:admin# show authen server_group
Command: show authen server_group

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

Total Entries : 5

DGS-3000-28XMP:admin#
```

6-20 create authen server_host

Description

This command is used to create an authentication server host. When an authentication server host is created, IP address and protocol are the index. That means over 1 authentication protocol services can be run on the same physical host. The maximum supported number of server hosts is 16.

Format

create authen server_host [<ipaddr> | <ipv6addr>] protocol [tacacs | xtacacs | tacacs+ | radius] {port <int 1-65535> | key [<key_string 254> | none] | timeout <int 1-255> | retransmit <int 1-20>}

Parameters

<ipaddr> - Enter the server host IP address.
<ipv6addr> - Enter the server host IPv6 address.
protocol - Specifies the host's authentication protocol. **tacacs** - Specifies the protocol as TACACS. **xtacacs** - Specifies the protocol as XTACACS. **tacacs+** - Specifies the protocol as TACACS+. **radius** - Specifies the protocol as RADIUS.
port - (Optional) Specifies the port number of authentication protocol for server host. Default value for TACACS/XTACACS/TACACS+ is 49. Default value for RADIUS is 1812. **<int 1-65535>** - Enter the authentication protocol port number here. This value must be between 1 and 65535.
key - (Optional) Specifies the key for TACACS+ and RADIUS authentication. If the value is null, no encryption will apply. This value is meaningless for TACACS and XTACACS. **<key_string 254>** - Enter the TACACS+ or the RADIUS key here. This key can be up to 254 characters long. **none** - Specifies that there is no encryption for TACACS+ and RADIUS authentication. This value is meaningless for TACACS and XTACACS.
timeout - (Optional) Specifies the time in second for waiting server reply. The default value is 5 seconds. **<int 1-255>** - Enter the timeout value here. This value must be between 1 and 255 seconds.
retransmit - (Optional) Specifies the count for re-transmit. This value is meaningless for TACACS+. Default value is 2. **<int 1-20>** - Enter the re-transmit value here. This value must be between 1 and 20.

Restrictions

Only Administrators can issue this command.

Example

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

```
DGS-3000-28XMP:admin# create authen server_host 10.1.1.222 protocol tacacs+ port 15555
timeout 10
Command: create authen server_host 10.1.1.222 protocol tacacs+ port 15555 timeout 10

Key is empty for TACACS+ or RADIUS.
Success.

DGS-3000-28XMP:admin#
```

6-21 config authen server_host

Description

This command is used to configure an authentication server host.

Format

config authen server_host [<ipaddr> | <ipv6addr>] protocol [tacacs | xtacacs | tacacs+ | radius] {port <int 1-65535> | key [<key_string 254> | none] | timeout <int 1-255> | retransmit <int 1-20>}

Parameters

<ipaddr> - Enter the server host IP address.
<ipv6addr> - Enter the server host IPv6 address.
protocol - Specifies the host's authentication protocol. **tacacs** - Specifies the protocol as TACACS. **xtacacs** - Specifies the protocol as XTACACS. **tacacs+** - Specifies the protocol as TACACS+. **radius** - Specifies the protocol as RADIUS.
port - (Optional) Specifies the port number of authentication protocol for server host. Default value for TACACS/XTACACS/TACACS+ is 49. The default value for RADIUS is 1812. **<int 1-65535>** - Enter the port number here. This value must be between 1 and 65535.
key - (Optional) Specifies the key for TACACS+ and RADIUS authentication. If the value is null, no encryption will apply. This value is meaningless for TACACS and XTACACS. **<key_string 254>** - Enter the TACACS+ key here. This value can be up to 254 characters long. **none** - Specifies that there is no encryption for TACACS+ and RADIUS authentication. This value is meaningless for TACACS and XTACACS.
timeout - (Optional) Specifies the time in second for waiting server reply. Default value is 5 seconds. **<int 1-255>** - Enter the timeout value here. This value must be between 1 and 255 seconds.
retransmit - (Optional) Specifies the count for re-transmit. This value is meaningless for TACACS+. Default value is 2. **<int 1-20>** - Enter the re-transmit value here. This value must be between 1 and 20.

Restrictions

Only Administrators can issue this command.

Example

To configure a TACACS+ authentication server host's key value:

```
DGS-3000-28XMP:admin# config authen server_host 10.1.1.222 protocol tacacs+ key "This is a
secret."
Command: config authen server_host 10.1.1.222 protocol tacacs+ key "This is a secret."

Success.

DGS-3000-28XMP:admin#
```

6-22 delete authen server_host

Description

This command is used to delete an authentication server host.

Format

delete authen server_host [<ipaddr> | <ipv6addr>] protocol [tacacs | xtacacs | tacacs+| radius]

Parameters

<ipaddr> - Enter the server host's IP address.
<ipv6addr> - Enter the server host IPv6 address.
protocol - Specifies the host's authentication protocol. **tacacs** - Specifies the protocol as TACACS. **xtacacs** - Specifies the protocol as XTACACS. **tacacs+** - Specifies the protocol as TACACS+. **radius** - Specifies the protocol as RADIUS.

Restrictions

Only Administrators can issue this command.

Example

To delete an authentication server host:

```
DGS-3000-28XMP:admin# delete authen server_host 10.1.1.222 protocol tacacs+
Command: delete authen server_host 10.1.1.222 protocol tacacs+

Success.

DGS-3000-28XMP:admin#
```

6-23 show authen server_host

Description

This command is used to display the authentication server hosts.

Format

show authen server_host

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To display all authentication server hosts:

```
DGS-3000-28XMP:admin# show authen server_host
Command: show authen server_host

IP Address       Protocol  Port   Timeout  Retransmit  Key
---------------  --------  -----  -------  ----------  -------------------------
10.1.1.222       TACACS+   15555  10       ------      This is a secret.

Total Entries : 1

DGS-3000-28XMP:admin#
```

6-24 config authen parameter response_timeout

Description

This command is used to configure the amount of time waiting or user input on console, Telnet, or SSH application.

Format

config authen parameter response_timeout <int 0-255>

Parameters

<int 0-255> - Enter the amount of time for user input on console, Telnet, or SSH. 0 means there is no time out. This value must be between 0 and 255. Default value is 30 seconds.

Restrictions

Only Administrators can issue this command.

Example

To configure the amount of time waiting or user input to be 60 seconds:

```
DGS-3000-28XMP:admin# config authen parameter response_timeout 60
Command: config authen parameter response_timeout 60

Success.

DGS-3000-28XMP:admin#
```

6-25 config authen parameter attempt

Description

This command is used to configure the maximum attempts for users trying to login or promote the privilege on console, Telnet, or SSH application.

Format

config authen parameter attempt <int 1-255>

Parameters

<int 1-255> - Enter the amount of attempts for users trying to login or promote the privilege on console, Telnet, or SSH. This value must be between 1 and 255. Default value is 3.

Restrictions

Only Administrators can issue this command.

Example

To configure the maximum attempts for users trying to login or promote the privilege to be 9:

```
DGS-3000-28XMP:admin# config authen parameter attempt 9
Command: config authen parameter attempt 9

Success.

DGS-3000-28XMP:admin#
```

6-26 show authen parameter

Description

This command is used to display the parameters of authentication.

Format

show authen parameter

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To display the parameters of authentication:

```
DGS-3000-28XMP:admin# show authen parameter
Command: show authen parameter

Response Timeout : 60 seconds
User Attempts    : 9

DGS-3000-28XMP:admin#
```

6-27 enable admin

Description

This command is used to enter the administrator level privilege. Promote the "user" privilege level to "admin" level. When the user enters this command, the authentication method TACACS, XTACACS, TACACS+, user-defined server groups, local enable, or none will be used to authenticate the user. Because TACACS, XTACACS and RADIUS don't support "enable" function in itself, if the user wants to use either one of these 3 protocols to do enable authentication, the user must create a special account on the server host first, which has a username "enable" and then configure its password as the enable password to support "enable" function.

This command cannot be used when authentication policy is disabled.

Format

enable admin

Parameters

None.

Restrictions

None.

Example

To enable administrator level privilege:

```
DGS-3000-28XMP:puser# enable admin
Command: enable admin

PassWord:******
Success.

DGS-3000-28XMP:admin#
```

6-28 config admin local_enable

Description

This command is used to configure the local enable password of administrator level privilege. When the user chooses the “local_enable” method to promote the privilege level, the enable password of the local device is needed. When the password information is not specified in the command, the system will prompt the user to input the password. For this case, the user can only input the plaintext password. If the password is present in the command, the user can select to input the password in the plaintext form or in the encrypted form. The encryption algorithm is based on SHA-1.

Format

config admin local_enable {encrypt [plain_text | sha_1] <password>}

Parameters

encrypt - (Optional) Specifies the password form.

plain_text - Specifies the password in plaintext form.

sha_1 - Specifies the password in SHA-1 encrypted form.
<password> - (Optional) Enter the password for promoting the privilege level. The length for a password in plain-text form and SHA-1 encrypted form are different. plain-text: Passwords can be from a minimum of 0 to a maximum of 15 characters. SHA-1: The length of encrypted passwords is fixed to 35 bytes long and the password is case-sensitive.

Restrictions

Only Administrators can issue this command.

Example

To configure the administrator password:

```
DGS-3000-28XMP:admin# config admin local_enable
Command: config admin local_enable

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

DGS-3000-28XMP:admin#
```

Chapter 7 Access Control List (ACL) Command List

create access_profile profile_id <value 1-512> {profile_name <name 32>} [ethernet{vlan {<hex 0x0-0x0fff>} | source_mac <macmask 000000000000-ffffffffffff> | destination_mac <macmask 000000000000-ffffffffffff> | 802.1p | ethernet_type}|ip {vlan {<hex 0x0-0x0fff>} | source_ip_mask <netmask> | destination_ip_mask <netmask> | dscp | [icmp {type | code} | igmp {type} | tcp {src_port_mask <hex0x0-0xffff> | dst_port_mask <hex 0x0-0xffff> | flag_mask [all | {urg | ack | psh | rst | syn | fin}]} | udp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | protocol_id_mask <hex 0x0-0xff> {user_define_mask <hex 0x0-0xffffffff>}]} | packet_content_mask {offset_chunk_1 <value 0-31> <hex 0x0-0xffffffff> | offset_chunk_2 <value 0-31> <hex 0x0-0xffffffff> | offset_chunk_3<value 0-31> <hex 0x0-0xffffffff> | offset_chunk_4 <value 0-31> <hex 0x0-0xffffffff>} | ipv6 {class |flowlabel | source_ipv6_mask <ipv6mask> | destination_ipv6_mask <ipv6mask> | [tcp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | udp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | icmp {type | code}]}]
delete access_profile [profile_id <value 1-512> | profile_name <name 32> | all]
config access_profile [profile_id <value 1-512> | profile_name <name 32>] [add access_id [auto_assign | <value 1-128>] [ethernet {[vlan <vlan_name 32> | vlan_id <vlanid 1-4094>] {mask <hex 0x0-0x0fff>} | source_mac <macaddr> {mask <macmask>} | destination_mac <macaddr> {mask <macmask>} | 802.1p <value 0-7> | ethernet_type <hex 0x0-0xffff>} | ip {[vlan <vlan_name 32> | vlan_id <vlanid 1-4094>] {mask <hex 0x0-0x0fff>} | source_ip <ipaddr> {mask <netmask>} | destination_ip <ipaddr> {mask <netmask>} | dscp <value 0-63> | [icmp {type <value 0-255> | code <value 0-255>} | igmp {type <value 0-255>} | tcp {src_port <value 0-65535> {mask <hex 0x0-0xffff>} | dst_port <value 0-65535> {mask <hex 0x0-0xffff>} | flag [all | {urg | ack | psh | rst | syn | fin}]} | udp {src_port <value 0-65535> {mask <hex 0x0-0xffff>} | dst_port <value 0-65535> {mask <hex 0x0-0xffff>}} | protocol_id <value 0-255> {user_define <hex 0x0-0xffffffff> {mask <hex 0x0-0xffffffff>}}]} | packet_content {offset_chunk_1 <hex 0x0-0xffffffff> {mask <hex 0x0-0xffffffff>} | offset_chunk_2 <hex 0x0-0xffffffff> {mask <hex 0x0-0xffffffff>} | offset_chunk_3 <hex 0x0-0xffffffff> {mask <hex 0x0-0xffffffff>} | offset_chunk_4 <hex 0x0-0xffffffff> {mask <hex 0x0-0xffffffff>}} | ipv6 {class <value 0-255> | flowlabel <hex 0x0-0xfffff> | source_ipv6 <ipv6addr> {mask<ipv6mask>} | destination_ipv6 <ipv6addr> {mask <ipv6mask>} | [tcp {src_port <value 0-65535> {mask <hex 0x0-0xffff>} | dst_port <value 0-65535> {mask <hex0x0-0xffff>}} | udp {src_port <value 0-65535> {mask <hex 0x0-0xffff>} | dst_port <value 0-65535> {mask <hex 0x0-0xffff>}} | icmp {type<value 0-255> | code <value 0-255>}]}] [port [<portlist> | all] | vlan_based [vlan <vlan_name 32> | vlan_id <vlanid 1-4094>]] [permit {priority <value 0-7> {replace_priority} |[replace_dscp_with <value 0-63> | replace_tos_precedence_with <value 0-7>] | counter [enable | disable]} | mirror | deny] {time_range <range_name 32>} | delete access_id <value 1-128>]
show access_profile {[profile_id <value 1-512> | profile_name <name 32>]}
config flow_meter [profile_id <value 1-512> | profile_name <name 32>] access_id <value 1-128> [rate [<value 1-10485760>] {burst_size [<value 1-262144>]} rate_exceed [drop_packet | remark_dscp <value 0-63>] | tr_tcm cir <value 1-10485760> {cbs <value 1-262144>} pir <value 1-10485760> {pbs <value 1-262144>} {[color_blind | color_aware]} {conform [permit | replace_dscp <value 0-63>] {counter [enable | disable]}} exceed [permit {replace_dscp <value 0-63>} | drop] {counter [enable | disable]} violate [permit {replace_dscp <value 0-63>} | drop] {counter [enable | disable]} | sr_tcm cir <value 1-10485760> cbs <value 1-262144> ebs <value 1-262144> {[color_blind | color_aware]} {conform [permit | replace_dscp <value 0-63>] {counter [enable | disable]}} exceed [permit {replace_dscp <value 0-63>} | drop] {counter [enable | disable]} violate [permit {replace_dscp <value 0-63>} | drop] {counter [enable | disable]} | delete]
show flow_meter {[profile_id <value 1-512> | profile_name <name 32>] {access_id <value 1-128>}}
config time_range <range_name 32> [hours start_time <time hh:mm:ss> end_time <time hh:mm:ss> weekdays <daylist> | delete]
show time_range
show current_config access_profile

7-1 create access_profile

Description

This command is used to create access control list profiles.

When creating ACL, each profile can have 128 rules/access IDs. However, when creating ACL type as Ethernet or IPv4 at the first time, 62 rules are reserved for the system. In this case, only 66 rules are available to configure. You can use the **show access_profile** command to see the available rules.

Profile ID 1 is reserved for Ethernet profile, and profile ID 2 is reserved for IPv4 profile. Both IDs cannot be deleted from the Switch.

The Switch supports the following profile types:

1. MAC DA, MAC SA, Ethernet Type, Outer VLAN Tag
2. Outer VLAN Tag, Source IPv4, Destination IPv4, DSCP, Protocol ID, TCP/UDP Source Port, TCP/UDP Destination Port, ICMP type/code, IGMP type, TCP flags
3. Source IPv6 Address, Class, Flow Label, IPv6 Protocol (Next Header)
4. Destination IPv6 Address, Class, Flow Label, IPv6 Protocol (Next Header)
5. Class, Flow Label, IPv6 Protocol (Next Header), TCP/UDP source port, TCP/UDP destination port, ICMP type/code, Outer VLAN Tag
6. Packet Content, Outer VLAN Tag
7. MAC SA, Ethernet Type, Source IPv4/ARP sender IP, Outer VLAN Tag
8. LLC Header/SNAP Header, Outer VLAN Tag
9. Source IPv6 Address, Class, IPv6 Protocol (Next Header), Outer VLAN Tag
10. Destination IPv6 Address, Class, IPv6 Protocol (Next Header), Outer VLAN Tag

Format

create access_profile profile_id <value 1-512> {profile_name <name 32>} [ethernet{vlan {<hex 0x0-0x0fff>} | source_mac <macmask 000000000000-ffffffffffff> | destination_mac <macmask 000000000000-ffffffffffff> | 802.1p | ethernet_type}|ip {vlan {<hex 0x0-0x0fff>} | source_ip_mask <netmask> | destination_ip_mask <netmask> | dscp | [icmp {type | code} | igmp {type} | tcp {src_port_mask <hex0x0-0xffff> | dst_port_mask <hex 0x0-0xffff> | flag_mask [all | {urg | ack | psh | rst | syn | fin}]} | udp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | protocol_id_mask <hex 0x0-0xff> {user_define_mask <hex 0x0-0xffffffff>}]} | packet_content_mask {offset_chunk_1 <value 0-31> <hex 0x0-0xffffffff> | offset_chunk_2 <value 0-31> <hex 0x0-0xffffffff> | offset_chunk_3<value 0-31> <hex 0x0-0xffffffff> | offset_chunk_4 <value 0-31> <hex 0x0-0xffffffff>} | ipv6 {class | flowlabel | source_ipv6_mask <ipv6mask> | destination_ipv6_mask <ipv6mask> | [tcp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | udp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | icmp {type | code}]}]

Parameters

<value 1-512> - Enter the profile ID here. This value must be between 1 and512.

profile_name – (Optional) Specifies the name of the profile. The maximum length is 32 characters.
- **<name 32>** - Enter the profile name here.

ethernet - Specifies this is an Ethernet mask.
- **vlan** - (Optional) Specifies a VLAN mask. Only the last 12 bits of the mask will be considered.
  - **<hex 0x0-0x0fff>** - Enter the VLAN mask value here.
- **source_mac** - (Optional) Specifies the source MAC mask.
  - **<macmask>** - Enter the source MAC address used here.
- **destination_mac** - (Optional) Specifies the destination MAC mask.
  - **<macmask>** - Enter the destination MAC address used here.
- **802.1p** - (Optional) Specifies the 802.1p priority tag mask.

ethernet_type - (Optional) Specifies the Ethernet type mask.

ip - Specifies this is a IPv4 mask.
- **vlan** - (Optional) Specifies a VLAN mask. Only the last 12 bits of the mask will be considered.
  - **<hex 0x0-0x0fff>** -Enter the VLAN mask value here.
- **source_ip_mask** - (Optional) Specifies a source IP address mask.
  - **<netmask>** - Enter the source IP address mask here.
- **destination_ip_mask** - (Optional) Specifies a destination IP address mask.
  - **<netmask>** - Enter the destination IP address mask here.
- **dscp** - (Optional) Specifies the DSCP mask.
- **icmp** - (Optional) Specifies that the rule applies to ICMP traffic.
  - **type** - Specifies the type of ICMP traffic.
  - **code** - Specifies the code of ICMP traffic
- **igmp** - (Optional) Specifies that the rule applies to IGMP traffic.
  - **type** - Specifies the type of IGMP traffic.
- **tcp** - (Optional) Specifies that the rule applies to TCP traffic.
  - **src_port_mask** - (Optional) Specifies the TCP source port mask.
    - **<hex 0x0-0xffff>** - Enter the TCP source port mask here.
  - **dst_port_mask** - (Optional) Specifies the TCP destination port mask.
    - **<hex 0x0-0xffff>** - Enter the TCP destination port mask here.
  - **flag_mask** - (Optional) Specifies the TCP flag field mask.
    - **all** – Specifies that all the flags will be used for the TCP mask.
    - **urg** – (Optional) Specifies that the TCP flag field will be set to ‘urg’.
    - **ack** - (Optional) Specifies that the TCP flag field will be set to ‘ack’.
    - **psh** - (Optional) Specifies that the TCP flag field will be set to ‘psh’.
    - **rst** - (Optional) Specifies that the TCP flag field will be set to ‘rst’.
    - **syn** - (Optional) Specifies that the TCP flag field will be set to ‘syn’.
    - **fin** - (Optional) Specifies that the TCP flag field will be set to ‘fin’.
- **udp** - (Optional) Specifies that the rule applies to UDP traffic.
  - **src_port_mask** - (Optional) Specifies the UDP source port mask.
    - **<hex 0x0-0xffff>** - Enter the UDP source port mask here.
  - **dst_port_mask** - (Optional) Specifies the UDP destination port mask.
    - **<hex 0x0-0xffff>** - Enter the UDP destination port mask here.
- **protocol_id_mask** - (Optional) Specifies that the rule applies to IP protocol ID traffic.
  - **<0x0-0xff>** - Enter the protocol ID mask here.
  - **user_define_mask** - (Optional) Specifies that the rule applies to the IP protocol ID, and that the mask option behind the IP header length is 4 bytes.
    - **<hex 0x0-0xffffffff>** - Enter a user-defined mask value here.

packet_content_mask - Specifies the packet content mask. Only one packet_content_mask profile can be created.
- **offset_chunk_1** - (Optional) Specifies that the offset chunk 1 will be used.
  - **<value 0-31>** - Enter the offset chunk 1 value here. This value must be between 0 and 31.
  - **<hex 0x0-0xffffffff>** - Enter the offset chunk 1 mask here.
- **offset_chunk_2** - (Optional) Specifies that the offset chunk 2 will be used.
  - **<value 0-31>** - Enter the offset chunk 2 value here. This value must be between 0 and 31.
  - **<hex 0x0-0xffffffff>** - Enter the offset chunk 2 mask here.
- **offset_chunk_3** - (Optional) Specifies that the offset chunk 3 will be used.
  - **<value 0-31>** - Enter the offset chunk 3 value here. This value must be between 0 and 31.
  - **<hex 0x0-0xffffffff>** - Enter the offset chunk 3 mask here.
- **offset_chunk_4** - (Optional) Specifies that the offset chunk 4 will be used.
  - **<value 0-31>** - Enter the offset chunk 4 value here. This value must be between 0 and 31.

<hex 0x0-0xffffffff> - Enter the offset chunk 4 mask here.

ipv6 - Specifies this is the IPv6 mask.
- **class** - (Optional) Specifies the IPv6 class.
- **flowlabel** - (Optional) Specifies the IPv6 flow label.
- **source_ipv6_mask** - (Optional) Specifies an IPv6 source sub-mask.
  - **<ipv6mask>** - Enter the source IPv6 mask value here.
- **destination_ipv6_mask** - (Optional) Specifies an IPv6 destination sub-mask.
  - **<ipv6mask>** -Enter the destination IPv6 mask value here.
- **tcp** - (Optional) Specifies that the rule applies to TCP traffic.
  - **src_port_mask** - (Optional) Specifies an IPv6 TCP source port mask.
    - **<hex 0x0-0xffff>** - Enter the TCP source port mask value here.
  - **dst_port_mask** - (Optional) Specifies an IPv6 TCP destination port mask.
    - **<hex 0x0-0xffff>** - Enter the TCP destination port mask value here.
- **udp** - (Optional) Specifies that the rule applies to UDP traffic.
  - **src_port_mask** - Specifies the UDP source port mask.
    - **<hex 0x0-0xffff>** - Enter the UDP source port mask value here.
  - **dst_port_mask** - Specifies the UDP destination port mask.
    - **<hex 0x0-0xffff>** - Enter the UDP destination port mask value here.
- **icmp** - (Optional) Specifies a mask for ICMP filtering.
  - **type** - (Optional) Specifies the inclusion of the ICMP type field in the mask.
  - **code** - (Optional) Specifies the inclusion of the ICMP code field in the mask.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To create three access profiles:

```
DGS-3000-28XMP:admin# create access_profile profile_id 1 profile_name t1 ethernet vlan
source_mac 00-00-00-00-00-01 destination_mac 00-00-00-00-00-02 802.1p ethernet_type
Command: create access_profile profile_id 1 profile_name 1 ethernet vlan source_mac 00-00-00-
00-00-01 destination_mac 00-00-00-00-00-02 802.1p ethernet_type


Success.


DGS-3000-28XMP:admin# create access_profile profile_id 2 profile_name 2 ip vlan
source_ip_mask 20.0.0.0 destination_ip_mask 10.0.0.0 dscp icmp type code
Command: create access_profile profile_id 2 profile_name t2 ip vlan source_ip_mask 20.0.0.0
destination_ip_mask 10.0.0.0 dscp icmp type code


Success.


DGS-3000-28XMP:admin# create access_profile profile_id 4 profile_name 4 packet_content_mask
offset_chunk_1 3 0xFFFF offset_chunk_2 5 0xFF00 offset_chunk_3 14 0xFFFF0000 offset_chunk_4
16 0xFF000000
Command: create access_profile profile_id 4 profile_name 4 packet_content_mask offset_chunk_1
3 0xFFFF offset_chunk_2 5 0xFF00 offset_chunk_3 14 0xFFFF0000 offset_chunk_4 16 0xFF000000


Success.


DGS-3000-28XMP:admin#
```

7-2 delete access_profile

Description

This command is used to delete access list profiles. ACL profile ID 1 and 2 cannot be deleted. When this command is issued for profile ID 1 and 2, all the settings within these profiles will be removed. When this command is issued for profile ID 3 and more, the complete profile will be deleted.

Format

delete access_profile [profile_id <value 1-512> | profile_name <name 32> | all]

Parameters

profile_id - Specifies the index of the access list profile. **<value 1-512>** - Enter the profile ID value here. This value must be between 1 and 512.
profile_name - Specifies the name of the profile. **<name 32>** - Enter the profile name. The maximum length is 32 characters.
all - Specifies that the whole access list profile will be deleted.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

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

```
DGS-3000-28XMP:admin# delete access_profile profile_id 1
Command: delete access_profile profile_id 1

Success.

DGS-3000-28XMP:admin#
```

7-3 config access_profile

Description

This command is used to configure an access list entry. The ACL mirror function works after the mirror has been enabled and the mirror port has been configured using the mirror command.

When applying an access rule to a target, the setting specified in the VLAN field will not take effect if the target is a VLAN.

Format

config access_profile [profile_id <value 1-512> | profile_name <name 32>] [add access_id [auto_assign | <value 1-128>] [ethernet {[vlan <vlan_name 32> | vlan_id <vlanid 1-4094>] {mask <hex 0x0-0x0fff>} | source_mac <macaddr> {mask <macmask>} | destination_mac <macaddr> {mask <macmask>} | 802.1p <value 0-7> | ethernet_type <hex 0x0-0xffff>} | ip {[vlan <vlan_name 32> | vlan_id <vlanid 1-4094>] {mask <hex 0x0-0x0fff>} | source_ip <ipaddr> {mask <netmask>} | destination_ip <ipaddr> {mask <netmask>} | dscp <value 0-63> | [icmp {type <value 0-255> | code <value 0-255>} | igmp {type <value 0-255>} | tcp {src_port <value 0-65535> {mask <hex 0x0-0xffff>} | dst_port <value 0-65535> {mask <hex 0x0-0xffff>} | flag [all | {urg | ack | psh | rst | syn | fin}]} | udp {src_port <value 0-65535> {mask <hex 0x0-0xffff>} | dst_port

<value 0-65535> {mask <hex 0x0-0xffff>}} | protocol_id <value 0-255> {user_define <hex 0x0-0xffffffff> {mask <hex 0x0-0xffffffff>}}]} | packet_content {offset_chunk_1 <hex 0x0-0xffffffff> {mask <hex 0x0-0xffffffff>} | offset_chunk_2 <hex 0x0-0xffffffff> {mask <hex 0x0-0xffffffff>} | offset_chunk_3 <hex 0x0-0xffffffff> {mask <hex 0x0-0xffffffff>} | offset_chunk_4 <hex 0x0-0xffffffff> {mask <hex 0x0-0xffffffff>}} | ipv6 {class <value 0-255> | flowlabel <hex 0x0-0xfffff> | source_ipv6 <ipv6addr> {mask<ipv6mask>} | destination_ipv6 <ipv6addr> {mask <ipv6mask>} | [tcp {src_port <value 0-65535> {mask <hex 0x0-0xffff>} | dst_port <value 0-65535> {mask <hex0x0-0xffff>}} | udp {src_port <value 0-65535> {mask <hex 0x0-0xffff>} | dst_port <value 0-65535> {mask <hex 0x0-0xffff>}} | icmp {type<value 0-255> | code <value 0-255>}]}] [port [<portlist> | all] | vlan_based [vlan <vlan_name 32> | vlan_id <vlanid 1-4094>]] [permit {priority <value 0-7> {replace_priority} | [replace_dscp_with <value 0-63> | replace_tos_precedence_with <value 0-7>] | counter [enable | disable]} | mirror | deny] {time_range <range_name 32>} | delete access_id <value 1-128>]

Parameters

profile_id - Specifies the index of the access list profile.
- **<value 1-512>** - Enter the profile ID value here. This value must be between 1 and 512.

profile_name - Specifies the name of the profile.
- **<name 32>** - Enter the profile name here. This name can be up to 32 characters long.

add - Specifies that a profile or a rule will be added.
- **access_id** - Specifies the index of the access list entry.
  - **auto_assign** - Specifies that the access ID will automatically be assigned.
  - **<value 1- 128>** - Enter the access ID used here. This value must be between 1 and 128.

ethernet - Specifies to configure the Ethernet access profile.
- **vlan** - (Optional) Specifies the VLAN name.
  - **<vlan_name 32>** - Enter the name of the VLAN here. This name can be up to 32 characters long.
- **vlan_id** - (Optional) Specifies the VLAN ID used.
  - **<vlanid 1-4094>** - Enter the VLAN ID used here. This value must be between 1 and 4094.
  - **mask** - (Optional) Specifies an additional mask parameter that can be configured.
    - **<hex 0x0-0x0fff>** - Enter the mask value here.
- **source_mac** - (Optional) Specifies the source MAC address.
  - **<macaddr>** - Enter the source MAC address used for this configuration here.
  - **mask** - (Optional) Specifies an additional mask parameter that can be configured.
    - **<macmask>** - Enter the source MAC mask used here.
- **destination_mac** - (Optional) Specifies the destination MAC address.
  - **<macaddr>** - Enter the destination MAC address used for this configuration here.
  - **mask** - (Optional) Specifies an additional mask parameter that can be configured.
    - **<macmask>** - Enter the destination MAC mask here.
- **802.1p** - (Optional) Specifies the value of the 802.1p priority tag.
  - **<value 0-7>** - Enter the 802.1p priority tag value. The priority tag ranges from 1 to 7.
- **ethernet_type** - (Optional) Specifies the Ethernet type.
  - **<hex 0x0-0xffff>** - Enter the Ethernet type mask here.

ip - Specifies to configure the IP access profile.
- **vlan** - (Optional) Specifies a VLAN name.
  - **<vlan_name 32>** - Enter the name of the VLAN here. This name can be up to 32 characters long.
- **vlan_id** - (Optional) Specifies that VLAN ID used.
  - **<vlanid 1-4094>** - Enter the VLAN ID used here. This value must be between 1 and 4094.
  - **mask** – (Optional) Specifies an additional mask parameter that can be configured.
    - **<hex 0x0-0x0fff>** - Enter the mask value here.
- **source_ip** - (Optional) Specifies an IP source address.
  - **<ipaddr>** - Enter the source IP address used for this configuration here.
  - **mask** - (Optional) Specifies an additional mask parameter that can be configured.

<netmask> - Enter the source netmask used here.

destination_ip - (Optional) Specifies an IP destination address.

<ipaddr> - Enter the destination IP address used for this configuration here.

mask - (Optional) Specifies an additional mask parameter that can be configured.

<netmask> - Enter the destination netmask used here.

dscp - (Optional) Specifies the value of DSCP. The DSCP value ranges from 0 to 63.

<value 0-63> - Enter the DSCP value here.

icmp - (Optional) Specifies to configure the ICMP parameters.

type - (Optional) Specifies that the rule will apply to the ICMP Type traffic value.

<value 0-255> - Enter the ICMP type traffic value here. This value must be between 0 and 255.

code - (Optional) Specifies that the rule will apply to the ICMP Code traffic value.

<value 0-255> - Enter the ICMP code traffic value here. This value must be between 0 and 255.

igmp - (Optional) Specifies to configure the IGMP parameters.

type - (Optional) Specifies that the rule will apply to the IGMP Type traffic value.

<value 0-255> - Enter the IGMP type traffic value here. This value must be between 0 and 255.

tcp - Specifies to configure the TCP parameters.

src_port - (Optional) Specifies that the rule will apply to a range of TCP source ports.

<value 0-65535> - Enter the TCP source port value here. This value must be between 0 and 65535.

mask - (Optional) Specifies an additional mask parameter that can be configured.

<hex 0x0-0xffff> - Enter the source port mask here.

dst_port - (Optional) Specifies that the rule will apply to a range of TCP destination ports.

<value 0-65535> - Enter the TCP destination port value here. This value must be between 0 and 65535.

mask - (Optional) Specifies an additional mask parameter that can be configured.

<hex 0x0-0xffff> - Enter the destination port mask here.

flag - (Optional) Specifies the TCP flag fields.

all - Specifies that all the TCP flags will be used in this configuration.

urg - (Optional) Specifies that the TCP flag field will be set to 'urg'.

ack - (Optional) Specifies that the TCP flag field will be set to 'ack'.

psh - (Optional) Specifies that the TCP flag field will be set to 'psh'.

rst - (Optional) Specifies that the TCP flag field will be set to 'rst'.

syn - (Optional) Specifies that the TCP flag field will be set to 'syn'.

fin - (Optional) Specifies that the TCP flag field will be set to 'fin'.

udp - Specifies to configure the UDP parameters.

src_port - (Optional) Specifies the UDP source port range.

<value 0-65535> - Enter the UDP source port value here. This value must be between 0 and 65535.

mask - (Optional) Specifies an additional mask parameter that can be configured.

<hex 0x0-0xffff> - Enter the source port mask here.

dst_port - (Optional) Specifies the UDP destination port range.

<value 0-65535> - Enter the UDP destination port value here. This value must be between 0 and 65535.

mask - (Optional) Specifies an additional mask parameter that can be configured.

<hex 0x0-0xffff> - Enter the destination port mask here.

protocol_id - Specifies that the rule will apply to the value of IP protocol ID traffic.

<value 0-255> - Enter the protocol ID used here.

user_define - (Optional) Specifies that the rule will apply to the IP protocol ID and that the mask options behind the first 4 bytes of the IP payload.

<hex 0x0-0xffffffff> - Enter the user-defined mask value here.

mask - Specifies an additional mask parameter that can be configured.

<hex 0x0-0xffffffff> - Enter the mask value here.

packet_content - Specifies the offset. Each offset defines 4 bytes of data which is identified as a single UDF

field.

offset_chunk_1 – (Optional) Specifies the value of the packet bytes to be matched. Offset chunk 1 will be used.

<hex 0x0-0xffffffff> - Enter the offset chunk 1 mask here.

offset_chunk_2 - (Optional) Specifies the value of the packet bytes to be matched. Offset chunk 2 will be used.

<hex 0x0-0xffffffff> - Enter the offset chunk 2 mask here.

offset_chunk_3 - (Optional) Specifies the value of the packet bytes to be matched. Offset chunk 3 will be used.

<hex 0x0-0xffffffff> - Enter the offset chunk 3 mask here.

offset_chunk_4 - (Optional) Specifies the value of the packet bytes to be matched. Offset chunk 4 will be used.

<hex 0x0-0xffffffff> - Enter the offset chunk 4 mask here.

ipv6 - Specifies that the rule applies to IPv6 fields.

class - (Optional) Specifies the value of the IPv6 class.

<value 0-255> - Enter the IPv6 class value here. This value must be between 0 and 255.

flowlabel - (Optional) Specifies the value of the IPv6 flow label.

<hex 0x0-0xffff> - Enter the IPv6 flow label mask used here.

source_ipv6 - (Optional) Specifies the value of the IPv6 source address.

<ipv6addr> - Enter the source IPv6 address used for this configuration here.

mask - (Optional) Specifies an additional mask parameter that can be configured.

<ipv6mask> - Enter the source IPv6 mask here.

destination_ipv6 - (Optional) Specifies the value of the IPv6 destination address.

<ipv6addr> - Enter the destination IPv6 address used for this configuration here.

mask - (Optional) Specifies an additional mask parameter that can be configured.

<ipv6mask> - Enter the destination IPv6 mask here.

tcp - (Optional) Specifies to configure the TCP parameters.

src_port - Specifies the value of the IPv6 Layer 4 TCP source port.

<value 0-65535> - Enter the TCP source port value here. This value must be between 0 and 65535.

mask - Specifies an additional mask parameter that can be configured.

<hex 0x0-0xffff> - Enter the TCP source port mask value here.

dst_port - (Optional) Specifies the value of the IPv6 Layer 4 TCP destination port.

<value 0-65535> - Enter the TCP destination port value here. This value must be between 0 and 65535.

mask - Specifies an additional mask parameter that can be configured.

<hex 0x0-0xffff> - Enter the TCP destination port mask value here.

udp - (Optional) Specifies to configure the UDP parameters.

src_port - Specifies the value of the IPv6 Layer 4 UDP source port.

<value 0-65535> - Enter the UDP source port value here. This value must be between 0 and 65535.

mask - Specifies an additional mask parameter that can be configured.

<hex 0x0-0xffff> - Enter the UDP source port mask value here.

dst_port - Specifies the value of the IPv6 Layer 4 UDP destination port.

<value 0-65535> - Enter the UDP destination port value here. This value must be between 0 and 65535.

mask - Specifies an additional mask parameter that can be configured.

<hex 0x0-0xffff> - Enter the UDP destination port mask value here.

icmp - (Optional) Specifies to configure the ICMP parameters used.

type - (Optional) Specifies that the rule applies to the value of ICMP type traffic.

<value 0-255> - Enter the ICMP type traffic value here. This value must be between 0 and 255.

code - (Optional) Specifies that the rule applies to the value of ICMP code traffic.

<value 0-255> - Enter the ICMP code traffic value here. This value must be between 0 and 255.

port - Specifies the port list used for this configuration.
- **<portlist>** - Enter a list of ports used for the configuration here.
- **all** - Specifies that all the ports will be used for this configuration.
- **vlan_based** - Specifies that the rule will be VLAN based.
  - **vlan** - Specifies the VLAN name used for this configuration.
    - **<vlan_name>** - Enter the VLAN name used for this configuration here.
  - **vlan_id** - Specifies the VLAN ID used for this configuration.
    - **<vlanid 1-4094>** - Enter the VLAN ID used here. This value must be between 1 and 4094.

permit - Specifies that packets matching the access rule are permitted by the Switch.
- **priority** - (Optional) Specifies that the priority of the packet will change if the packet matches the access rule.
  - **<value 0-7>** - Enter the priority value here. This value must be between 0 and 7.
  - **replace_priority** - (Optional) Specifies that the 802.1p priority of the outgoing packet will be replaced.
- **replace_dscp_with** - (Optional) Specifies that the DSCP of the outgoing packet is changed with the new value. If using this action without an action priority, the packet will be sent to the default TC.
  - **<value 0-63>** - Enter the replace DSCP with value here. This value must be between 0 and 63.
- **replace_tos_precedence_with** - (Optional) Specifies that the IP precedence of the outgoing packet is changed with the new value. If used without an action priority, the packet is sent to the default TC.
  - **<value 0-7>** - Enter the replace ToS precedence with value here. This value must be between 0 and 7.
- **counter** - (Optional) Specifies whether the ACL counter feature is enabled or disabled. This parameter is optional. The default option is disabled. If the rule is not bound with the flow_meter, all matching packets are counted. If the rule is bound with the flow_meter, then the “counter” is overridden.
  - **enable** - Specifies that the ACL counter feature will be enabled.
  - **disable** - Specifies that the ACL counter feature will be disabled.

mirror - Specifies that packets matching the access rules are copied to the mirror port.

deny - Specifies that packets matching the access rule are filtered by the Switch.

time_range - (Optional) Specifies the name of the time range entry.
- **<range_name 32>** - Enter the time range name here. This name can be up to 32 characters long.

delete - Specifies that a profile or a rule will be deleted.
- **access_id** - Specifies the index of the access list entry.
  - **<value 1- 128>** - Enter the access ID used here. This value must be between 1 and 128.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure a rule entry for a packet content mask profile:

```
DGS-3000-28XMP:admin#config access_profile profile_id 4 add access_id auto_assign
packet_content offset_chunk_3 0xF0 port all deny
Command: config access_profile profile_id 4 add access_id auto_assign packet_content
offset_chunk_3 0xF0 port all deny

Success.

DGS-3000-28XMP:admin#
```

7-4 show access_profile

Description

This command is used to display the current access list table.

Format

show access_profile {[profile_id <value 1-512> | profile_name <name 32>]}

Parameters

profile_id - (Optional) Specifies the index of the access list profile. **<value 1-512>** - Enter the profile ID used here. This value must be between 1 and 512.
profile_name - (Optional) Specifies the name of the profile. **<name 32>** - Enter the profile name used here. This name can be up to 32 characters long.

Restrictions

None.

Example

To display the current access list table:

```
DGS-3000-28XMP:admin#show access_profile
Command: show access_profile

Access Profile Table

Total User Set Rule Entries : 1
Total Used HW Entries       : 125
Total Available HW Entries  : 899

================================================================================
Profile ID: 1     Profile name: t1  Type: Ethernet

MASK on
    VLAN            : 0xFFF
    Source MAC      : 00-00-00-00-00-01
    Destination MAC : 00-00-00-00-00-02
    802.1p
    Ethernet Type

Available HW Entries : 66
================================================================================



================================================================================
Profile ID: 2     Profile name: 2  Type: IPv4
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

The following example displays an access profile that supports an entry mask for each rule:

```
DGS-3000-28XMP:admin#show access_profile profile_id 1
Command: show access_profile profile_id 1

Access Profile Table

================================================================================
Profile ID: 1     Profile name: t1  Type: Ethernet

MASK on
    VLAN            : 0xFFF
    Source MAC      : 00-00-00-00-00-01
    Destination MAC : 00-00-00-00-00-02
    802.1p
    Ethernet Type

Available HW Entries : 66
================================================================================


DGS-3000-28XMP:admin#
```

The following example displays the packet content mask profile for the profile with an ID of 4:

```
DGS-3000-28XMP:admin#show access_profile profile_id 4
Command: show access_profile profile_id 4

Access Profile Table

================================================================================
Profile ID: 4     Profile name: 4  Type: User Defined

MASK on
    offset_chunk_1 : 3      value : 0x0000FFFF
    offset_chunk_2 : 5      value : 0x0000FF00
    offset_chunk_3 : 14     value : 0xFFFF0000
    offset_chunk_4 : 16     value : 0xFF000000

Available HW Entries : 127
--------------------------------------------------------------------------------
Rule ID : 1    (auto assign)    Ports: 1-28

Match on
    offset_chunk_3 : 14     value : 0x00000000

Action:
    Deny

================================================================================
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

7-5 config flow_meter

Description

This command is used to configure the flow-based metering function. The metering function supports three modes: single rate two color, single rate three color, and two rate three color. The access rule must be created before the parameters of this function can be applied.

For the single rate two color mode, users may set the preferred bandwidth for this rule, in Kbps, and once the bandwidth has been exceeded, overflowing packets will either be dropped or have a drop precedence set, depending on the user configuration.

For single rate three color mode, users need to specify the committed rate, in Kbps, the committed burst size, and the excess burst size.

For the two rate three color mode, users need to specify the committed rate in Kbps, the committed burst size, the peak rate and the peak burst size.

There are two cases for mapping the color of a packet: Color-blind mode and Color-aware mode. In the Color-blind case, the determination for the packet's color is based on the metering result. In the Color-aware case, the determination for the packet's color is based on the metering result and the ingress DSCP.

When color-blind or color-aware is not specified, color-blind is the default mode.

The green color packet will be treated as the conforming action, the yellow color packet will be treated as the exceeding action, and the red color packet will be treated as the violating action.

The replace DSCP action can be performed on packets that conform (GREEN) and packets that do not conform (YELLOW and RED). If drop YELLOW/RED is selected, the action to replace the DSCP will not take effect.

Format

config flow_meter [profile_id <value 1-512> | profile_name <name 32>] access_id <value 1-128> [rate [<value 1-10485760>] {burst_size [<value 1-262144>]} rate_exceed [drop_packet | remark_dscp <value 0-63>] | tr_tcm cir <value 1-10485760> {cbs <value 1-262144>} pir <value 1-10485760> {pbs <value 1-262144>} {[color_blind | color_aware]} {conform [permit | replace_dscp <value 0-63>] {counter [enable | disable]}} exceed [permit {replace_dscp <value 0-63>} | drop] {counter [enable | disable]} violate [permit {replace_dscp <value 0-63>} | drop] {counter [enable | disable]} | sr_tcm cir <value 1-10485760> cbs <value 1-262144> ebs <value 1-262144> {[color_blind | color_aware]} {conform [permit | replace_dscp <value 0-63>] {counter [enable | disable]}} exceed [permit {replace_dscp <value 0-63>} | drop] {counter [enable | disable]} violate [permit {replace_dscp <value 0-63>} | drop] {counter [enable | disable]} | delete]

Parameters

profile_id - Specifies the profile ID.
- **<value 1-512>** - Enter the profile ID here. This value must be between 1 and 512.

profile_name - Specifies the name of the profile. The maximum length is 32 characters.
- **<name 32>** - Enter the profile name used here.

access_id - Specifies the access ID.
- **<value 1-128>** - Enter the access ID used here. This value must be between 1 and 128.

rate - Specifies the rate for single rate two color mode. Specifies the committed bandwidth in Kbps for the flow.
- **<value 1-10485760>** - Enter the rate for single rate two color mode here. This value must be between 1 and 10485760.
- **burst_size** - (Optional) Specifies the burst size for the single rate two color mode. The unit is Kbytes.
  - **<value 1-262144>** - Enter the burst size value here. This value must be between 1 and 262144.
- **rate_exceed** - Specifies the action for packets that exceeds the committed rate in single rate, two color mode.
  - **drop_packet** - Specifies to drop the packet immediately.
  - **remark_dscp** – Specifies to mark the packet with a specified DSCP. The packet is set to have a high drop precedence.
    - **<value 0-63>** - Enter the remark DSCP value here. This value must be between 0 and 63.

tr_tcm - Specifies the "two rate three color mode".

cir - Specifies the Committed Information Rate. The unit is in Kbps. CIR should always be equal or less than PIR.

<value 1-10485760> - Enter the CIR value here. This value must be between 1 and 10485760.

cbs - (Optional) Specifies the Committed Burst Size. The unit is Kbytes. That is to say, 1 means 1Kbytes. This parameter is an optional parameter. The default value is 4*1024.

<value 1-262144> - Enter the CBS value here. This value must be between 1 and 262144.

pir - Specifies the “Peak Information Rate”. The unit is in Kbps. PIR should always be equal to or greater than CIR.

<value 1-10485760> - Enter the peak information rate value here. This value must be between 1 and 10485760.

pbs - (Optional) Specifies the “Peak Burst Size”. The unit is in Kbytes. This parameter is an optional parameter. The default value is 4*1024.

<value 1-262144> - Enter the peak burst size value here. This value must be between 1 and 262144.

color_blind - (Optional) Specifies the meter mode as color-blind. The default is color-blind mode.

color_aware - (Optional) Specifies the meter mode as color-aware. The final color of the packet is determined by the initial color of the packet and the metering result.

conform - (Optional) Specifies the action when a packet is mapped to the “green” color.

permit - Specifies to permit the packet.

replace_dscp - Specifies to change the DSCP value of the packet.

<value 0-63> - Enter the replace DSCP value here. This value must be between 0 and 63.

counter - (Optional) Specifies the ACL counter. This is optional. The default is “disable”. The resource may be limited so that a counter cannot be turned on. Counters will be cleared when the function is disabled.

enable - Specifies that the ACL counter option will be enabled.

disable - Specifies that the ACL counter option will be disabled.

exceed - Specifies the action when a packet is mapped to the “yellow” color.

permit - Specifies to permit the packet.

replace_dscp - (Optional) Specifies to change the DSCP value of the packet.

<value 0-63> - Enter the replace DSCP value here. This value must be between 0 and 63.

drop - Specifies to drop the packet.

counter - (Optional) Specifies the ACL counter. This is optional. The default is “disable”. The resource may be limited so that a counter cannot be turned on. Counters will be cleared when the function is disabled.

enable - Specifies that the ACL counter option will be enabled.

disable - Specifies that the ACL counter option will be disabled.

violate - Specifies the action when a packet is mapped to the “red” color.

permit - Specifies to permit the packet.

replace_dscp - (Optional) Specifies to change the DSCP value of the packet.

<value 0-63> - Enter the replace DSCP value here. This value must be between 0 and 63.

drop - Specifies to drop the packet.

counter - (Optional) Specifies the ACL counter. This is optional. The default is “disable”. The resource may be limited so that a counter cannot be turned on. Counters will be cleared when the function is disabled.

enable - Specifies that the ACL counter option will be enabled.

disable - Specifies that the ACL counter option will be disabled.

sr_tcm - Specifies “single rate three color mode”.

cir - Specifies the Committed Information Rate. The unit is Kbps.

<value 0- 10485760> - Enter the CIR value here. This value must be between 0 and 10485760.

cbs - Specifies the Committed Burst Size. The unit is Kbytes.

<value 1-262144> - Enter the CBS value here. This value must be between 1 and 262144.

ebs - Specifies the Excess Burst Size. The unit is Kbytes.

<value 1-262144> - Enter the EBS value here. This value must be between 1 and 262144.

color_blind - (Optional) Specifies the meter mode as color-blind. The default is color-blind mode.

color_aware - (Optional) Specifies the meter mode as color-aware. The final color of the packet is determined by the initial color of the packet and the metering result.

conform - (Optional) Specifies the action when a packet is mapped to the “green” color.
- **permit** - Permits the packet.
- **replace_dscp** - Specifies to change the DSCP value of the packet.
  - **<value 0-63>** - Enter the replace DSCP value here. This value must be between 0 and 63.
- **counter** - (Optional) Specifies the ACL counter. This is optional. The default is “disable”. The resource may be limited so that a counter cannot be turned on. Counters will be cleared when the function is disabled.
  - **enable** - Specifies that the ACL counter option will be enabled.
  - **disable** - Specifies that the ACL counter option will be disabled.

exceed - Specifies the action when a packet is mapped to the “yellow” color.
- **permit** - Specifies to permit the packet.
  - **replace_dscp** - (Optional) Specifies to change the DSCP value of the packet.
    - **<value 0-63>** - Enter the replace DSCP value here. This value must be between 0 and 63.
- **drop** - Specifies to drop the packet.
- **counter** - (Optional) Specifies the ACL counter. This is optional. The default is “disable”. The resource may be limited so that a counter cannot be turned on. Counters will be cleared when the function is disabled.
  - **enable** - Specifies that the ACL counter option will be enabled.
  - **disable** - Specifies that the ACL counter option will be disabled.

violate - Specifies the action when a packet is mapped to the “red” color.
- **permit** - Specifies to permit the packet.
  - **replace_dscp** - (Optional) Specifies to change the DSCP value of the packet.
    - **<value 0-63>** - Enter the replace DSCP value here. This value must be between 0 and 63.
- **drop** - Specifies to drop the packet.
- **counter** - (Optional) Specifies the ACL counter. This is optional. The default is “disable”. The resource may be limited so that a counter cannot be turned on. Counters will be cleared when the function is disabled.
  - **enable** - Specifies that the ACL counter option will be enabled.
  - **disable** - Specifies that the ACL counter option will be disabled.

delete - Specifies to delete the specified flow_meter.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure a “two rate, three color” flow meter:

```
DGS-3000-28XMP:admin# config flow_meter profile_id 1 access_id 1 tr_tcm cir 1000 cbs 2000 pir
2000 pbs 2000 color_blind conform permit counter enable exceed permit replace_dscp 60 counter
enable violate drop
Command: config flow_meter profile_id 1 access_id 1 tr_tcm cir 1000 cbs 2000 pir 2000 pbs
2000 color_blind conform permit counter enable exceed permit replace_dscp 60 counter enable
violate drop


Success.
DGS-3000-28XMP:admin#
```

7-6 show flow_meter

Description

This command is used to display the flow-based metering (ACL Flow Metering) configuration.

Format

show flow_meter {[profile_id <value 1-512> | profile_name <name 32>] {access_id <value 1- 128>}}

Parameters

profile_id - (Optional) Specifies the profile ID. **<value 1-512>** - Enter the profile ID used here. This value must be between 1 and 512.
profile_name - (Optional) Specifies the name of the profile. **<name 32>** - Enter the profile name used here. The maximum length is 32 characters.
access_id - (Optional) Specifies the access ID. **<value 1- 128>** - Enter the access ID used here. This value must be between 1 and 128.

Restrictions

None.

Example

To display the flow metering configuration:

```
DGS-3000-28XMP:admin# show flow_meter
Command: show flow_meter

Flow Meter Information
------------------------------------------------------------------------------
Profile ID:1     Access ID:1     Mode : trTCM / ColorBlind
CIR(Kbps):1000     CBS(Kbyte):2000     PIR(Kbps):2000     PBS(Kbyte):2000
Action:
      Conform : Permit                        Counter: Enabled
       Exceed : Permit     Replace DSCP: 60   Counter: Enabled
      Violate : Drop                          Counter: Disabled
------------------------------------------------------------------------------
Total Entries: 1

DGS-3000-28XMP:admin#
```

7-7 config time_range

Description

This command is used to define a specific range of time to activate a function on the Switch by specifying which time range in a day and which days in a week are covered in the time range. The specified time range is based on the SNTP time or the configured time. If this time is not available, the time range will not be met.

Format

config time_range <range_name 32> [hours start_time <time hh:mm:ss> end_time <time hh:mm:ss> weekdays <daylist> | delete]

Parameters

<range_name 32> - Enter the time range name used here. This name can be up to 32 characters long.

hours - Specifies the time of a day.

start_time - Specifies the starting time of a day.

<time hh:mm:ss> - Enter the starting time here. (24-hr time). For example, 19:00 means 7PM. 19 is also acceptable. The time specified in the start_time parameter must be smaller than the time specified in the end_time parameter.

end_time - Specifies the ending time of a day. (24-hr time)

<time hh:mm:ss> - Enter the ending time here. (24-hr time). For example, 19:00 means 7PM. 19 is also acceptable. The time specified in the start_time parameter must be smaller than the time specified in the end_time parameter.

weekdays - Specifies the list of days contained in the time range. Use a dash to define a period of days. Use a comma to separate specific days.

<daylist> - Enter the weekdays that will be included in this configuration here. For example, mon-fri (Monday to Friday). sun, mon, fri (Sunday, Monday and Friday)

delete - Deletes a time range profile. When a time_range profile has been associated with ACL entries, deleting the time_range profile will fail.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure a time range named “1” that starts every Monday at 01:01:01am and ends at 02:02:02am:

```
DGS-3000-28XMP:admin# config time_range 1 hours start_time 1:1:1 end_time 2:2:2 weekdays mon
Command: config time_range 1 hours start_time 1:1:1 end_time 2:2:2 weekdays mon

Success.

DGS-3000-28XMP:admin#
```

7-8 show time_range

Description

This command is used to display the current time range settings.

Format

show time_range

Parameters

None.

Restrictions

None.

Example

To display the current time range settings:

```
DGS-3000-28XMP:admin# show time_range
Command: show time_range

Time Range Information
------------------------------
Range Name                : 1
Weekdays                  : Mon
Start Time                : 01:01:01
End Time                  : 02:01:01

Total Entries :1

DGS-3000-28XMP:admin#
```

7-9 show current_config access_profile

Description

This command is used to display the ACL part of the current configuration, when logged in with user level privileges.

The overall current configuration can be displayed by using the **show config current_config** command, which is accessible with administrator level privileges.

Format

show current_config access_profile

Parameters

None.

Restrictions

None.

Example

To display the ACL part of the current configuration:

```
DGS-3000-28XMP:admin# show current_config access_profile
Command: show current_config access_profile

#------------------------------------------------------------------

# ACL

create access_profile ethernet vlan profile_id 1
config access_profile profile_id 1 add access_id 1 ethernet vlan default port 1 permit

create access_profile ip source_ip_mask 255.255.255.255 profile_id 2
config access_profile profile_id 2 add access_id 1 ip source_ip 10.10.10.10 port 2 deny


#------------------------------------------------------------------

DGS-3000-28XMP:admin#
```

7-10 show access_profile hw_info

Description

This command is used to display the ACL hardware usage information.

Format

show access_profile hw_info

Parameters

None.

Restrictions

None.

Example

To display the ACL hardware usage information:

```
DGS-3000-28XMP:admin#show access_profile hw_info
Command: show access_profile hw_info

Slice ID/
Priority   Profile ID           Owner             Number of Rules
========== =========== ======================== ===================
 1/4094      1          System                        62
           -------------------------------------------------------
           Used                                      62
           Available                                 66
-------------------------------------------------------------------
 2/4093      2          System                        62
           -------------------------------------------------------
           Used                                      62
           Available                                 66
-------------------------------------------------------------------
 3/0
           -------------------------------------------------------
           Used                                      0
           Available                                 128
-------------------------------------------------------------------
 4/0
           -------------------------------------------------------
           Used                                      0
           Available                                 128
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

Chapter 8 Address Resolution Protocol (ARP) Command List

create arpentry <ipaddr> <macaddr>
delete arpentry [<ipaddr> | all]
config arpentry <ipaddr> <macaddr>
config arp_aging time <value 0-65535>
clear arptable
show arpentry {ipif <ipif_name 12> | ipaddress <ipaddr> | static | mac_address <macaddr>}

8-1 create arpentry

Description

This command is used to enter a static ARP entry into the Switch's ARP table.

Format

create arpentry <ipaddr> <macaddr>

Parameters

<ipaddr> - The IP address of the end node or station.
<macaddr> - The MAC address corresponding to the IP address above.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To create a static ARP entry for the IP address 10.48.74.121 and MAC address 00-50-BA-00-07-36:

```
DGS-3000-28XMP:admin# create arpentry 10.48.74.121 00-50-BA-00-07-36
Command: create arpentry 10.48.74.121 00-50-BA-00-07-36

Success.

DGS-3000-28XMP:admin#
```

8-2 delete arpentry

Description

This command is used to delete an ARP entry by specifying the IP address of the entry or all ARP entries.

Format

delete arpentry [<ipaddr> | all]

Parameters

<ipaddr> - The IP address of the end node or station.
all - Delete all ARP entries.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

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

```
DGS-3000-28XMP:admin# delete arpentry 10.48.74.121
Command: delete arpentry 10.48.74.121

Success.

DGS-3000-28XMP:admin#
```

8-3 config arpentry

Description

This command is used to configure a static entry's MAC address in the ARP table. Specifies the IP address and MAC address of the entry.

Format

config arpentry <ipaddr> <macaddr>

Parameters

<ipaddr> - The IP address of the end node or station.
<macaddr> - The MAC address corresponding to the IP address above.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure a static ARP entry, whose IP address is 10.48.74.121, set its MAC address to 00-50-BA-00-07-37:

```
DGS-3000-28XMP:admin# config arpentry 10.48.74.121 00-50-BA-00-07-37
Command: config arpentry 10.48.74.121 00-50-BA-00-07-37

Success.

DGS-3000-28XMP:admin#
```

8-4 config arp_aging time

Description

This command is used to set the maximum amount of time, in minutes, that a dynamic ARP entry can remain in the Switch's ARP table, without being accessed, before it is dropped from the table.

Format

config arp_aging time <value 0-65535>

Parameters

<value 0-65535>- Enter the ARP age-out time, in minutes. This value must be between 0 and 65535 minutes. The default value is 20.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure ARP aging time to 30 minutes:

```
DGS-3000-28XMP:admin# config arp_aging time 30
Command: config arp_aging time 30

Success.

DGS-3000-28XMP:admin#
```

8-5 clear arptable

Description

This command is used to clear all the dynamic entries from ARP table.

Format

clear arptable

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To clear the ARP table:

```
DGS-3000-28XMP:admin# clear arptable
Command: clear arptable

Success.

DGS-3000-28XMP:admin#
```

8-6 show arpentry

Description

This command is used to display the ARP table. You can filter the display by IP address, MAC address, Interface name, or static entries.

Format

show arpentry {ipif <ipif_name 12> | ipaddress <ipaddr> | static | mac_address <macaddr>}

Parameters

ipif - (Optional) Specifies the name of the IP interface the end node or station for which the ARP table entry was made, resides on. **<ipif_name 12>** - Enter the IP interface name here. This value can be up to 12 characters long.
ipaddress - (Optional) Specifies the IP address of the end node or station. **<ipaddr>** - Enter the IP address here.
static - (Optional) Specifies to display the static entries in the ARP table.
mac_address - (Optional) Specifies to display the ARP entries by MAC address. **<macaddr>** - Enter the MAC address here.

Restrictions

None.

Example

To display the ARP table:

```
DGS-3000-28XMP:admin# show arpentry
Command: show arpentry

ARP Aging Time : 20

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

Total Entries: 6

DGS-3000-28XMP:admin#
```

Chapter 9 ARP Spoofing Prevention Command List

config arp_spoofing_prevention [add gateway_ip <ipaddr> gateway_mac <macaddr> ports [<portlist> | all] | delete gateway_ip <ipaddr>]
config arp_spoofing_prevention syslog state [enable | disable]
show arp_spoofing_prevention

9-1 config arp_spoofing_prevention

Description

This command is used to configure the spoofing prevention entry to prevent spoofing of MAC addresses for the protected gateway. When an entry is created, those ARP packets whose sender IP matches the gateway IP of an entry, but the source MAC field does not match the gateway MAC of the entry will be dropped by the system.

Format

config arp_spoofing_prevention [add gateway_ip <ipaddr> gateway_mac <macaddr> ports [<portlist> | all] | delete gateway_ip <ipaddr>]

Parameters

add - Specifies to add an ARP spoofing prevention entry. **gateway_ip** - Specifies a gateway IP address to be configured. **<ipaddr>** - Enter the IP address used for this configuration here. **gateway_mac** - Specifies a gateway MAC address to be configured. **<macaddr>** - Enter the MAC address used for this configuration here. **ports** - Specifies a range of ports to be configured. **<portlist>** - Enter a list of ports used for the configuration here. **all** - Specifies all ports to be configured.
delete - Specifies to delete an ARP spoofing prevention entry. **gateway_ip** - Specifies a gateway IP to be configured. **<ipaddr>** - Enter the IP address used for this configuration here.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the ARP spoofing prevention entry:

```
DGS-3000-28XMP:admin# config arp_spoofing_prevention add gateway_ip 10.254.254.251
gateway_mac 00-00-00-11-11-11 ports 1-2
Command: config arp_spoofing_prevention add gateway_ip 10.254.254.251 gateway_ma
c 00-00-00-11-11-11 ports 1-2

Success.

DGS-3000-28XMP:admin#
```

9-2 config arp_spoofing_prevention syslog state

Description

This command is used to configure the syslog state of the ARP spoofing prevention.

Format

config arp_spoofing_prevention syslog state [enable | disable]

Parameters

enable -	Specifies to enable logging the MAC address of the attack when the IP address of the attack matches the gateway.
disable -	Specifies to disable logging the MAC address of the attack when the IP address of the attack matches the gateway.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable the syslog state of the ARP spoofing prevention:

```
DGS-3000-28XMP:admin#config arp_spoofing_prevention syslog state enable
Command: config arp_spoofing_prevention syslog state enable

Success.

DGS-3000-28XMP:admin#
```

9-3 show arp_spoofing_prevention

Description

This command is used to show the ARP spoofing prevention entry.

Format

show arp_spoofing_prevention

Parameters

None.

Restrictions

None.

Example

To display the ARP spoofing prevention entries:

```
DGS-3000-28XMP:admin#show arp_spoofing_prevention
Command: show arp_spoofing_prevention

 Log State: Enabled

Gateway IP         Gateway MAC          Ports
------------------ -------------------  --------------------
10.254.254.251     00-00-00-11-11-11    1-2

 Total Entries: 1


DGS-3000-28XMP:admin#
```

Chapter 10 Auto-Backup Command List

enable autobackup
disable autobackup
config autobackup path [tftp [<ipaddr> | <ipv6addr> | <domain_name 255>] dest_file <path_filename 64> | ftp [ftp: <string 128>] | none]
config autobackup mode [save_config | time_period | all]
config autobackup time_schedule [interval <min 1-525600> | periodic <time hh:mm:ss> {mon | tue | wed | thu | fri | sat | sun | weekdays | weekends | every_day}(1) | none]
config autobackup log state [enable | disable]
config autobackup trap state [enable | disable]
enable autobackup_encryption
disable autobackup_encryption
config autobackup file_template [<desc 64> | none]
show autobackup

10-1 enable autobackup

Description

This command is used to enable the auto-backup function.

Format

enable autobackup

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable the auto-backup function:

```
DGS-3000-28XMP:admin#enable autobackup
Command: enable autobackup

Success.

DGS-3000-28XMP:admin#
```

10-2 disable autobackup

Description

This command is used to disable the auto-backup function.

Format

disable autobackup

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To disable the auto-backup function:

```
DGS-3000-28XMP:admin#disable autobackup
Command: disable autobackup

Success.

DGS-3000-28XMP:admin#
```

10-3 config autobackup path

Description

This command is used to configure the path for the auto-backup function.

Format

config autobackup path [tftp [<ipaddr> | <ipv6addr> | <domain_name 255>] dest_file <path_filename 64> | ftp [ftp: <string 128>] | none]

Parameters

tftp - Specifies to back up running configuration to the remote server via TFTP.

<ipaddr> - Enter the IP address of the TFTP server.

<ipv6addr> - Enter the IPv6 address of the TFTP server.

<domain_name 255> - Enter the domain name of the host.

dest_file - Specifies the destination file path to be used.

<path_filename 64> - Enter the file path name. This can be a relative path name or an absolute path name.

ftp - Specifies to back up running configuration to the remote server via FTP.

ftp: - Specifies the FTP directory.

<string 128> - Enter the FTP string in the plain-text or the encrypted format here. This can be up to 128 characters long. The plain-text format should be entered in the following format: **user:password@ipaddr:tcpport/path_filename**. The encrypted format can only be entered when

auto-backup encryption is enabled, using the **enable autobackup_encryption** command. However, if auto-backup encryption is enabled and the FTP string is entered in the plain-text format, the FTP string will be saved in the configuration file in the encrypted format.

none - Specifies that there is no backup path.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the path for the auto-backup function via TFTP:

```
DGS-3000-28XMP:admin#config autobackup path tftp 10.48.74.121 dest_file backup.txt
Command: config autobackup path tftp 10.48.74.121 dest_file backup.txt

Success.

DGS-3000-28XMP:admin#
```

To configure the path for the auto-backup function via FTP:

```
DGS-3000-28XMP:admin#config autobackup path ftp ftp: user:12345@10.90.90.1:21/backup.txt
Command: config autobackup path ftp ftp: user:12345@10.90.90.1:21/backup.txt

Success.

DGS-3000-28XMP:admin#
```

10-4 config autobackup mode

Description

This command is used to configure the auto-backup mode. The running configuration is uploaded to the remote server based on the specified mode.

Format

config autobackup mode [save_config | time_period | all]

Parameters

save_config - Specifies to upload the running configuration file to the remote server when it is saved. This is the default value.

time_period - Specifies to upload the running configuration file to the remote server based on the time schedule configured in the **config autobackup time_schedule** command.

all - Specifies to upload the running configuration file to the remote server for both events mentioned above.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the auto-backup mode:

```
DGS-3000-28XMP:admin#config autobackup mode save_config
Command: config autobackup mode save_config

Success.

DGS-3000-28XMP:admin#
```

10-5 config autobackup time_schedule

Description

This command is used to configure the time schedule of the auto-backup function. The running configuration is uploaded to the remote server without saving in the NVRAM.

Format

config autobackup time_schedule [interval <min 1-525600> | periodic <time hh:mm:ss> {mon | tue | wed | thu | fri | sat | sun | weekdays | weekends | every_day}(1) | none]

Parameters

interval - Specifies the time interval between uploading the running configuration.
- **<min 1-525600>** - Enter time interval in minutes. The default value is 1440.

periodic - Specifies to upload the running configuration at the specific time.
- **<time hh:mm:ss>** - Enter the time in hour, minute, and second.
- **mon** - Specifies to upload on Mondays.
- **tue** - Specifies to upload on Tuesdays.
- **wed** - Specifies to upload on Wednesdays.
- **thu** - Specifies to upload on Thursdays.
- **fri** - Specifies to upload on Fridays.
- **sat** - Specifies to upload on Saturdays.
- **sun** - Specifies to upload on Sundays.
- **weekdays** - Specifies to upload during weekdays.
- **weekends** - Specifies to upload during weekends.
- **every_day** - Specifies to upload every day.

none - Specifies that there is no time schedule.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the time interval between uploading the running configuration:

```
DGS-3000-28XMP:admin#config autobackup time_schedule interval 1440
Command: config autobackup time_schedule interval 1440

Success.

DGS-3000-28XMP:admin#
```

10-6 config autobackup log state

Description

This command is used to configure the log state of the auto-backup function.

Format

config autobackup log state [enable | disable]

Parameters

enable - Specifies to enable the log state of the auto-backup function. This is the default value.
disable - Specifies to disable the log state of the auto-backup function.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To disable the log state of the auto-backup function:

```
DGS-3000-28XMP:admin#config autobackup log state disable
Command: config autobackup log state disable

Success.

DGS-3000-28XMP:admin#
```

10-7 config autobackup trap state

Description

This command is used to configure the trap state of the auto-backup function.

Format

config autobackup trap state [enable | disable]

Parameters

enable - Specifies to enable the trap state of the auto-backup function. This is the default value.
disable - Specifies to disable the trap state of the auto-backup function.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To disable the trap state of the auto-backup function:

```
DGS-3000-28XMP:admin#config autobackup trap state disable
Command: config autobackup trap state disable

Success.

DGS-3000-28XMP:admin#
```

10-8 enable autobackup_encryption

Description

This command is used to encrypt the FTP path when using the auto-backup function to upload the running configuration via FTP.

Format

enable autobackup_encryption

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable the encryption of the auto-backup function:

```
DGS-3000-28XMP:admin#enable autobackup_encryption
Command: enable autobackup_encryption

Success.

DGS-3000-28XMP:admin#
```

10-9 disable autobackup_encryption

Description

This command is used to decrypt the FTP path when use the auto-backup function to upload the running configuration via FTP.

Format

disable autobackup_encryption

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To disable the encryption of the auto-backup function:

```
DGS-3000-28XMP:admin#disable autobackup_encryption
Command: disable autobackup_encryption

Success.

DGS-3000-28XMP:admin#
```

10-10 config autobackup file_template

Description

This command is used to configure the file template of the auto-backup function. When configuring the file name, the following rules must be considered:

- This parameter must be a string. It can be any character contained in double quotation marks (" "), for example "switch".
- A formatted key string is a string that should be translated before being used as the filename. The formatted key string is formed using the following format: by **"%"+"keyword"+":"**
    - **%** - Indicates that the string that follows this character is a formatted key string.
    - **keyword** - Indicates that the keyword will be translated based on the actual value of the system. A command will be refused if an unknown or unsupported keyword is detected. The following keyword definitions must be considered:
        - d: Indicates the day of the month. This must be two digits from 01 to 31.
        - m: Indicates the month. This must be two digits from 01 to 12.
        - y: Indicates the last two digits of the year. This must be two digits from 00 to 99.
        - Y: Indicates the year. This must be four digits, for example 2016.
        - H: Indicates the hour. This must be two digits from 00 to 23.
        - M: Indicates the minutes. This must be two digits from 00 to 59.
        - S: Indicates the seconds. This must be two digits from 00 to 59.
    - **:** - Indicates the end of the formatted key sting. If the formatted key string is the last parameter of the command, its ending character (":") can be ignored. Any spaces between **"%"** and **":"** in the formatted key string will be ignored.

The formatted key string can be any the following characters: 0~9, a~z, A~Z, !@#$%^&()_+-=[]{};'.,<>`.

In the formatted key string, the "\" character is used as the escape character. Special characters after the "\" is the character itself like "\%" will allow the use of "%" itself, not the start indicator of a formatted key string.

Spaces outside of the formatted key string will be encapsulated.

Format

config autobackup file_template [<desc 64> | none]

Parameters

<desc 64> - Enter how to generate the uploaded filename.
none - Specifies to clear the file template and revert to the default template. The default template is “%d:-%m:-%Y:_%H:-%M:-%S:”.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the file template of the auto-backup function:

```
DGS-3000-28XMP:admin#config autobackup file_template "switch_%d:%m:%y:_%H:%M:"
Command: config autobackup file_template "switch_%d:%m:%y:_%H:%M:"

Success.

DGS-3000-28XMP:admin#
```

10-11 show autobackup

Description

This command is used to display the settings of the auto-backup function.

Format

show autobackup

Parameters

None.

Restrictions

None.

Example

To display the settings of the auto-backup function in the save configuration mode:

```
DGS-3000-28XMP:admin#show autobackup
Command: show autobackup

Autobackup Settings
--------------------------------------------------------------------------------
State        : Enabled
Path         : tftp://10.48.74.121/backup.txt
Mode         : Save configuration
Time schedule: -
File Template: "switch_%d:%m:%y:_%H:%M:"
Log State    : Enabled
Trap State   : Enabled
Encryption   : Enabled


DGS-3000-28XMP:admin#
```

To display the settings of the auto-backup function in the time period mode:

```
DGS-3000-28XMP:admin#show autobackup
Command: show autobackup

Autobackup Settings
--------------------------------------------------------------------------------
State        : Enabled
Path         : Ftp://user:123@192.168.0.1/backup.txt
Mode         : Time period
Time schedule: 12:30 Weekends
File Template: "switch_%d:%m:%Y:_%H:%M:"
Log State    : Enabled
Trap State   : Enabled
Encryption   : Disabled


DGS-3000-28XMP:admin#
```

To display the settings of the auto-backup function in the “all” mode:

```
DGS-3000-28XMP:admin#show autobackup
Command: show autobackup

Autobackup Settings
--------------------------------------------------------------------------------
State        : Disabled
Path         : Ftp://user@192.168.0.1/backup.txt
Mode         : All
Time schedule: 12:30 Mon
File Template: "switch_%d:%m:%Y:_%H:%M:"
Log State    : Enabled
Trap State   : Enabled
Encryption   : Disabled


DGS-3000-28XMP:admin#
```

To display the settings of the auto-backup function when auto-backup encryption is enabled:

```
DGS-3000-28XMP:admin#show autobackup
Command: show autobackup

Autobackup Settings
--------------------------------------------------------------------------------
State        : Enabled
Path         : ftp ******
Mode         : All
Time schedule: 12:30 Mon
File Template: "switch_%d:%m:%Y:_%H:%M:"
Log State    : Enabled
Trap State   : Enabled
Encryption   : Enabled


DGS-3000-28XMP:admin#
```

Chapter 11 Auto-Configuration Command List

enable autoconfig
disable autoconfig
show autoconfig
config autoconfig timeout <value 1-65535>

11-1 enable autoconfig

Description

This command is used to enable auto-configuration. When enabled, during power on initialization, the Switch will get the configuration file pathname and TFTP server IP address from the DHCP server. Then, the Switch will download the configuration file from the TFTP server for configuration of the system.

Format

enable autoconfig

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable auto-configuration:

```
DGS-3000-28XMP:admin# enable autoconfig
Command: enable autoconfig

Success.

DGS-3000-28XMP:admin#
```

11-2 disable autoconfig

Description

This command is used to disable auto-configuration. When disabled, the Switch will configure itself using the local configuration file

Format

disable autoconfig

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To disable auto-configuration:

```
DGS-3000-28XMP:admin# disable autoconfig
Command: disable autoconfig

Success.

DGS-3000-28XMP:admin#
```

11-3 show autoconfig

Description

This command is used to display if the auto-configuration is enabled or disabled.

Format

show autoconfig

Parameters

None.

Restrictions

None.

Example

To show the auto-configuration status:

```
DGS-3000-28XMP:admin# show autoconfig
Command: show autoconfig

Autoconfig State: Disabled
Timeout         : 50 sec

DGS-3000-28XMP:admin#
```

11-4 config autoconfig timeout

Description

This command is used to configure the timeout value. This timer is used to limit the length of time for getting configuration settings from the network. When timeout occurs, the auto-configuration operation will be stopped and the local configuration file will be used to configure the system.

Format

config autoconfig timeout <value 1-65535>

Parameters

<value 1-65535> - Specifies the timeout length in seconds. The default setting is 50 seconds.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure auto configuration timeout:

```
DGS-3000-28XMP:admin# config autoconfig timeout 60
Command: config autoconfig timeout 60

Success.

DGS-3000-28XMP:admin#
```

Chapter 12 Auto-Image Command List

enable autoimage
disable autoimage
config autoimage timeout <value 1-65535>
show autoimage

12-1 enable autoimage

Description

This command is used to enable the auto-image function. When enabled, the Switch automatically upgrades the firmware during the next bootup process. Because this function follows the same design as the auto-configuration function, a DHCP server and a TFTP server must be in the network. When the Switch boots up and the auto-image function is enabled, the Switch automatically becomes a DHCP client. The Switch will receive the network settings from the DHCP server including the TFTP server address and image file name. After requiring the network settings, the Switch downloads the firmware from the specified TFTP server. After the firmware was downloaded, the Switch will reboot.

Format

enable autoimage

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To enable the auto-image function:

```
DGS-3000-28XMP:admin#enable autoimage
Command: enable autoimage

Success.

DGS-3000-28XMP:admin#
```

12-2 disable autoimage

Description

This command is used to disable the auto-image function. When disabled, the Switch will use the local image file to boot up.

Format

disable autoimage

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To disable the auto-image function:

```
DGS-3000-28XMP:admin#disable autoimage
Command: disable autoimage

Success.

DGS-3000-28XMP:admin#
```

12-3 config autoimage timeout

Description

This command is used to specify the timeout value to get the image file through the network. If the image file cannot be received by the time, the auto-image function will be stopped and the current image file will be used.

Format

config autoimage timeout <value 1-65535>

Parameters

<value 1-65535> - Enter the timeout value in seconds. The default value is 50 seconds.

Restrictions

Only Administrators can issue this command.

Example

To configure the timeout value of the auto-image function:

```
DGS-3000-28XMP:admin#config autoimage timeout 60
Command: config autoimage timeout 60

Success.

DGS-3000-28XMP:admin#
```

12-4 show autoimage

Description

This command is used to display the auto-image status.

Format

show autoimage

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To display the auto-image status:

```
DGS-3000-28XMP:admin#show autoimage
Command: show autoimage

Autoimage State: Enabled
Timeout        : 60 sec


DGS-3000-28XMP:admin#
```

Chapter 13 Basic Commands Command List

create account [admin | operator | power_user | user] <username 15> {encrypt [plain_text | sha_1] <password>}
config account <username> {encrypt [plain_text | sha_1] <password>}
show account
delete account <username>
show switch
enable telnet {<tcp_port_number 1-65535>}
disable telnet
enable web {<tcp_port_number 1-65535>}
disable web
reboot {force_agree}
reset {[config | system]} {force_agree}
config firmware image <path_filename64>boot_up
create ipif <ipif_name 12> <network_address> <vlan_name 32> {state [enable | disable]}
config ipif <ipif_name 12> [{ipaddress <network_address> | vlan <vlan_name 32> | state [enable | disable]} | bootp | dhcp | ipv6 [ipv6address <ipv6networkaddr> | state [enable | disable]] | ip_mtu <value 512-1712> | ipv4 state [enable | disable] | dhcpv6_client [enable | disable] | dhcp_option12 [hostname <hostname 63> | clear_hostname | state [enable | disable]]]
delete ipif [<ipif_name 12> {ipv6address <ipv6networkaddr>} | all]
enable ipif [<ipif_name 12> | all]
disable ipif [<ipif_name 12> | all]
show ipif {<ipif_name 12>}
enable ipif_ipv6_link_local_auto [<ipif_name 12> | all]
disable ipif_ipv6_link_local_auto [<ipif_name 12> | all]
show ipif_ipv6_link_local_auto {<ipif_name 12>}
enable ip_tcp_pmtu_discovery
disable ip_tcp_pmtu_discovery
config ip_tcp_pmtu_discovery age_timer [<min 1-30> | infinite]
show ip_tcp_pmtu_discovery

13-1 create account

Description

This command is used to create user accounts. The username is between 1 and 15 characters, the password is between 0 and 15 characters. It is case sensitive. The maximum number of accounts (include admin and user) is 8.

Format

create account [admin | operator | power_user | user] <username 15> {encrypt [plain_text | sha_1] <password>}

Parameters

admin - Specifies the name of the admin account.
operator - Specifies the name for the operator user account.
power_user - Specifies the name for the Power-user account.
user - Specifies the name of the user account.
<username 15> - Enter the username used here. This name can be up to 15 characters long.
encrypt - (Optional) Specifies the encryption applied to the account. **plain_text** - Specifies the password in plaintext form. **sha_1** - Specifies the password in the SHA-1 encrypted form. **<password>** - Enter the password for the user account. The length of password in plain-text form and in encrypted form are different. For the plain-text form, passwords must have a minimum of 0 character and can have a maximum of 15 characters. For the encrypted form password, the length is fixed to 35 bytes long. The password is case-sensitive.

Restrictions

Only Administrators can issue this command.

Example

To create the admin-level user “dlink”:

```
DGS-3000-28XMP:admin# create account admin dlink
Command: create account admin dlink

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

Success.

DGS-3000-28XMP:admin#
```

To create the user-level user “Remote-Manager”:

```
DGS-3000-28XMP:admin# create account user Remote-Manager
Command: create account user Remote-Manager

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

Success.

DGS-3000-28XMP:admin#
```

13-2 config account

Description

This command is used to configure user accounts. When the password information is not specified in the command, the system will prompt the user to input the password interactively. For this case, the user can only input the plaintext password.

If the password is present in the command, the user can select to input the password in the plaintext form or in the encrypted form. The encryption algorithm is based on SHA-1.

Format

config account <username> {encrypt [plain_text | sha_1] <password>}

Parameters

<username> - Enter the user name of the account that has been defined.

encrypt - (Optional) Specifies that the password will be encrypted.

plain_text - Specifies the password in plaintext form.

sha_1 - Specifies the password in the SHA-1 encrypted form.

<password> - Enter the password for the user account. The length for of password in plain-text form and in encrypted form are different. For the plain-text form, passwords must have a minimum of 0 character and can have a maximum of 15 characters. For the encrypted form password, the length is fixed to 35 bytes long. The password is case-sensitive.

Restrictions

Only Administrators can issue this command.

Example

To configure the user password of “dlink” account:

```
DGS-3000-28XMP:admin# config account dlink
Command: config account dlink

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

Success.

DGS-3000-28XMP:admin#
```

To configure the user password of “administrator” account:

```
DGS-3000-28XMP:admin# config account administrator encrypt sha_1
*@&cRDtpNCeBiq15KOQsKVyrA0sAiCIZQwq
Command: config account administrator encrypt sha_1 *@&cRDtpNCeBiq15KOQsKVyrA0sAiCIZQwq

Success.

DGS-3000-28XMP:admin#
```

13-3 show account

Description

This command is used to display user accounts that have been created.

Format

show account

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To display the accounts that have been created:

```
DGS-3000-28XMP:admin# show account
Command: show account

 Current Accounts:
 Username             Access Level
 ---------------      ------------
 admin                Admin
 oper                 Operator
 power                Power_user
 user                 User

 Total Entries : 4

DGS-3000-28XMP:admin#
```

13-4 delete account

Description

This command is used to delete an existing account.

Format

delete account <username>

Parameters

<username> - Enter the user name to be deleted.

Restrictions

Only Administrators can issue this command.

Example

To delete the user account “System”:

```
DGS-3000-28XMP:admin# delete account System
Command: delete account System

Success.

DGS-3000-28XMP:admin#
```

13-5 show switch

Description

This command is used to display the Switch information.

Format

show switch

Parameters

None.

Restrictions

None.

Example

To display the Switch information:

```
DGS-3000-28XMP:admin#show switch
Command: show switch

Device Type                : DGS-3000-28XMP Gigabit Ethernet Switch
MAC Address                : F0-7D-68-15-10-00
IP Address                 : 10.90.90.90 (Manual)
VLAN Name                  : default
Subnet Mask                : 255.0.0.0
Default Gateway            : 0.0.0.0
Boot PROM Version          : Build 4.00.001
Firmware Version           : Build 4.00.010
Hardware Version           : B1
Serial Number              : DGS-3000-28XMP
System Name                :
System Location            :
System Uptime              : 0 days, 2 hours, 35 minutes, 11 seconds
System Contact             :
Spanning Tree              : Disabled
GVRP                       : Disabled
IGMP Snooping              : Disabled
MLD Snooping               : Disabled
VLAN Trunk                 : Disabled
Telnet                     : Enabled (TCP 23)
Web                        : Enabled (TCP 80)
SNMP                       : Disabled
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

13-6 enable telnet

Description

This command is used to enable Telnet and configure port number.

Format

enable telnet {<tcp_port_number 1-65535>}

Parameters

<tcp_port_number 1-65535> - (Optional) The TCP port number. TCP ports are numbered between 1 and 65535. The “well-known” TCP port for the Telnet protocol is 23.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable Telnet and configure port number:

```
DGS-3000-28XMP:admin# enable telnet 23
Command: enable telnet 23

Success.

DGS-3000-28XMP:admin#
```

13-7 disable telnet

Description

This command is used to disable Telnet.

Format

disable telnet

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To disable Telnet:

```
DGS-3000-28XMP:admin# disable telnet
Command: disable telnet

Success.

DGS-3000-28XMP:admin#
```

13-8 enable web

Description

This command is used to enable HTTP and configure port number.

Format

enable web {<tcp_port_number 1-65535>}

Parameters

<tcp_port_number 1-65535> - (Optional) Enter the TCP port number. TCP ports are numbered between 1 and 65535. The “well-known” TCP port for the HTTP protocol is 80.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable HTTP and configure port number:

```
DGS-3000-28XMP:admin# enable web 80
Command: enable web 80

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

DGS-3000-28XMP:admin#
```

13-9 disable web

Description

This command is used to disable HTTP.

Format

disable web

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To disable HTTP:

```
DGS-3000-28XMP:admin# disable web
Command: disable web

Success.

DGS-3000-28XMP:admin#
```

13-10 reboot

Description

This command is used to restart the Switch.

Format

reboot {force_agree}

Parameters

force_agree - (Optional) Specifies to immediately reboot the Switch without further confirmation.

Restrictions

Only Administrators can issue this command.

Example

To reboot the Switch:

```
DGS-3000-28XMP:admin# reboot
Command: reboot

Are you sure to proceed with the system reboot?(y/n)
Please wait, the switch is rebooting…
```

13-11 reset

Description

This command is used to provide reset functions. The configuration setting will be reset to the default setting by the **reset config** command. For the **reset system** command, the device will store the reset setting in the NVRAM and then reboot the system. The **reset** command will not reset the IP address, logs, user accounts and banner configured on the system.

Format

reset {[config | system]} {force_agree}

Parameters

config - (Optional) Specifies that all configuration parameters will be reset to default settings. The device will not save the settings to the NVRAM or reboot.
system - (Optional) Specifies that all parameters will be reset to default settings. Then the Switch will do a factory reset, save the settings to the NVRAM, and reboot.
force_agree - (Optional) Specifies to immediately reset to default settings without further confirmation.

Restrictions

Only Administrators can issue this command.

Example

To reset the Switch:

```
DGS-3000-28XMP:admin# reset system
Command: reset system

Are you sure you want to proceed with system reset?(y/n)
 y-(reset all include configuration, save, reboot )
 n-(cancel command) y
Reboot & Load Factory Default Configuration...

Saving configurations and logs to NV-RAM...... Done.
Please wait, the switch is rebooting...
```

13-12 config firmware image

Description

This command is used to select a firmware file as a boot-up file. This command is required when multiple firmware images are supported.

Format

config firmware image <path_filename64> boot_up

Parameters

<path_filename64> - Enter a firmware file on the device file system.
boot_up - Specifies the firmware as the boot-up firmware.

Restrictions

Only Administrators can issue this command.

Example

To configure c:/DES3200_Run_4_00_014.had as the boot-up image:

```
DGS-3000-28XMP:admin# config firmware image c:/DES3200_Run_4_02_004.had boot_up
Command: config firmware image c:/DES3200_Run_4_02_004.had boot_up

Success.

DGS-3000-28XMP:admin#
```

13-13 create ipif

Description

This command is used to create an IP interface.

Format

create ipif <ipif_name 12> <network_address> <vlan_name 32> {state [enable | disable]}

Parameters

<ipif_name 12> - Enter the IP interface name here. This name can be up to 12 characters long.
<network_address> - Specifies the IPv4 network address (xx.xx.xx.xx/xx). It specifies a host address and length of the network mask.
<vlan_name 32> - Enter the VLAN name used here. This name can be up to 32 characters long.
state - (Optional) Specifies the state of the IP interface. **enable** - Specifies that the IP interface state will be enabled. **disable** - Specifies that the IP interface state will be disabled.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To create an IP interface:

```
DGS-3000-28XMP:admin# create ipif Inter2 192.168.16.1/24 default state enable
Command: create ipif Inter2 192.168.16.1/24 default state enable

Success.

DGS-3000-28XMP:admin#
```

13-14 config ipif

Description

This command is used to configure the IP interface.

Format

config ipif <ipif_name 12> [{ipaddress <network_address> | vlan <vlan_name 32> | state [enable | disable]} | bootp | dhcp | ipv6 [ipv6address <ipv6networkaddr> | state [enable | disable]] | ip_mtu <value 512-1712> | ipv4 state [enable | disable] | dhcpv6_client [enable | disable] | dhcp_option12 [hostname <hostname 63> | clear_hostname | state [enable | disable]]]

Parameters

<ipif_name 12> - Enter the IP interface name used here. This name can be up to 12 characters long.
ipaddress - (Optional) Specifies a network on an ipif. The address should specify a host address and length of the network mask. Since an ipif can have only one IPv4 address, the newly configured address will overwrite the original one. **<network_address>** - Enter the network address used here.
vlan - (Optional) Specifies the name of the VLAN here. **<vlan_name 32>** - Enter the VLAN name used here. This name can be up to 32 characters long.
state - (Optional) Specifies to enable or disable the interface. **enable** - Specifies to enable the interface. **disable** - Specifies to disable the interface.

bootp - Specifies to use BOOTP to obtain the IPv4 address.

dhcp - Specifies to use DHCP to obtain the IPv4 address.

ipv6 - Specifies that the IPv6 configuration will be done.

- **ipv6address** - Specifies the IPv6 network address. The address should specify a host address and length of network prefix. There can be multiple IPv6 addresses defined on an interface. Thus, as a new address is defined, it is added on this ipif.
  - **<ipv6networkaddr>** - Enter the IPv6 address used here.
- **state** - Specifies that the IPv6 interface state will be set to enabled or disabled.
  - **enable** - Specifies that the IPv6 interface will be enabled.
  - **disable** - Specifies that the IPv6 interface will be disabled.

ip_mtu - Specifies to configure the IP Maximum Transmission Unit (MTU) of an interface.

- **<value 512-1712>** - Enter the MTU value. The default value is 1500 bytes.

ipv4 - Specifies that the IPv4 configuration will be done.

- **state** - Specifies that the IPv4 interface state will be set to enabled or disabled.
  - **enable** - Specifies that the IPv4 interface will be enabled.
  - **disable** - Specifies that the IPv4 interface will be disabled.

dhcpv6_client - Specifies the DHCPv6 client state of the interface.

- **enable** - Specifies that the DHCPv6 client state of the interface will be enabled.
- **disable** - Specifies that the DHCPv6 client state of the interface will be disabled.

dhcp_option12 - Specifies the DHCP Option 12.

- **hostname** - Specifies the host name to be inserted in the DHCPDISCOVER and DHCPREQUEST message.
  - **<hostname 63>** - Enter a name starting with a letter, end with a letter or digit, and only consists of letters, digits, and hyphens. The maximal length is 63.
- **clear_hostname** - Specifies to clear the hostname setting. If host name is empty, the system name will be used to encode Option 12. If the length of the system name is longer than 63, the superfluous characters will be truncated. If the system name is also empty, then the product model name will be used to encode Option 12.
- **state** - Specifies to enable or disable insertion of Option 12 in the DHCPDISCOVER and DHCPREQUEST message. The state is disable by default.
  - **enable** - Specifies to enable insertion of Option 12 in the DHCPDISCOVER and DHCPREQUEST message.
  - **disable** - Specifies to disable insertion of Option 12 in the DHCPDISCOVER and DHCPREQUEST message.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure an interface's IPv4 network address:

```
DGS-3000-28XMP:admin# config ipif System ipaddress 192.168.69.123/24 vlan default
Command: config ipif System ipaddress 192.168.69.123/24 vlan default

Success.

DGS-3000-28XMP:admin#
```

13-15 delete ipif

Description

This command is used to delete an IP interface.

Format

delete ipif [<ipif_name 12> {ipv6address <ipv6networkaddr>} | all]

Parameters

<ipif_name 12> - Enter the IP interface name used here. This name can be up to 12 characters long. **ipv6address** – (Optional) Specifies the IPv6 network address. The address should specify a host address and length of network prefix. There can be multiple IPv6 addresses defined on an interface. **<ipv6networkaddr>** - Enter the IPv6 address used here.
all – Specifies that all the IP interfaces will be used.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete an IP interface:

```
DGS-3000-28XMP:admin# delete ipif newone
Command: delete ipif newone

Success.

DGS-3000-28XMP:admin#
```

13-16 enable ipif

Description

This command is used to enable the IP interface.

Format

enable ipif [<ipif_name 12> | all]

Parameters

<ipif_name 12> - Enter the IP interface name used here. This name can be up to 12 characters long.
all - Specifies that all the IP interfaces will be enabled.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable an IP interface:

```
DGS-3000-28XMP:admin# enable ipif newone
Command: enable ipif newone

Success.

DGS-3000-28XMP:admin#
```

13-17 disable ipif

Description

This command is used to disable an IP interface.

Format

disable ipif [<ipif_name 12> | all]

Parameters

<ipif_name 12> - Enter the IP interface name used here. This name can be up to 12 characters long.
all - Specifies that all the IP interfaces will be disabled.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To disable an IP interface:

```
DGS-3000-28XMP:admin# disable ipif newone
Command: disable ipif newone

Success.

DGS-3000-28XMP:admin#
```

13-18 show ipif

Description

This command is used to display an IP interface.

Format

show ipif {<ipif_name 12>}

Parameters

<ipif_name 12> - (Optional) Enter the IP interface name used here. This name can be up to 12 characters long.

Restrictions

None.

Example

To display an IP interface:

```
DGS-3000-28XMP:admin#show ipif
Command: show ipif

IP Interface                : System
VLAN Name                   : default
Interface Admin State       : Enabled
DHCPv6 Client State         : Disabled
Link Status                 : LinkUp
IPv4 Address                : 10.90.90.90/8 (Manual)
IPv4 State                  : Enabled
IPv6 State                  : Enabled
IP MTU                      : 1500
DHCP Option12 State         : Disabled
DHCP Option12 Host Name     :


Total Entries: 1

DGS-3000-28XMP:admin#
```

13-19 enable ipif_ipv6_link_local_auto

Description

This command is used to enable the auto-configuration of link local address when there are no IPv6 addresses explicitly configured. When an IPv6 address is explicitly configured, the link local address will be automatically configured, and the IPv6 processing will be started. When there is no IPv6 address explicitly configured, by default, link local address is not configured and the IPv6 processing will be disabled. By enabling this automatic configuration, the link local address will be automatically configured and IPv6 processing will be started.

Format

enable ipif_ipv6_link_local_auto [<ipif_name 12> | all]

Parameters

<ipif_name 12> - Enter the IP interface name used here. This name can be up to 12 characters long.
all - Specifies that all the IP interfaces will be used.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable the IP interface for IPv6 link local automatic:

```
DGS-3000-28XMP:admin# enable ipif_ipv6_link_local_auto newone
Command: enable ipif_ipv6_link_local_auto newone

Success.

DGS-3000-28XMP:admin#
```

13-20 disable ipif_ipv6_link_local_auto

Description

This command is used to disable the auto-configuration of the link local address when no IPv6 address are configured.

Format

disable ipif_ipv6_link_local_auto [<ipif_name 12> | all]

Parameters

<ipif_name 12> - Enter the IP interface name used here. This name can be up to 12 characters long.
all - Specifies that all the IP interfaces will be used.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To disable the IP interface for IPv6 link local automatic:

```
DGS-3000-28XMP:admin# disable ipif_ipv6_link_local_auto newone
Command: disable ipif_ipv6_link_local_auto newone

Success.

DGS-3000-28XMP:admin#
```

13-21 show ipif_ipv6_link_local_auto

Description

This command is used to display the link local address automatic configuration state.

Format

show ipif_ipv6_link_local_auto {<ipif_name 12>}

Parameters

<ipif_name 12> - (Optional) Enter the IP interface name used here. This name can be up to 12 characters long.

Restrictions

None.

Example

To display the link local address automatic configuration state.

```
DGS-3000-28XMP:admin# show ipif_ipv6_link_local_auto
Command: show ipif_ipv6_link_local_auto

 IPIF: System          Automatic Link Local Address: Disabled

DGS-3000-28XMP:admin#
```

13-22 enable ip_tcp_pmtu_discovery

Description

This command is used to enable TCP Path Maximum Transmission Unit (PMTU) discovery function on the Switch.

Format

enable ip_tcp_pmtu_discovery

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable TCP PMTU discovery:

```
DGS-3000-28XMP:admin#enable ip_tcp_pmtu_discovery
Command: enable ip_tcp_pmtu_discovery

Success.

DGS-3000-28XMP:admin#
```

13-23 disable ip_tcp_pmtu_discovery

Description

This command is used to disable TCP PMTU discovery function on the Switch.

Format

disable ip_tcp_pmtu_discovery

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To disable TCP PMTU discovery:

```
DGS-3000-28XMP:admin#disable ip_tcp_pmtu_discovery
Command: disable ip_tcp_pmtu_discovery

Success.

DGS-3000-28XMP:admin#
```

13-24 config ip_tcp_pmtu_discovery age_timer

Description

This command is used to configure the aging time for TCP PMTU discovery on the Switch.

Format

config ip_tcp_pmtu_discovery age_timer [<min 1-30> | infinite]

Parameters

<min 1-30> - Enter the aging time in minutes. The default value is 10 minutes.
infinite - Specifies that TCP PMTU discovery will not be aged out.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the aging time for TCP PMTU discovery to 1 minute:

```
DGS-3000-28XMP:admin#config ip_tcp_pmtu_discovery age_timer 1
Command: config ip_tcp_pmtu_discovery age_timer 1

Success.

DGS-3000-28XMP:admin#
```

13-25 show ip_tcp_pmtu_discovery

Description

This command is used to display the information of TCP PMTU discovery.

Format

show ip_tcp_pmtu_discovery

Parameters

None.

Restrictions

None.

Example

To display the information of TCP PMTU discovery:

```
DGS-3000-28XMP:admin#show ip_tcp_pmtu_discovery
Command: show ip_tcp_pmtu_discovery

IP TCP Path-mtu-discovery: Enabled
IP TCP Path-mtu-discovery Aging Time: 1 min


DGS-3000-28XMP:admin#
```

Chapter 14 BPDU Attack Protection Command List

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

14-1 config bpdu_protection ports

Description

This command is used to configure the BPDP protection function for the ports on the Switch. In general, there are two states in BPDU protection function. One is normal state, and another is under attack state. The under attack state has three modes: drop, block, and shutdown. A BPDU protection-enabled port will enter under attack state when it receives one STP BPDU packet. And it will take action based on the configuration. Thus, BPDU protection can only be enabled on STP-disabled port.

BPDU protection has a higher priority than the Forward BPDU (FBPDU) setting configured by configure STP command in the determination of BPDU handling. That is, when FBPDU is configured to forward STP BPDU but BPDU protection is enabled, then the port will not forward STP BPDU.

Format

config bpdu_protection ports [<portlist> | all] {state [enable | disable] | mode [drop | block | shutdown]}(1)

Parameters

<portlist> - Specifies a range of ports to be configured (port number).
all - Specifies that all ports will be configured.
state - Specifies the BPDU protection state. The default state is disable **enable** - Specifies to enable BPDU protection. **disable** - Specifies to disable BPDU protection.
mode - Specifies the BPDU protection mode. The default mode is shutdown **drop** - Specifies to drop all received BPDU packets when the port enters under_attack state. **block** - Specifies to drop all packets (include BPDU and normal packets) when the port enters under_attack state. **shutdown** - Specifies to shut down the port when the port enters under_attack state.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To set the port state enable and drop mode:

```
DGS-3000-28XMP:admin# config bpdu_protection ports 1 state enable mode drop
Commands: config bpdu_protection ports 1 state enable mode drop

Success.

DGS-3000-28XMP:admin#
```

14-2 config bpdu_protection recovery_timer

Description

This command is used to configure BPDU protection recovery timer. When a port enters the 'under attack' state, it can be disabled or blocked based on the configuration. The state can be recovered manually or by the auto recovery mechanism. To manually recover the port, the user needs to disable and re-enable the port.

Format

config bpdu_protection recovery_timer [<sec 60-1000000> | infinite]

Parameters

<sec 60 –1000000> - Enter the timer (in seconds) used by the Auto-recovery mechanism to recover the port. The valid range is 60 to 1000000. The default value is 60.
infinite - Specifies that the port will not be recovered automatically.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the bpdu_protection recovery_timer to 120 seconds on the Switch:

```
DGS-3000-28XMP:admin# config bpdu_protection recovery_timer 120
Commands: config bpdu_protection recovery_timer 120

Success.

DGS-3000-28XMP:admin#
```

14-3 config bpdu_protection

Description

This command is used to configure the BPDU protection trap state or state for the Switch.

Format

config bpdu_protection [trap | log] [none | attack_detected | attack_cleared | both]

Parameters

trap - Specifies the trap state.

log - Specifies the log state.
none - Specifies that neither attack_detected nor attack_cleared is trapped or logged.
attack_detected - Specifies that events will be logged or trapped when the BPDU attacks are detected.
attack_cleared - Specifies that events will be logged or trapped when the BPDU attacks are cleared.
both - Specifies that the events of attack_detected and attack_cleared shall be trapped or logged.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the BPDU protection trap state as both on the Switch:

```
DGS-3000-28XMP:admin# config bpdu_protection trap both
Commands: config bpdu_protection trap both

Success.

DGS-3000-28XMP:admin#
```

14-4 enable bpdu_protection

Description

This command is used to enable BPDU protection function globally for the Switch.

Format

enable bpdu_protection

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable BPDU protection function globally on the Switch:

```
DGS-3000-28XMP:admin# enable bpdu_protection
Commands: enable bpdu_protection

Success.

DGS-3000-28XMP:admin#
```

14-5 disable bpdu_protection

Description

This command is used to disable BPDU protection function globally for the Switch.

Format

disable bpdu_protection

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To disable BPDU protection function globally on the Switch:

```
DGS-3000-28XMP:admin# disable bpdu_protection
Commands: disable bpdu_protection

Success.

DGS-3000-28XMP:admin#
```

14-6 show bpdu_protection

Description

This command is used to display BPDU protection global configuration, or per-port configuration and current status.

Format

show bpdu_protection {ports {<portlist>}}

Parameters

ports - (Optional) Specifies a range of ports to be configured. **<portlist>** - Enter a range of ports here.

Restrictions

None.

Example

To display the global configuration of BPDU protection on the Switch:

```
DGS-3000-28XMP:admin# show bpdu_protection
Commands: show bpdu_protection

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


DGS-3000-28XMP:admin#
```

To show the BPDU protection status on ports 1-12:

```
DGS-3000-28XMP:admin# show bpdu_protection ports 1-12
Commands: show bpdu_protection ports 1-12

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

DGS-3000-28XMP:admin#
```

Chapter 15 Cable Diagnostics Command List

cable_diag ports [<portlist> | all]

15-1 cable_diag ports

Description

This command is used to configure cable diagnostics on ports. For Fast Ethernet (FE) ports, two pairs of cable will be diagnosed. For Gigabit Ethernet (GE) ports, four pairs of cable will be diagnosed.

The following test result can be displayed.

- **Open** - The cable in the error pair does not have a connection at the specified position.
- **Short** - The cable in the error pair has a short problem at the specified position.
- **Crosstalk** - The cable in the error pair has a crosstalk problem at the specified position.
- **Shutdown** - The remote partner is powered off.
- **Unknown** - The diagnosis does not obtain the cable status. Please try again.
- **OK** - The pair or cable has no error.
- **No cable** - The port does not have any cable connected to the remote partner.

When a port is in link-up status, the test will obtain the distance of the cable. Since the status is link-up, the cable will not have the short or open problem. But the test may still detect the crosstalk problem.

When a port is in link-down status, the link-down may be caused by many factors.

1. When the port has a normal cable connection, but the remote partner is powered off, the cable diagnosis can still diagnose the health of the cable as if the remote partner is powered on.
2. When the port does not have any cable connection, the result of the test will indicate no cable.
3. The test will detect the type of error and the position where the error occurs.

When the link partner is Fast Ethernet ports:

- Where the **link partner is powered on with no errors** and the **link is up**, this command cannot detect the cable length
- Where the **link partner is powered on with errors**, this command can detect whether the error is open, short, or crosstalk. In this case this command can also detect the distance of the error
- Where the l**ink partner is powered down with no errors** and the **link is down**, this command cannot detect the cable length
- When the **link partner is powered down with errors**, this command can detect whether the error is open, short, or crosstalk. In this case this command can also detect the distance of the error
- When there is **no link partner** with **no errors** and the **link is up**, this command can detect the cable length
- When there is **no link partner with errors**, this command can detect whether the error is open, short, or crosstalk. In this case this command can also detect the distance of the error

When the link partner is Gigabit Ethernet ports:

- Where the **link partner is powered on with no errors** and the **link is up**, this command can detect the cable length
- Where the **link partner is powered on with errors**, this command can detect whether the error is open, short, or crosstalk. In this case this command can also detect the distance of the error
- Where the **link partner is powered down with no errors** and the **link is down**, this command cannot detect the cable length
- When the **link partner is powered down with errors**, this command can detect whether the error is open, short, or crosstalk. In this case this command can also detect the distance of the error
- When there is **no link partner with no errors** and the **link is up**, this command can detect the cable length
- When there is **no link partner with errors**, this command can detect whether the error is open, short, or crosstalk. In this case this command can also detect the distance of the error

NOTE: This test is only for copper cable. The fiber port is not tested. For the combo ports, only the copper media will be tested. The cable diagnosis does not support on the Pair 1 and 4 if the link partner is FE port. If the link partner is FE port, the target port's link will be down after the test.

Format

cable_diag ports [<portlist> | all]

Parameters

<portlist> - Enter a list of ports used for the configuration here.
all - Specifies that all the ports will be used for this configuration.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

Test the cable on port 1, 11, and 12:

```
DGS-3000-28XMP:admin# cable_diag ports 1,11-12
Command: cable_diag ports 1,11-12

Perform Cable Diagnostics ...

Port      Type      Link Status    Test Result                Cable Length (M)
------  ----------  -------------  -------------------------  -----------------
1       100BASE-T   Link Up        OK                               4
11      100BASE-T   Link Down      No Cable                         -
12      100BASE-T   Link Down      No Cable                         -


DGS-3000-28XMP:admin#
```

Chapter 16 Command Logging Command List

enable command logging
disable command logging
show command logging

16-1 enable command logging

Description

This command is used to enable the command logging function. This is disabled by default.

NOTE: When the Switch is under booting procedure, all configuration command should not be logged. When the user under AAA authentication, the user name should not changed if user uses “enable admin” command to replace its privilege.

Format

enable command logging

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To enable the command logging function:

```
DGS-3000-28XMP:admin# enable command logging
Command: enable command logging

Success.

DGS-3000-28XMP:admin#
```

16-2 disable command logging

Description

This command is used to disable the command logging function.

Format

disable command logging

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To disable the command logging:

```
DGS-3000-28XMP:admin# disable command logging
Command: disable command logging

Success.

DGS-3000-28XMP:admin#
```

16-3 show command logging

Description

This command is used to display the Switch's general command logging configuration status.

Format

show command logging

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To show the command logging configuration status:

```
DGS-3000-28XMP:admin# show command logging
Command: show command logging

Command Logging State : Disabled

DGS-3000-28XMP:admin#
```

Chapter 17 Compound Authentication Command List

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

17-1 enable authorization attributes

Description

This command is used to enable authorization.

Format

enable authorization attributes

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To globally enable authorization attributes:

```
DGS-3000-28XMP:admin# enable authorization attributes
Command: enable authorization attributes

Success.

DGS-3000-28XMP:admin#
```

17-2 disable authorization attributes

Description

This command is used to disable authorization.

Format

disable authorization attributes

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To globally disable authorization attributes:

```
DGS-3000-28XMP:admin# disable authorization attributes
Command: disable authorization attributes

Success.

DGS-3000-28XMP:admin#
```

17-3 create authentication guest_vlan

Description

This command is used to assign a static VLAN to be a guest VLAN. The specific VLAN which is assigned to be a guest VLAN must already exist. The specific VLAN which is assigned to be a guest VLAN can't be deleted.

Format

create authentication guest_vlan [vlan <vlan_name 32> | vlanid <vlanid 1-4094>]

Parameters

vlan - Specifies the guest VLAN by VLAN name. **<vlan_name 32>** - Enter the guest VLAN by VLAN name. The VLAN name can be up to 32 characters long.
vlanid - Specifies the guest VLAN by VLAN ID. **<vlanid 1-4094>** - Enter the guest VLAN by VLAN ID. The VLAN ID value must be between 1 and 4094.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To assign a static VLAN to be a guest VLAN:

```
DGS-3000-28XMP:admin#create authentication guest_vlan vlan guestVLAN
Command: create authentication guest_vlan vlan guestVLAN

Success.

DGS-3000-28XMP:admin#
```

17-4 delete authentication guest_vlan

Description

This command is used to delete guest VLAN setting, but won't delete the static VLAN.

All ports which enable guest VLAN will move to original VLAN after deleting guest VLAN.

Format

delete authentication guest_vlan [vlan <vlan_name 32> | vlanid <vlanid 1-4094>]

Parameters

vlan - Specifies the guest VLAN by VLAN name. **<vlan_name 32>** - Enter the VLAN name here. This name can be up to 32 characters long.
vlanid - Specifies the guest VLAN by VLAN ID. **<vlanid 1-4094>** - Enter the VLAN ID here. This ID must be between 1 and 4094.

Restrictions

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

Example

To delete guest VLAN configuration:

```
DGS-3000-28XMP:admin#delete authentication guest_vlan vlan guestVLAN
Command: delete authentication guest_vlan vlan guestVLAN

Success.

DGS-3000-28XMP:admin#
```

17-5 config authentication guest_vlan

Description

This command is used to assign or remove ports to or from a guest VLAN.

Format

config authentication guest_vlan [vlan <vlan_name 32> | vlanid <vlanid 1-4094>] [add | delete] ports [<portlist> | all]

Parameters

vlan - Specifies the guest VLAN name.
  <vlan_name 32> - Enter the guest VLAN name. The VLAN name can be up to 32 characters long.

vlanid - Specifies the guest VLAN VID.
  <vlanid 1-4094> - Enter the guest VLAN VID. The VLAN ID value must be between 1 and 4094.

add - Specifies to add a port list to the guest VLAN.

delete - Specifies to delete a port list from the guest VLAN.

ports - Specifies a port or range of ports to configure.
  <portlist> - Enter a range of ports to configure.
  all - Specifies to configure all ports.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure authentication for all ports for a guest VLAN called “guestVLAN”:

```
DGS-3000-28XMP:admin#config authentication guest_vlan vlan guestVLAN add ports
all
Command: config authentication guest_vlan vlan guestVLAN add ports all

Success.

DGS-3000-28XMP:admin#
```

17-6 config authentication ports

Description

This command is used to configure the authorization mode and authentication method on ports.

Format

config authentication ports [<portlist> | all] {auth_mode [port_based | host_based] | multi_authen_methods [none | any | dot1x_impb | impb_wac | mac_impb| mac_wac]}(1)

Parameters

<portlist> - Enter a port or range of ports to configure.

all - Specifies to configure all ports.

auth_mode - The authorization mode is port-based or host-based.
  port-based - If one of the attached hosts passes the authentication, all hosts on the same port will be granted access to the network. If the user fails the authentication, this port will keep trying the next authentication.

host-based - Specifies to allow every user to be authenticated individually. The "vlanid" can authenticate the client on a specific authenticated VLAN(s).If the "vlanid" is not specified, or all the VLANs are disabled, it means the host does not care which VLAN the client comes from. The client will be authenticated if the client's MAC address (regardless of the VLAN) is not authenticated.

multi_authen_methods - Specifies the method for compound authentication.

none - Specifies that compound authentication is not enabled.

any - Specifies if any of the authentication methods (802.1X, MAC, and WAC) pass, then pass.

dot1x_impb - Dot1x will be verified first, and then IMPB will be verified. Both authentications need to be passed.

impb_wac - WAC will be verified first, and then IMPB will be verified. Both authentications need to be passed.

mac_impb - MAC will be verified first, and then IMPB will be verified. Both authentications need to be passed.

mac_wac - MAC will be verified first, and then WAC will be verified. Both authentications need to be passed.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

The following example sets the authentication mode of all ports to host-based:

```
DGS-3000-28XMP:admin#config authentication ports all auth_mode host_based
Command: config authentication ports all auth_mode host_based

Success.

DGS-3000-28XMP:admin#
```

The following example sets the compound authentication method of all ports to “any”:

```
DGS-3000-28XMP:admin#config authentication ports all multi_authen_methods any

Command: config authentication ports all multi_authen_methods any

Success.

DGS-3000-28XMP:admin#
```

17-7 config authentication server failover

Description

This command is used to configure the failover authentication of the authentication server.

Format

config authentication server failover [local | permit | block]

Parameters

local - Specifies to use local DB to authenticate the client.

permit - Specifies that the client is always regarded as authenticated.

block - Specifies to block the client. This is the default.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the failover authentication state:

```
DGS-3000-28XMP:admin# config authentication server failover local
Command: config authentication server failover local

Success.

DGS-3000-28XMP:admin#
```

17-8 show authorization

Description

This command is used to display authorization status.

Format

show authorization

Parameters

None.

Restrictions

None.

Example

This example displays authorization status:

```
DGS-3000-28XMP:admin# show authorization
Command: show authorization

Authorization for Attributes: Enabled.

DGS-3000-28XMP:admin#
```

17-9 show authentication

Description

This command is used to display authentication global configuration.

Format

show authentication

Parameters

None.

Restrictions

None.

Example

To show authentication global configuration:

```
DGS-3000-28XMP:admin# show authentication
Command: show authentication

Authentication Server Failover: Local.

DGS-3000-28XMP:admin#
```

17-10 show authentication guest_vlan

Description

This command is used to display guest VLAN information.

Format

show authentication guest_vlan

Parameters

None.

Restrictions

None.

Example

To display the guest VLAN setting:

```
DGS-3000-28XMP:admin#show authentication guest_vlan
Command: show authentication guest_vlan


Guest VLAN VID         : 2
Guest VLAN Member Ports: 1-28

 Total Entries: 1


DGS-3000-28XMP:admin#
```

17-11 show authentication ports

Description

This command is used to display the authentication method and authorization mode on ports.

Format

show authentication ports {<portlist>}

Parameters

<portlist> - (Optional) Enter to display compound authentication on specific port(s).

Restrictions

None.

Example

To display the authentication settings for ports 1 to 3:

```
DGS-3000-28XMP:admin#show authentication ports 1-3
Command: show authentication ports 1-3

 Port  Methods        Auth Mode
 ---- -------------- -----------
 1    Any            Host-based
 2    Any            Host-based
 3    Any            Host-based

DGS-3000-28XMP:admin#
```

Chapter 18 Configuration Command List

show config [effective | modified | current_config | boot_up | file <pathname 64>] {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}} {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}} {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}}}}}
config configuration <pathname 64> [boot_up | active]
save {[config <pathname 64> | log | all]}
show boot_file

18-1 show config

Description

This command is used to display the content of the current configuration, the configuration to be used in next boot, or the configuration file specified by the command.

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

include: includes lines that contain the specified filter string.

exclude: excludes lines that contain the specified filter string

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

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

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

Format

show config [effective | modified | current_config | boot_up | file <pathname 64>] {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}} {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}} {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}}}}}

Parameters

effective - Specifies to only display the commands which affects the behavior of the device. For example, if STP is disabled, then for STP configuration, only “STP is disabled” is displayed. All other lower level settings regarding STP are not displayed. The lower level setting will only be displayed when the higher level setting is enabled. Note that this parameter is only for the current configuration.
modified - Specifies to only display the commands which are not default settings. Note that this parameter is only for the current configuration.
current_config - Specifies the current configuration.
boot_up - Specifies the list of the bootup configuration.

file - Specifies to display the configuration file.

<pathname 64> - Enter an absolute pathname on the device file system. This name can be up to 64 characters long.

include - (Optional) Specifies to include lines that contain the specified filter string.

exclude - (Optional) Specifies to exclude lines that contain the specified filter string.

begin - (Optional) Specifies the first line that contains the specified filter string will be the first line of the output.

<filter_string 80> - Enter a filter string that is enclosed by the symbol ". Thus, the filter string itself cannot contain the “ character. The filter string is case sensitive. This value can be up to 80 characters long.

<filter_string 80> - (Optional) Enter a filter string that is enclosed by the symbol ". Thus, the filter string itself cannot contain the “ character. The filter string is case sensitive. This value can be up to 80 characters long.

<filter_string 80> - (Optional) Enter a filter string that is enclosed by the symbol ". Thus, the filter string itself cannot contain the “ character. The filter string is case sensitive. This value can be up to 80 characters long.

include - (Optional) Specifies to include lines that contain the specified filter string.

exclude - (Optional) Specifies to exclude lines that contain the specified filter string.

begin - (Optional) Specifies the first line that contains the specified filter string will be the first line of the output.

<filter_string 80> - Enter a filter string that is enclosed by the symbol ". Thus, the filter string itself cannot contain the “ character. The filter string is case sensitive. This value can be up to 80 characters long.

<filter_string 80> - (Optional) Enter a filter string that is enclosed by the symbol ". Thus, the filter string itself cannot contain the “ character. The filter string is case sensitive. This value can be up to 80 characters long.

<filter_string 80> - (Optional) Enter a filter string that is enclosed by the symbol ". Thus, the filter string itself cannot contain the “ character. The filter string is case sensitive. This value can be up to 80 characters long.

include - (Optional) Specifies to include lines that contain the specified filter string.

exclude - (Optional) Specifies to exclude lines that contain the specified filter string.

begin - (Optional) Specifies the first line that contains the specified filter string will be the first line of the output.

<filter_string 80> - Enter a filter string that is enclosed by the symbol ". Thus, the filter string itself cannot contain the “ character. The filter string is case sensitive. This value can be up to 80 characters long.

<filter_string 80> - (Optional) Enter a filter string that is enclosed by the symbol ". Thus, the filter string itself cannot contain the “ character. The filter string is case sensitive. This value can be up to 80 characters long.

<filter_string 80> - (Optional) Enter a filter string that is enclosed by the symbol ". Thus, the filter string itself cannot contain the “ character. The filter string is case sensitive.

Restrictions

Only Administrators can issue this command.

Example

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

```
DGS-3000-28XMP:admin#show config modified
Command: show config modified

#------------------------------------------------------------------------
#                    DGS-3000-28XMP Gigabit Ethernet Switch
#                                Configuration
#
#                           Firmware: Build 4.00.010
#           Copyright(C) 2018 D-Link Corporation. All rights reserved.
#------------------------------------------------------------------------


# DEVICE


# DDP


# BASIC

# ACCOUNT LIST
# ACCOUNT END

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

18-2 config configuration

Description

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

Format

config configuration <pathname 64> [boot_up | active]

Parameters

<pathname 64> - Specifies a configuration file on the device file system.
boot_up - Specifies it as a boot up file.
active - Specifies to apply the configuration.

Restrictions

Only Administrators can issue this command.

Example

To configure the Switch’s configuration file as boot up:

```
DGS-3000-28XMP:admin# config configuration config.cfg boot_up
Command: config configuration config.cfg boot_up

Success.
DGS-3000-28XMP:admin#
```

18-3 save

Description

This command is used to save the current configuration to a file.

Format

save {[config <pathname 64> | log | all]}

Parameters

config - (Optional) Specifies to save the configuration to a file. **<pathname64>** - Enter the absolute pathname on the device file system. If pathname is not specified, it refers to the boot up configuration file.	
log - (Optional) Specifies to save the log.	
all - (Optional) Specifies to save the configuration and the log.	

Restrictions

Only Administrators and Operators can issue this command.

Example

To save the configuration:

```
DGS-3000-28XMP:admin# save config c:/3200.cfg
Command: save config c:/3200.cfg

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

DGS-3000-28XMP:admin#
```

18-4 show boot file

Description

This command is used to display the configuration file and firmware image assigned as boot-up files.

Format

show boot_file

Parameters

None.

Restrictions

None.

Example

To display the boot file:

```
DGS-3000-28XMP:admin# show boot_file
Command: show boot_file

  Bootup Firmware       : /c:/runtime.had
  Bootup Configuration  : /c:/config.cfg

DGS-3000-28XMP:admin#
```

Chapter 19 Connectivity Fault Management (CFM) Command List

create cfm md <string 22> {md_index <uint 1-4294967295>} level <int 0-7>
config cfm md [<string 22> | md_index <uint 1-4294967295>] {mip [none | auto | explicit] | sender_id [none | chassis | manage | chassis_manage]}
create cfm ma <string 22> {ma_index <uint 1-4294967295>} md [<string 22> | md_index <uint 1-4294967295>]
config cfm ma [<string 22> | ma_index <uint 1-4294967295>] md [<string 22> | md_index <uint 1-4294967295>] {vlanid <vlanid 1-4094> | mip [none | auto | explicit | defer] | sender_id [none | chassis | manage | chassis_manage | defer] | ccm_interval [10ms | 100ms | 1sec | 10sec | 1min | 10min] | mepid_list [add | delete] <mepid_list>}
create cfm mep <string 32> mepid <int 1-8191> md [<string 22> | md_index <uint 1-4294967295>] ma [<string 22> | ma_index <uint 1-4294967295>] direction [inward | outward] port <port>
config cfm mep [mepname <string 32> | mepid <int 1-8191> md [<string 22> | md_index <uint 1-4294967295>] ma [<string 22> | ma_index <uint 1-4294967295>]] {state [enable | disable] | ccm [enable | disable] | pdu_priority <int 0-7> | fault_alarm [all | mac_status | remote_ccm | error_ccm | xcon_ccm | none] | alarm_time <centisecond 250 -1000> | alarm_reset_time <centisecond 250-1000>}
delete cfm mep [mepname <string 32> | mepid <int 1-8191> md [<string 22> | md_index <uint 1-4294967295>] ma [<string 22> | ma_index <uint 1-4294967295>]]
delete cfm ma [<string 22> | ma_index <uint 1-4294967295>] md [<string 22> | md_index <uint 1-4294967295>]
delete cfm md [<string 22> | md_index <uint 1-4294967295>]
enable cfm
disable cfm
config cfm ports <portlist> state [enable | disable]
show cfm ports <portlist>
show cfm {[md [<string 22> | md_index <uint 1-4294967295>] {ma [<string 22> | ma_index <uint 1-4294967295>] {mepid <int 1-8191>}} | mepname <string 32>]}
show cfm fault {md [<string 22> | md_index <uint 1-4294967295>] {ma [<string 22> | ma_index <uint 1-4294967295>]}}
show cfm port <port> {level <int 0-7> | direction [inward | outward] | vlanid <vlanid 1-4094>}
cfm loopback <macaddr> [mepname <string 32> | mepid <int 1-8191> md [<string 22> | md_index <uint 1-4294967295>] ma [<string 22> | ma_index <uint 1-4294967295>]] {num <int 1-65535> | [length <int 0-1500> | pattern <string 1500>] | pdu_priority <int 0-7>}
cfm linktrace <macaddr> [mepname <string 32> | mepid <int 1-8191> md [<string 22> | md_index <uint 1-4294967295>] ma [<string 22> | ma_index <uint 1-4294967295>]] {ttl <int 2-255> | pdu_priority <int 0-7>}
show cfm linktrace [mepname <string 32> | mepid <int 1-8191> md [<string 22> | md_index <uint 1-4294967295>] ma [<string 22> | ma_index <uint 1-4294967295>]] {trans_id <uint>}
delete cfm linktrace {[md [<string 22> | md_index <uint 1-4294967295>] {ma [<string 22> | ma_index <uint 1-4294967295>] {mepid <int 1-8191>}} | mepname <string 32>]}
show cfm mipccm
config cfm mp_ltr_all [enable | disable]
show cfm mp_ltr_all
show cfm remote_mep [mepname <string 32> | md [<string 22> | md_index <uint 1-4294967295>] ma [<string 22> | ma_index <uint 1-4294967295>] mepid <int 1-8191>] remote_mepid <int 1-8191>
show cfm pkt_cnt {[ports <portlist> {[rx | tx]} | [rx | tx] | ccm]}

clear cfm pkt_cnt {[ports <portlist> {[rx | tx]} | [rx | tx] | ccm]}

19-1 create cfm md

Description

This command is used to create a maintenance domain.

Format

create cfm md <string 22> {md_index <uint 1-4294967295>} level <int 0-7>

Parameters

<string 22> - Enter the maintenance domain name. This name can be up to 22 characters long.
md_index - (Optional) Specifies the maintenance domain index. **<uint 1-4294967295>** - Enter the maintenance domain index value here. This value must be between 1 and 4294967295.
level - Specifies the maintenance domain level. **<int 0-7>** - Enter the maintenance domain level here. This value must be between 0 and 7.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To create a maintenance domain called “op_domain” and assign a maintenance domain level of “2”:

```
DGS-3000-28XMP:admin# create cfm md op_domain level 2
Command: create cfm md op_domain level 2

Success.

DGS-3000-28XMP:admin#
```

19-2 config cfm md

Description

This command is used to configure the parameters of a maintenance domain. The creation of MIPs on an MA is useful to trace the link, MIP by MIP. It also allows the user to perform a loopback from an MEP to an MIP.

Format

config cfm md [<string 22> | md_index <uint 1-4294967295>] {mip [none | auto | explicit] | sender_id [none | chassis | manage | chassis_manage]}

Parameters

<string 22> - Enter the maintenance domain name. This name can be up to 22 characters long.

md_index - Specifies the maintenance domain index.

<uint 1-4294967295> - Enter the maintenance domain index value here. This value must be between 1 and 4294967295.

mip - (Optional) Specifies the MIP creation policy.

none - Specifies not to create MIPs. This is the default value.

auto - Specifies that MIPs can always be created on any ports in this MD, if that port is not configured with an MEP of this MD. For the intermediate switch in an MA, the setting must be automatic in order for the MIPs to be created on this device.

explicit - Specifies that MIPs can be created on any ports in this MD, only if the next existent lower level has an MEP configured on that port, and that port is not configured with an MEP of this MD.

sender_id - (Optional) Specifies the control transmission of the sender ID TLV.

none - Specifies not to transmit the sender ID TLV. This is the default value.

chassis - Specifies to transmit the sender ID TLV with the chassis ID information.

manage - Specifies to transmit the sender ID TLV with the managed address information.

chassis_manage - Specifies to transmit sender ID TLV with chassis ID information and manage address information.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the maintenance domain called “op_domain” and specify the explicit option for creating MIPs:

```
DGS-3000-28XMP:admin# config cfm md op_domain mip explicit
Command: config cfm md op_domain mip explicit

Success.

DGS-3000-28XMP:admin#
```

19-3 create cfm ma

Description

This command is used to create a maintenance association. Different MAs in an MD must have different MA names. Different MAs in different MDs may have the same MA Name.

Format

create cfm ma <string 22> {ma_index <uint 1-4294967295>} md [<string 22> | md_index <uint 1-4294967295>]

Parameters

<string 22> - Enter the maintenance association name. This name can be up to 22 characters long.

ma_index - (Optional) Specifies the maintenance association index.

<uint 1-4294967295> - Enter the maintenance association index value here. This value must be between 1

and 4294967295.

md - Specifies the maintenance domain name.

<string 22> - Enter the maintenance domain name here. This name can be up to 22 characters long.

md_index - Specifies the maintenance domain index.

<uint 1-4294967295> - Enter the maintenance domain index value here. This value must be between 1 and 4294967295.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To create a maintenance association called “op1” and assign it to the maintenance domain “op_domain”:

```
DGS-3000-28XMP:admin# create cfm ma op1 md op_domain
Command: create cfm ma op1 md op_domain

Success.

DGS-3000-28XMP:admin#
```

19-4 config cfm ma

Description

This command is used to configure the parameters of a maintenance association. The MEP list specified for an MA can be located in different devices. MEPs must be created on the ports of these devices explicitly. An MEP will transmit a CCM packet periodically across the MA. The receiving MEP will verify these received CCM packets from the other MEPs against this MEP list for the configuration integrity check.

Format

config cfm ma [<string 22> | ma_index <uint 1-4294967295>] md [<string 22> | md_index <uint 1-4294967295>] {vlanid <vlanid 1-4094> | mip [none | auto | explicit | defer] | sender_id [none | chassis | manage | chassis_manage | defer] | ccm_interval [10ms | 100ms | 1sec | 10sec | 1min | 10min] | mepid_list [add | delete] <mepid_list>}

Parameters

<string 22> - Enter the maintenance association name. This name can be up to 22 characters long.

ma_index - Specifies the maintenance association index.

<uint 1-4294967295> - Enter the maintenance association index value here. This value must be between 1 and 4294967295.

md - Specifies the maintenance domain name.

<string 22> - Enter the maintenance domain name here. This name can be up to 22 characters long.

md_index - Specifies the maintenance domain index.

<uint 1-4294967295> - Enter the maintenance domain index value here. This value must be between 1 and 4294967295.

vlanid - (Optional) Specifies the VLAN Identifier. Different MAs must be associated with different VLANs.

<vlanid 1-4094> - Enter the VLAN ID used here. This value must be between 1 and 4094.

mip - (Optional) Specifies the MIP creation policy.

none - Specifies not to create MIPs.

auto - Specifies that MIPs can always be created on any ports in this MA, if that port is not configured with an MEP of that MA.

explicit - Specifies that MIP can be created on any ports in this MA, only if the next existing lower level has an MEP configured on that port, and that port is not configured with an MEP of this MA.

defer - Specifies to inherit the setting configured for the maintenance domain that this MA is associated with. This is the default value.

sender_id - (Optional) Specifies the control transmission of the sender ID TLV.

none - Specifies not to transmit the sender ID TLV. This is the default value.

chassis - Specifies to transmit the sender ID TLV with the chassis ID information.

manage - Specifies to transmit the sender ID TLV with the manage address information.

chassis_manage - Specifies to transmit the sender ID TLV with the chassis ID information and the manage address information.

defer - Specifies to inherit the setting configured for the maintenance domain that this MA is associated with. This is the default value.

ccm_interval - (Optional) Specifies the CCM interval.

10ms - Specifies that the CCM interval will be set to 10 milliseconds. Not recommended.

100ms - Specifies that the CCM interval will be set to 100 milliseconds. Not recommended.

1sec - Specifies that the CCM interval will be set to 1 second.

10sec - Specifies that the CCM interval will be set to 10 seconds. This is the default value.

1min - Specifies that the CCM interval will be set to 1 minute.

10min - Specifies that the CCM interval will be set to 10 minutes.

mepid_list - (Optional) Specifies the MEPIDs contained in the maintenance association. The range of the MEPID is 1-8191.

add - Specifies to add MEPID(s).

delete - Specifies to delete MEPID(s). By default, there is no MEPID in a newly created maintenance association.

<mepid_list> - Enter the MEP ID list here.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure a CFM MA:

```
DGS-3000-28XMP:admin# config cfm ma op1 md op_domain vlanid 1 ccm_interval 1sec
Command: config cfm ma op1 md op_domain vlanid 1 ccm_interval 1sec

Success.

DGS-3000-28XMP:admin#
```

19-5 create cfm mep

Description

This command is used to create an MEP. Different MEPs in the same MA must have a different MEPID. MD name, MA name, and MEPID together identify an MEP.

Different MEPs on the same device must have a different MEP name. Before creating an MEP, its MEPID should be configured in the MA's MEPID list.

Format

create cfm mep <string 32> mepid <int 1-8191> md [<string 22> | md_index <uint 1-4294967295>] ma [<string 22> | ma_index <uint 1-4294967295>] direction [inward | outward] port <port>

Parameters

<string 32> - Enter the MEP name used. It is unique among all MEPs configured on the device. This name can be up to 32 characters long.
mepid - Specifies the MEP ID. It should be configured in the MA's MEPID list. **<int 1-8191>** - Enter the MEP ID used here. This value must be between 1 and 8191.
md - Specifies the maintenance domain name. **<string 22>** - Enter the maintenance domain name used here. This name can be up to 22 characters long. **md_index** - Specifies the maintenance domain index. **<uint 1-4294967295>** - Enter the maintenance domain index value here. This value must be between 1 and 4294967295.
ma - Specifies the maintenance association name. **<string 22>** - Enter the maintenance association name used here. This name can be up to 22 characters long. **ma_index** - Specifies the maintenance association index. **<uint 1-4294967295>** - Enter the maintenance association index value here. This value must be between 1 and 4294967295.
direction - Specifies the MEP direction. **inward** - Specifies the inward facing (up) MEP. **outward** - Specifies the outward facing (down) MEP.
port - Specifies the port number. This port should be a member of the MA's associated VLAN. **<port>** - Enter the port number used here.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To create a CFM MEP:

```
DGS-3000-28XMP:admin# create cfm mep mep1 mepid 1 md op_domain ma op1 direction inward port 2
Command: create cfm mep mep1 mepid 1 md op_domain ma op1 direction inward port 2

Success.

DGS-3000-28XMP:admin#
```

19-6 config cfm mep

Description

This command is used to configure the parameters of an MEP.

An MEP may generate 5 types of Fault Alarms, as shown below by their priorities from high to low:

- Cross-connect CCM Received: priority 5
- Error CCM Received: priority 4

- Some Remote MEPs Down: priority 3
- Some Remote MEP MAC Status Errors: priority 2
- Some Remote MEP Defect Indications: priority 1

If multiple types of the fault occur on an MEP, only the fault with the highest priority will be alarmed.

Format

config cfm mep [mepname <string 32> | mepid <int 1-8191> md [<string 22> | md_index <uint 1-4294967295>] ma [<string 22> | ma_index <uint 1-4294967295>]] {state [enable | disable] | ccm [enable | disable] | pdu_priority <int 0-7> | fault_alarm [all | mac_status | remote_ccm | error_ccm | xcon_ccm | none] | alarm_time <centisecond 250 -1000> | alarm_reset_time <centisecond 250-1000>}

Parameters

mepname - Specifies the MEP name.
- **<string 32>** - Enter the MEP name used here. This name can be up to 32 characters long.

mepid - Specifies the MEP ID.
- **<int 1-8191>** - Enter the MEP ID used here. This value must be between 1 and 8191.
- **md** - Specifies the maintenance domain name.
  - **<string 22>** - Enter the maintenance domain name used here. This name can be up to 22 characters long.
  - **md_index** - Specifies the maintenance domain index.
    - **<uint 1-4294967295>** - Enter the maintenance domain index value here. This value must be between 1 and 4294967295.
- **ma** - Specifies the maintenance association name.
  - **<string 22>** - Enter the maintenance association name used here. This name can be up to 22 characters long.
  - **ma_index** - Specifies the maintenance association index.
    - **<uint 1-4294967295>** - Enter the maintenance association index value here. This value must be between 1 and 4294967295.

state - (Optional) Specifies the MEP administrative state.
- **enable** - Specifies that the MEP will be enabled.
- **disable** - Specifies that the MEP will be disabled. This is the default value.

ccm - (Optional) Specifies the CCM transmission state.
- **enable** - Specifies that the CCM transmission will be enabled.
- **disable** - Specifies that the CCM transmission will be disabled. This is the default value.

pdu_priority - (Optional) Specifies that the 802.1p priority is set in the CCMs and the Linktrace Messages (LTMs) messages transmitted by the MEP. The default value is 7.
- **<int 0-7>** - Enter the PDU priority value here. This value must be between 0 and 7.

fault_alarm - (Optional) Specifies the control types of the fault alarms sent by the MEP.
- **all** - Specifies that all types of fault alarms will be sent.
- **mac_status** - Specifies that only the fault alarms whose priority is equal to or higher than “Some Remote MEP MAC Status Errors” are sent.
- **remote_ccm** - Specifies that only the fault alarms whose priority is equal to or higher than “Some Remote MEPs Down” are sent.
- **error_ccm** - Specifies that only the fault alarms whose priority is equal to or higher than “Error CCM Received” are sent.
- **xcon_ccm** - Specifies that only the fault alarms whose priority is equal to or higher than “Cross-connect CCM Received” are sent.
- **none** - Specifies that no fault alarm is sent. This is the default value.

alarm_time - (Optional) Specifies the time that a defect must exceed before the fault alarm can be sent. The unit is centisecond. The default value is 250.

<centisecond 250-1000> - Enter the alarm time value here. This value must be between 250 and 1000 centiseconds.

alarm_reset_time - (Optional) Specifies the dormant duration time before a defect is triggered before the fault can be re-alarmed. The unit is centisecond. The default value is 1000.

<centisecond 250-1000> - Enter the alarm reset time value here. This value must be between 250 and 1000 centiseconds.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure a CFM MEP:

```
DGS-3000-28XMP:admin# config cfm mep mepname mep1 state enable ccm enable
Command: config cfm mep mepname mep1 state enable ccm enable

Success.

DGS-3000-28XMP:admin#
```

19-7 delete cfm mep

Description

This command is used to delete a previously created MEP.

Format

delete cfm mep [mepname <string 32> | mepid <int 1-8191> md [<string 22> | md_index <uint 1-4294967295>] ma [<string 22> | ma_index <uint 1-4294967295>]]

Parameters

mepname - Specifies the MEP name.

<string 32> - Enter the MEP name used here. This name can be up to 32 characters long.

mepid - Specifies the MEP ID.

<int 1-8191> - Enter the MEP ID used here. This value must be between 1 and 8191.

md - Specifies the maintenance domain name.

<string 22> - Enter the maintenance domain name used here. This name can be up to 22 characters long.

md_index - Specifies the maintenance domain index.

<uint 1-4294967295> - Enter the maintenance domain index value here. This value must be between 1 and 4294967295.

ma - Specifies the maintenance association name.

<string 22> - Enter the maintenance association name used here. This name can be up to 22 characters long.

ma_index - Specifies the maintenance association index.

<uint 1-4294967295> - Enter the maintenance association index value here. This value must be between 1 and 4294967295.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete a CFM MEP:

```
DGS-3000-28XMP:admin# delete cfm mep mepname mep1
Command: delete cfm mep mepname mep1

Success.

DGS-3000-28XMP:admin#
```

19-8 delete cfm ma

Description

This command is used to delete a created maintenance association. All MEPs created in the maintenance association will be deleted automatically.

Format

delete cfm ma [<string 22> | ma_index <uint 1-4294967295>] md [<string 22> | md_index <uint 1-4294967295>]

Parameters

<string 22> - Enter the maintenance association name. This name can be up to 22 characters long.
ma_index - Specifies the maintenance association index. **<uint 1-4294967295>** - Enter the maintenance association index value here. This value must be between 1 and 4294967295.
md - Specifies the maintenance domain name. **<string 22>** - Enter the maintenance domain name used here. This name can be up to 22 characters long. **md_index** - Specifies the maintenance domain index. **<uint 1-4294967295>** - Enter the maintenance domain index value here. This value must be between 1 and 4294967295.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete a CFM MA:

```
DGS-3000-28XMP:admin# delete cfm ma op1 md op_domain
Command: delete cfm ma op1 md op_domain

Success.

DGS-3000-28XMP:admin#
```

19-9 delete cfm md

Description

This command is used to delete a previously created maintenance domain. All the MEPs and maintenance associations created in the maintenance domain will be deleted automatically.

Format

delete cfm md [<string 22> | md_index <uint 1-4294967295>]

Parameters

<string 22> - Enter the maintenance domain name. This name can be up to 22 characters long.
md_index - Specifies the maintenance domain index. **<uint 1-4294967295>** - Enter the maintenance domain index value here. This value must be between 1 and 4294967295.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete a CFM MD:

```
DGS-3000-28XMP:admin# delete cfm md op_domain
Command: delete cfm md op_domain

Success.

DGS-3000-28XMP:admin#
```

19-10 enable cfm

Description

This command is used to enable the CFM globally.

Format

enable cfm

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable the CFM globally:

```
DGS-3000-28XMP:admin# enable cfm
Command: enable cfm

Success.

DGS-3000-28XMP:admin#
```

19-11 disable cfm

Description

This command is used to disable the CFM globally.

Format

disable cfm

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To disable the CFM globally:

```
DGS-3000-28XMP:admin# disable cfm
Command: disable cfm

Success.

DGS-3000-28XMP:admin#
```

19-12 config cfm ports

Description

This command is used to enable or disable the CFM function on a per-port basis. By default, the CFM function is disabled on all ports.

If the CFM is disabled on a port:

1. MIPs are never created on that port.
2. MEPs can still be created on that port, and the configuration can be saved.
3. MEPs created on that port can never generate or process CFM PDUs. If the user issues a Loopback or Linktrace test on those MEPs, it will prompt the user to inform them that the CFM function is disabled on that port.

Format

config cfm ports <portlist> state [enable | disable]

Parameters

<portlist> - Enter the list of ports used for this configuration.
state - Specifies that the CFM function will be enabled or disabled. **enable** - Specifies that the CFM function will be enabled. **disable** - Specifies that the CFM function will be disabled.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the CFM ports:

```
DGS-3000-28XMP:admin# config cfm ports 2-5 state enable
Command: config cfm ports 2-5 state enable

Success.

DGS-3000-28XMP:admin#
```

19-13 show cfm ports

Description

This command is used to show the CFM state of specified ports.

Format

show cfm ports <portlist>

Parameters

<portlist> - Enter the list of logical ports.

Restrictions

None.

Example

To show the CFM ports:

```
DGS-3000-28XMP:admin# show cfm ports 3-6
Command: show cfm ports 3-6

Port   State
-----  --------
3      Enabled
4      Enabled
5      Enabled
6      Disabled

DGS-3000-28XMP:admin#
```

19-14 show cfm port

Description

This command is used to show MEPs and MIPs created on a port.

Format

show cfm port <port> {level <int 0-7> | direction [inward | outward] | vlanid <vlanid 1-4094>}

Parameters

<port> - Enter the port number used here.
level - (Optional) Specifies the MD Level. If not specified, all levels are shown. **<int 0-7>** - Enter the MD level value here. This value must be between 0 and 7.
direction - (Optional) Specifies the MEP direction. If not specified, both directions and the MIP are shown. **inward** - Specifies that the MEP direction will be inward facing. **outward** - Specifies that the MEP direction will be outward facing.
vlanid - (Optional) Specifies the VLAN identifier. If not specified, all VLANs are shown. **<vlanid 1-4094>** - Enter the VLAN ID used here. This value must be between 1 and 4094.

Restrictions

None.

Example

To show the MEPs and MIPs created on a port:

```
DGS-3000-28XMP:admin# show cfm port 2
Command: show cfm port 2

MAC Address: 00-01-02-03-04-02
MD Name      MA Name      MEPID  Level  Direction  VID
-----------  -----------  -----  -----  ---------  ----
op_domain    op1          1      2      Inward     1

DGS-3000-28XMP:admin#
```

19-15 cfm linktrace

Description

This command is used to issue a CFM link track message.

Format

cfm linktrace <macaddr> [mepname <string 32> | mepid <int 1-8191> md [<string 22> | md_index <uint 1-4294967295>] ma [<string 22> | ma_index <uint 1-4294967295>]] {ttl <int 2-255> | pdu_priority <int 0-7>}

Parameters

<macaddr> - Specifies the destination MAC address.

mepname - Specifies the MEP name used.
- **<string 32>** - Enter the MEP name used here. This name can be up to 32 characters long.

mepid - Specifies the MEP ID used.
- **<int 1-8191>** - Enter the MEP ID used here. This value must be between 1 and 8191.
- **md** - Specifies the maintenance domain name.
  - **<string 22>** - Enter the maintenance domain name here. This name can be up to 22 characters long.
  - **md_index** - Specifies the maintenance domain index.
    - **<uint 1-4294967295>** - Enter the maintenance domain index value here. This value can be between 1 and 4294967295.
- **ma** - Specifies the maintenance association name.
  - **<string 22>** - Enter the maintenance association name here. This name can be up to 22 characters long.
  - **ma_index** - Specifies the maintenance association index.
    - **<uint 1-4294967295>** - Enter the maintenance association index value here. This value can be between 1 and 4294967295.

ttl - (Optional) Specifies the LTM TTL value. The default value is 64.
- **<int 2-255>** - Enter the LTM TTL value here. This value must be between 2 and 255.

pdu_priority - (Optional) Specifies the 802.1p priority to be set in the transmitted LTM. If not specified, it uses the same priority as CCMs sent by the MA.
- **<int 0-7>** - Enter the PDU priority value here. This value must be between 0 and 7.

Restrictions

None.

Example

To transmit an LTM:

```
DGS-3000-28XMP:admin# cfm linktrace 00-01-02-03-04-05 mepname mep1
Command: cfm linktrace 00-01-02-03-04-05 mepname mep1

Transaction ID: 26
Success.

DGS-3000-28XMP:admin#
```

19-16 show cfm linktrace

Description

This command is used to display Linktrace Reply (LTR) information. The maximum LTRs allowed on the Switch is 128.

Format

show cfm linktrace [mepname <string 32> | mepid <int 1-8191> md [<string 22> | md_index <uint 1-4294967295>] ma [<string 22> | ma_index <uint 1-4294967295>]] {trans_id <uint>}

Parameters

mepname - Specifies the MEP name used.
- **<string 32>** - Enter the MEP name used here. This name can be up to 32 characters long.

mepid - Specifies the MEP ID used.
- **<int 1-8191>** - Enter the MEP ID used here. This value must be between 1 and 8191.
- **md** - Specifies the maintenance domain name.
  - **<string 22>** - Enter the maintenance domain name here. This name can be up to 22 characters long.
  - **md_index** - Specifies the maintenance domain index.
    - **<uint 1-4294967295>** - Enter the maintenance domain index value here. This value must between 1 and 4294967295.
- **ma** - Specifies the maintenance association name.
  - **<string 22>** - Enter the maintenance association name here. This name can be up to 22 characters long.
  - **ma_index** - Specifies the maintenance association index.
    - **<uint 1-4294967295>** - Enter the maintenance association index value here. This value must between 1 and 4294967295.

trans_id - (Optional) Specifies the identifier of the transaction displayed.
- **<uint>** - Enter the transaction ID used here.

Restrictions

None.

Example

To display the LTR when the **config cfm mp_ltr_all** command is enabled:

```
DGS-3000-28XMP:admin# show cfm linktrace mepname mep1 trans_id 26
Command: show cfm linktrace mepname mep1 trans_id 26

Transaction ID: 26
From MEP mep1 to 32-00-70-89-31-06
Start Time    : 2011-11-22 16:05:08

Hop  MEPID  Ingress MAC Address  Egress MAC Address   Forwarded  Relay Action
---  -----  ------------------  ------------------  ---------  ------------
1    -      00-00-00-00-00-00    32-00-70-89-41-06    Yes        FDB
2    -      00-32-28-40-09-07    00-32-28-40-09-05    Yes        FDB
3    2      00-00-00-00-00-00    32-00-70-89-31-06    No         Hit

DGS-3000-28XMP:admin# ”
```

To show the LTR when the **config cfm mp_ltr_all** command is disabled:

```
DGS-3000-28XMP:admin# show cfm linktrace mepname mep1 trans_id 27
Command: show cfm linktrace mepname mep1 trans_id 27

Transaction ID: 27
From MEP mep1 to 32-00-70-89-31-06
Start Time    : 2011-11-22 16:28:56

Hop  MEPID  Ingress MAC Address  Egress MAC Address   Forwarded  Relay Action
---  -----  ------------------  ------------------  ---------  ------------
1    -      00-00-00-00-00-00    32-00-70-89-41-06    Yes        FDB
2    -      00-32-28-40-09-07    00-32-28-40-09-05    Yes        FDB
3    2      00-00-00-00-00-00    32-00-70-89-31-06    No         Hit

DGS-3000-28XMP:admin# ”
```

19-17 delete cfm linktrace

Description

This command is used to delete the stored LTR data that have been initiated by the specified MEP.

Format

delete cfm linktrace {[md [<string 22> | md_index <uint 1-4294967295>] {ma [<string 22> | ma_index <uint 1-4294967295>] {mepid <int 1-8191>}} | mepname <string 32>]}

Parameters

md - (Optional) Specifies the maintenance domain name.

<string 22> - Enter the maintenance domain name here. This name can be up to 22 characters long.

md_index - Specifies the maintenance domain index.

<uint 1-4294967295> - Enter the maintenance domain index value here. This value must be between 1 and 4294967295.

ma - (Optional) Specifies the maintenance association name.

<string 22> - Enter the maintenance association name here. This name can be up to 22 characters long.

ma_index - Specifies the maintenance association index.

<uint 1-4294967295> - Enter the maintenance association index value here. This value must be between 1 and 4294967295.

mepid - (Optional) Specifies the MEP ID used.

<int 1-8191> - Enter the MEP ID used here. This value must be between 1 and 8191.

mepname - (Optional) Specifies the MEP name used.

<string 32> - Enter the MEP name used here. This name can be up to 32 characters long.

Restrictions

None.

Example

To delete the CFM LTR:

```
DGS-3000-28XMP:admin# delete cfm linktrace mepname mep1
Command: delete cfm linktrace mepname mep1

Success.

DGS-3000-28XMP:admin#
```

19-18 show cfm mipccm

Description

This command is used to show the MIP CCM database entries. All entries in the MIP CCM database will be shown. A MIP CCM entry is similar to a FDB which keeps the forwarding port information of a MAC entry.

Format

show cfm mipccm

Parameters

None.

Restrictions

None.

Example

To show MIP CCM database entries:

```
DGS-3000-28XMP:admin# show cfm mipccm
Command: show cfm mipccm

MA          VID   MAC Address        Port
----------  ----  -----------------  -----
opma        1     xx-xx-xx-xx-xx-xx  2
opma        1     xx-xx-xx-xx-xx-xx  3

Total: 2

DGS-3000-28XMP:admin#
```

19-19 config cfm mp_ltr_all

Description

This command is used to configure all MPs in the forwarding path of the LTM to reply with LTRs, whether they are on a Bridge or not. According to IEEE 802.1ag, a Bridge replies with one LTR to an LTM.

Format

config cfm mp_ltr_all [enable | disable]

Parameters

enable - Specifies to enable this feature.
disable - Specifies to disable this feature.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure all MPs in the forwarding path of the LTM to reply with LTRs, whether they are on a Bridge or not:

```
DGS-3000-28XMP:admin# config cfm mp_ltr_all enable
Command: config cfm mp_ltr_all enable

Success.

DGS-3000-28XMP:admin#
```

19-20 show cfm mp_ltr_all

Description

This command is used to show the current configuration of the "all MPs reply LTRs" function.

Format

show cfm mp_ltr_all

Parameters

None.

Restrictions

None.

Example

To show the configuration of the "all MPs reply LTRs" function:

```
DGS-3000-28XMP:admin# show cfm mp_ltr_all
Command: show cfm mp_ltr_all

All MPs reply LTRs: Disabled

DGS-3000-28XMP:admin#
```

19-21 show cfm remote_mep

Description

This command is used to show remote MEPs.

Format

show cfm remote_mep [mepname <string 32> | md [<string 22> | md_index <uint 1-4294967295>] ma [<string 22> | ma_index <uint 1-4294967295>] mepid <int 1-8191>] remote_mepid <int 1-8191>

Parameters

mepname - Specifies the MEP name used.
- **<string 32>** - Enter the MEP name used here. This name can be up to 32 characters long.

md Specifies the maintenance domain name.
- **<string 22>** - Enter the maintenance domain name here. This name can be up to 22 characters long.
- **md_index** - Specifies the maintenance domain index.
  - **<uint 1-4294967295>** - Enter the maintenance domain index value here. This value must between 1 and 4294967295.
- **ma** - Specifies the maintenance association name.
  - **<string 22>** - Enter the maintenance association name here. This name can be up to 22 characters long.
  - **ma_index** - Specifies the maintenance association index.
    - **<uint 1-4294967295>** - Enter the maintenance association index value here. This value must between 1 and 4294967295.
- **mepid** - Specifies the MEP ID used.
  - **<int 1-8191>** - Enter the MEP ID used here. This value must be between 1 and 8191.

remote_mepid - Specifies the Remote MEP ID used.
- **<int 1-8191>** - Enter the remote MEP ID used here. This value must be between 1 and 8191.

Restrictions

None.

Example

To show the CFM Remote MEP information:

```
DGS-3000-28XMP:admin# show cfm remote_mep mepname mep1 remote_mepid 2
Command: show cfm remote_mep mepname mep1 remote_mepid 2

Remote MEPID             : 2
MAC Address              : 00-11-22-33-44-02
Status                   : OK
RDI                      : Yes
Port State               : Blocked
Interface Status         : Down
Last CCM Serial Number   : 1000
Sender Chassis ID        : 00-11-22-33-44-00
Sender Management Address: SNMP-UDP-IPv4 10.90.90.90:161
Detect Time              : 2008-01-01 12:00:00

DGS-3000-28XMP:admin#
```

19-22 show cfm pkt_cnt

Description

This command is used to show the CFM packet's RX/TX counters.

Format

show cfm pkt_cnt {[ports <portlist> {[rx | tx]} | [rx | tx] | ccm]}

Parameters

ports - (Optional) Specifies the port counters to show. If not specified, all ports will be shown. **<portlist>** - Enter the list of ports used for this configuration here. **rx** - (Optional) Specifies to display the RX counter. **tx** - (Optional) Specifies to display the TX counter. If not specified, both of them will be shown.
rx - (Optional) Specifies to display the RX counter.
tx - (Optional) Specifies to display the TX counter. If not specified, both of them will be shown.
ccm - (Optional) Specifies the CCM RX counters.

Restrictions

None.

Example

To show the CFM packet's RX/TX counters:

```
DGS-3000-28XMP:admin# show cfm pkt_cnt
Command: show cfm pkt_cnt

CFM RX Statistics
-------------------------------------------------------------------------------
Port  AllPkt   CCM      LBR      LBM      LTR      LTM      VidDrop  OpcoDrop
----- -------- -------- -------- -------- -------- -------- -------- --------
all   2446     2434     0        9        0        3        0        0
1     2446     2434     0        9        0        3        0        0
2     0        0        0        0        0        0        0        0
3     0        0        0        0        0        0        0        0
4     0        0        0        0        0        0        0        0
5     0        0        0        0        0        0        0        0
6     0        0        0        0        0        0        0        0
7     0        0        0        0        0        0        0        0
8     0        0        0        0        0        0        0        0
9     0        0        0        0        0        0        0        0
10    0        0        0        0        0        0        0        0
11    0        0        0        0        0        0        0        0
12    0        0        0        0        0        0        0        0
13    0        0        0        0        0        0        0        0
14    0        0        0        0        0        0        0        0
15    0        0        0        0        0        0        0        0
16    0        0        0        0        0        0        0        0
17    0        0        0        0        0        0        0        0
18    0        0        0        0        0        0        0        0
19    0        0        0        0        0        0        0        0
20    0        0        0        0        0        0        0        0
21    0        0        0        0        0        0        0        0
22    0        0        0        0        0        0        0        0
23    0        0        0        0        0        0        0        0
24    0        0        0        0        0        0        0        0
25    0        0        0        0        0        0        0        0
26    0        0        0        0        0        0        0        0
27    0        0        0        0        0        0        0        0
28    0        0        0        0        0        0        0        0

CFM TX Statistics
-----------------------------------------------------------
Port  AllPkt   CCM      LBR      LBM      LTR      LTM
----- -------- -------- -------- -------- -------- --------
all   1974     1974     0        0        0        0
1     1974     1974     0        0        0        0
2     0        0        0        0        0        0
3     0        0        0        0        0        0
4     0        0        0        0        0        0
5     0        0        0        0        0        0
6     0        0        0        0        0        0
7     0        0        0        0        0        0
8     0        0        0        0        0        0
9     0        0        0        0        0        0
10    0        0        0        0        0        0
11    0        0        0        0        0        0
12    0        0        0        0        0        0
13    0        0        0        0        0        0
```

```
14    0         0         0         0         0         0
15    0         0         0         0         0         0
16    0         0         0         0         0         0
17    0         0         0         0         0         0
18    0         0         0         0         0         0
19    0         0         0         0         0         0
20    0         0         0         0         0         0
21    0         0         0         0         0         0
22    0         0         0         0         0         0
23    0         0         0         0         0         0
24    0         0         0         0         0         0
25    0         0         0         0         0         0
26    0         0         0         0         0         0
27    0         0         0         0         0         0
28    0         0         0         0         0         0

DGS-3000-28XMP:admin# show cfm pkt_cnt ccm
Command: show cfm pkt_cnt ccm

CCM RX counters:
XCON   = Cross-connect CCMs
Error  = Error CCMs
Normal = Normal CCMs

MEP Name    VID  Port  Level  Direction  XCON       Error      Normal
----------- ---- ----- ------ ---------- ---------- ---------- ----------
1           1    1     1      Inward     0          0          0
28mep       45   3     7      Inward     0          0          2438
                               ------------------------------------------
                               Total:     0          0          2438

DGS-3000-28XMP:admin#
```

19-23 clear cfm pkt_cnt

Description

This command is used to clear the CFM packet's RX/TX counters.

Format

clear cfm pkt_cnt {[ports <portlist> {[rx | tx]} | [rx | tx] | ccm]}

Parameters

ports - (Optional) The ports which require need the counters clearing. If not specified, all ports will be cleared. **<portlist>** - Enter the list of ports used for this configuration here. **rx** - (Optional) Specifies to clear the RX counter. **tx** - (Optional) Specifies to clear the TX counter. If not specified, both of them will be cleared.
rx - (Optional) Specifies to clear the RX counter.
tx - (Optional) Specifies to clear the TX counter. If not specified, both of them will be cleared.
ccm - (Optional) Specifies the CCM RX counters.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To clear the CFM packet's RX/TX counters:

```
DGS-3000-28XMP:admin# clear cfm pkt_cnt
Command: clear cfm pkt_cnt

Success.

DGS-3000-28XMP:admin# clear cfm pkt_cnt ccm
Command: clear cfm pkt_cnt ccm

Success.

DGS-3000-28XMP:admin#
```

Chapter 20 Connectivity Fault Management (CFM) Extension Command List

config cfm ais md [<string 22> | md_index <uint 1-4294967295>] ma [<string 22> | ma_index <uint 1-4294967295>] mepid <int 1-8191> {period [1sec | 1min] | level <int 0-7> | state [enable | disable]}(1)
config cfm lock md [<string 22> | md_index <uint 1-4294967295>] ma [<string 22> | ma_index <uint 1-4294967295>] mepid <int 1-8191> {period [1sec | 1min] | level <int 0-7> | state [enable | disable]}(1)
show cfm {[md [<string 22> | md_index <uint 1-4294967295>] {ma [<string 22> | ma_index <uint 1-4294967295>] {mepid <int 1-8191>}} | mepname <string 32>]}
show cfm fault {md [<string 22> | md_index <uint 1-4294967295>] {ma [<string 22> | ma_index <uint 1-4294967295>]}}
cfm lock md [<string 22> | md_index <uint 1-4294967295>] ma [<string 22> | ma_index <uint 1-4294967295>] mepid <int 1-8191> remote_mepid <int 1-8191> action [start | stop]
cfm loopback <macaddr> [mepname <string 32> | mepid <int 1-8191> md [<string 22> | md_index <uint 1-4294967295>] ma [<string 22> | ma_index <uint 1-4294967295>]] {num <int 1-65535> | [length <int 0-1500> | pattern <string 1500>] | pdu_priority <int 0-7>}

20-1 config cfm ais md

Description

This command is used to configure the parameters of the Alarm Indication Signal (AIS) function on a MEP.

Format

config cfm ais md [<string 22> | md_index <uint 1-4294967295>] ma [<string 22> | ma_index <uint 1-4294967295>] mepid <int 1-8191> {period [1sec | 1min] | level <int 0-7> | state [enable | disable]}(1)

Parameters

<string 22> - Enter the maintenance domain name. The maximum length is 22 characters.
md_index - Specifies the maintenance domain index. **<uint 1-4294967295>** - Enter the maintenance domain index value here. This value must be between 1 and 4294967295.
ma - Specifies the maintenance association name. **<string 22>** - Enter the maintenance association name. The maximum length is 22 characters. **ma_index** - Specifies the maintenance association index. **<uint 1-4294967295>** - Enter the maintenance association index value here. This value must be between 1 and 4294967295.
mepid - Specifies the MEPID. **<int 1-8191>** - Enter the MEP MEPID between 1 and 8191.
period - Specifies the transmitting interval of the AIS PDU. **1sec** - Specifies that the transmitting interval period will be set to 1 second. **1min** - Specifies that the transmitting interval period will be set to 1 minute.
level - Specifies the client level ID to which the MEP sends AIS PDU. The default client MD level is the MD level that the most immediate client layer MIPs and MEPs exist on. **<int 0-7>** - Enter the client level ID used here. This value must be between 0 and 7.

state - Specifies the AIS function state used.
- **enable** - Specifies that AIS function state will be enabled.
- **disable** - Specifies that AIS function state will be disabled.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the AIS function so that it is enabled and has a client level of 5:

```
DGS-3000-28XMP:admin#config cfm ais md op-domain ma op-ma mepid 1 state enable level 5
Command: config cfm ais md op-domain ma op-ma mepid 1 state enable level 5

Success.

DGS-3000-28XMP:admin#
```

20-2 config cfm lock md

Description

This command is used to configure the parameters of the LCK function on a MEP.

Format

config cfm lock md [<string 22> | md_index <uint 1-4294967295>] ma [<string 22> | ma_index <uint 1-4294967295>] mepid <int 1-8191> {period [1sec | 1min] | level <int 0-7> | state [enable | disable]}(1)

Parameters

<string 22> - Enter the maintenance domain name. The maximum length is 22 characters.

md_index - Specifies the maintenance domain index.
- **<uint 1-4294967295>** - Enter the maintenance domain index value here. This value must be between 1 and 4294967295.

ma - Specifies the maintenance association name.
- **<string 22>** - Enter the maintenance association name. The maximum length is 22 characters.
- **ma_index** - Specifies the maintenance association index.
  - **<uint 1-4294967295>** - Enter the maintenance association index value here. This value must be between 1 and 4294967295.

mepid - Specifies the MEPID.
- **<int 1-8191>** - Enter the MEP MEPID between 1 and 8191.

period - Specifies the transmitting interval of the LCK PDU.
- **1sec** - Specifies that the transmitting interval period will be set to 1 second.
- **1min** - Specifies that the transmitting interval period will be set to 1 minute.

level - Specifies the client level ID to which the MEP sends LCK PDU. The default client MD level is the MD level that the most immediate client layer MIPs and MEPs exist on.
- **<int 0-7>** - Enter the client level ID used here. This value must be between 0 and 7.

state - Specifies the LCK function state used.

enable - Specifies that LCK function state will be enabled.

disable - Specifies that LCK function state will be disabled.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the LCK function state as enabled and specify a client level of 5:

```
DGS-3000-28XMP:admin#config cfm lock md op-domain ma op-ma mepid 1 state enab
le level 5
Command: config cfm lock md op-domain ma op-ma mepid 1 state enable level 5

Success.

DGS-3000-28XMP:admin#
```

20-3 show cfm

Description

This command is used to show the CFM configuration.

Format

show cfm {[md [<string 22> | md_index <uint 1-4294967295>] {ma [<string 22> | ma_index <uint 1-4294967295>] {mepid <int 1-8191>}} | mepname <string 32>]}

Parameters

md - (Optional) Specifies the maintenance domain name.

<string 22> - Enter the maintenance domain name used here. This name can be up to 22 characters long.

md_index - Specifies the maintenance domain index.

<uint 1-4294967295> - Enter the maintenance domain index value here. This value must be between 1 and 4294967295.

ma - (Optional) Specifies the maintenance association name.

<string 22> - Enter the maintenance association name used here. This name can be up to 22 characters long.

ma_index - Specifies the maintenance association index.

<uint 1-4294967295> - Enter the maintenance association index value here. This value must be between 1 and 4294967295.

mepid - (Optional) Specifies the MEP ID.

<int 1-8191> - Enter the MEP ID used here. This value must be between 1 and 8191.

mepname - (Optional) Specifies the MEP name.

<string 32> - Enter the MEP name used here. This name can be up to 32 characters long.

Restrictions

None.

Example

To show the CFM configuration:

```
DGS-3000-28XMP:admin# show cfm
Command: show cfm

CFM State: Enabled

MD Index    MD Name                 Level
----------  ----------------------  -----
1           op_domain               2

DGS-3000-28XMP:admin# show cfm md op_domain
Command: show cfm md op_domain

MD Index    : 1
MD Name     : op_domain
MD Level    : 2
MIP Creation: Explicit
SenderID TLV: None

MA Index    MA Name                 VID
----------  ----------------------  ----
1           op1                     1

DGS-3000-28XMP:admin# show cfm md op_domain ma op1
Command: show cfm md op_domain ma op1

MA Index    : 1
MA Name     : op1
MA VID      : 1
MIP Creation: Defer
CCM Interval: 1 second
SenderID TLV: Defer
MEPID List  : 1

MEPID  Direction  Port   Name         MAC Address
-----  ---------  -----  -----------  -----------------
1      Inward     2      mep1         00-01-02-03-04-02


DGS-3000-28XMP:admin# show cfm mepname mep1
Command: show cfm mepname mep1

Name                : mep1
MEPID               : 1
Port                : 2
Direction           : Inward
CFM Port Status     : Disabled
MAC Address         : 00-01-02-03-04-02
MEP State           : Enabled
CCM State           : Enabled
PDU Priority        : 7
Fault Alarm         : Disabled
Alarm Time          : 250 centisecond((1/100)s)
```

```
Alarm Reset Time    : 1000 centisecond((1/100)s)
Highest Fault       : None
Out-of-Sequence CCMs: 0 received
Cross-connect CCMs  : 0 received
Error CCMs          : 0 received
Normal CCMs         : 0 received
Port Status CCMs    : 0 received
If Status CCMs      : 0 received
CCMs transmitted    : 0
In-order LBRs       : 0 received
Out-of-order LBRs   : 0 received
Next LTM Trans ID   : 0
Unexpected LTRs     : 0 received
LBMs Transmitted    : 0


Remote
MEPID  MAC Address       Status RDI PortSt  IfSt       Detect Time
------ ----------------- ------ --- ------- ---------- -------------------
2      FF-FF-FF-FF-FF-FF FAILED No  No      No         2011-07-13 12:00:00

DGS-3000-28XMP:admin#
```

20-4 show cfm fault

Description

This command is used to display all the fault conditions detected by the MEPs contained in the specified MA or MD. This display provides the overview of the fault status by MEPs.

Format

show cfm fault {md [<string 22> | md_index <uint 1-4294967295>] {ma [<string 22> | ma_index <uint 1-4294967295>]}}

Parameters

md - (Optional) Specifies the maintenance domain name.

<string 22> - Enter the maintenance domain name used here. This name can be up to 22 characters long.

md_index - Specifies the maintenance domain index.

<uint 1-4294967295> - Enter the maintenance domain index value here. This value must be between 1 and 4294967295.

ma - (Optional) Specifies the maintenance association name.

<string 22> - Enter the maintenance association name used here. This name can be up to 22 characters long.

ma_index - Specifies the maintenance association index.

<uint 1-4294967295> - Enter the maintenance association index value here. This value must be between 1 and 4294967295.

Restrictions

None.

Example

To show the CFM faults:

```
DGS-3000-28XMP:admin# show cfm fault
Command: show cfm fault

MD Name      MA Name      MEPID  Status
-----------  -----------  -----  --------------------------------
op_domain    op1          1      Cross-connect CCM Received

DGS-3000-28XMP:admin#
```

20-5 cfm lock md

Description

This command is used to start/stop cfm management lock. This command will result in the MEP sending a LCK PDU to client level MEP.

Format

cfm lock md [<string 22> | md_index <uint 1-4294967295>] ma [<string 22> | ma_index <uint 1-4294967295>] mepid <int 1-8191> remote_mepid <int 1-8191> action [start | stop]

Parameters

<string 22> - Enter the maintenance domain name here. This name can be up to 22 characters long.

md_index - Specifies the MD index value used.
- **<uint 1-4294967295>** - Enter the MD index value used here. This value must be between 1 and 4294967295.

ma - Specifies the maintenance association name.
- **<string 22>** - Enter the maintenance association name here. This name can be up to 22 characters long.
- **ma_index** - Specifies the MA index value used.
  - **<uint 1-4294967295>** - Enter the MA index value used here. This value must be between 1 and 4294967295.

mepid - The MEP ID in the MD which sends the LCK frame.
- **<int 1-8191>** - Enter the MEP ID value here. This value must be between 1 and 8191.

remote_mepid - Specifies the ID of the remote MEP.
- **<int 1-8191>** - Enter the remote MEP ID used here. This value must be between 1 and 8191.

action - Specifies to start or to stop the management lock function.
- **start** - Specifies to start the management lock function.
- **stop** - Specifies to stop the management lock function.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To start management lock:

```
DGS-3000-28XMP:admin#cfm lock md op-domain ma op-ma mepid 1 remote_mepid 2 ac
tion start
Command: cfm lock md op-domain ma op-ma mepid 1 remote_mepid 2 action start

Success.

DGS-3000-28XMP:admin#
```

20-6 cfm loopback

Description

This command is used to start a CFM loopback test. You can press Ctrl+C to exit the loopback test. The MAC address represents the destination MEP or MIP that can be reached by this MAC address. The MEP represents the source MEP to initiate the loopback message.

Format

cfm loopback <macaddr> [mepname <string 32> | mepid <int 1-8191> md [<string 22> | md_index <uint 1-4294967295>] ma [<string 22> | ma_index <uint 1-4294967295>]] {num <int 1-65535> | [length <int 0-1500> | pattern <string 1500>] | pdu_priority <int 0-7>}

Parameters

<macaddr> - Enter the destination MAC address here.

mepname - Specifies the MEP name used.
- **<string 32>** - Enter the MEP name used here. This name can be up to 32 characters long.

mepid - Specifies the MEP ID used.
- **<int 1-8191>** - Enter the MEP ID used here. This value must be between 1 and 8191.
- **md** - Specifies the maintenance domain name.
  - **<string 22>** - Enter the maintenance domain name here. This name can be up to 22 characters long.
  - **md_index** - Specifies the maintenance domain index.
    - **<uint 1-4294967295>** - Enter the maintenance domain index value here. This value must be between 1 and 4294967295.
    - **ma** - Specifies the maintenance association name.
      - **<string 22>** - Enter the maintenance association name here. This name can be up to 22 characters long.
      - **ma_index** - Specifies the maintenance association index.
        - **<uint 1-4294967295>** - Enter the maintenance association index value here. This value must be between 1 and 4294967295.

num - (Optional) Number of Loopback Messages (LBMs) to be sent. The default value is 4.
- **<int 1-65535>** - Enter the number of LBMs to be sent here. This value must be between 1 and 65535.

length - (Optional) The payload length of the LBM to be sent. The default is 0.
- **<int 0-1500>** - Enter the payload length here. This value must be between 0 and 1500.

pattern - (Optional) An arbitrary amount of data to be included in a Data TLV, along with an indication whether the Data TLV is to be included.
- **<string 1500>** - Enter the pattern used here. This value can be up to 1500 characters long.

pdu_priority - (Optional) The 802.1p priority to be set in the transmitted LBMs. If not specified, it uses the same priority as CCMs and LTMs sent by the MA.
- **<int 0-7>** - Enter the PDU priority value here. This value must be between 0 and 7.

Restrictions

None.

Example

To transmit a LBM:

```
DGS-3000-28XMP:admin# cfm loopback 32-00-70-89-31-06 mepname mep1
Command: cfm loopback 32-00-70-89-31-06 mepname mep1

Reply from 32-00-70-89-31-06: bytes=0 time=50ms
Reply from 32-00-70-89-31-06: bytes=0 time=50ms
Reply from 32-00-70-89-31-06: bytes=0 time=50ms
Reply from 32-00-70-89-31-06: bytes=0 time=50ms

CFM loopback statistics for 32-00-70-89-31-06:
        Packets: Sent=4, Received=4, Lost=0(0% loss).

DGS-3000-28XMP:admin#
```

Chapter 21 CPU Interface Filtering Command List

create cpu access_profile profile_id <value 1-5> [ethernet {vlan | source_mac <macmask 000000000000-ffffffffffff> | destination_mac <macmask 000000000000-ffffffffffff> | 802.1p | ethernet_type} | ip {vlan | source_ip_mask <netmask> | destination_ip_mask <netmask> | dscp | [icmp {type | code} | igmp {type} | tcp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff> | flag_mask [all | {urg | ack | psh | rst | syn | fin}]} | udp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | protocol_id_mask <hex 0x0-0xff> {user_define_mask <hex 0x0-0xffffffff>}]} | packet_content_mask {offset_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>} | ipv6 {class | flowlabel | source_ipv6_mask <ipv6mask> | destination_ipv6_mask <ipv6mask>}]
delete cpu access_profile [profile_id <value 1-5> | all]
config cpu access_profile profile_id <value 1-5> [add access_id [auto_assign | <value 1-100>] [ethernet {[vlan <vlan_name 32> | vlan_id <vlanid 1-4094>] | source_mac <macaddr> | destination_mac <macaddr> | 802.1p <value 0-7> | ethernet_type <hex 0x0-0xffff>} | ip {[vlan <vlan_name 32> | vlan_id <vlanid 1-4094>] | 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> | flag [all | {urg | ack | psh | rst | syn | fin}]} | udp {src_port <value 0-65535> | dst_port <value 0-65535>} | protocol_id <value 0-255> {user_define <hex 0x0-0xffffffff>}]} | 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>} | ipv6 {class <value 0-255> | flowlabel <hex 0x0-0xfffff> | source_ipv6 <ipv6addr> | destination_ipv6 <ipv6addr>}] port [<portlist> | all] [permit | deny] {time_range <range_name 32>} | delete access_id <value 1-100>]
enable cpu_interface_filtering
disable cpu_interface_filtering
show cpu access_profile {profile_id <value 1-5>}

21-1 create cpu access_profile profile_id

Description

This command is used to create CPU access list profiles.

Format

create cpu access_profile profile_id <value 1-5> [ethernet {vlan \| source_mac <macmask 000000000000-ffffffffffff> \| destination_mac <macmask 000000000000-ffffffffffff> \| 802.1p \| ethernet_type} \| ip {vlan \| source_ip_mask <netmask> \| destination_ip_mask <netmask> \| dscp \| [icmp {type \| code} \| igmp {type} \| tcp {src_port_mask <hex 0x0-0xffff> \| dst_port_mask <hex 0x0-0xffff> \| flag_mask [all \| {urg \| ack \| psh \| rst \| syn \| fin}]} \| udp {src_port_mask <hex 0x0-0xffff> \| dst_port_mask <hex 0x0-0xffff>} \| protocol_id_mask <hex 0x0-0xff> {user_define_mask <hex 0x0-0xffffffff>}]} \| packet_content_mask {offset_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>} \| ipv6 {class \| flowlabel \| source_ipv6_mask <ipv6mask> \| destination_ipv6_mask <ipv6mask>}]

Parameters

<value 1-5> - Enter the profile ID value here. This value must be between 1 and 5.

ethernet - Specifies that the profile type will be Ethernet.
- **vlan** - (Optional) Specifies a VLAN mask.
- **source_mac** - (Optional) Specifies the source MAC mask.
  - **<macmask>** - Enter the source MAC mask here.
- **destination_mac** - (Optional) Specifies the destination mac mask.
  - **<macmask>** - Enter the destination MAC mask here.
- **802.1p** - (Optional) Specifies the 802.1p priority tag mask.
- **ethernet_type** - (Optional) Specifies the Ethernet type mask.

ip - Specifies that the profile type will be IP.
- **vlan** - (Optional) Specifies a VLAN mask.
- **source_ip_mask** - (Optional) Specifies an IP source submask.
  - **<netmask>** - Enter the IP source submask here.
- **destination_ip_mask** - (Optional) Specifies an IP destination submask.
  - **<netmask>** - Enter the IP destination submask here.
- **dscp** - (Optional) Specifies the DSCP mask.
- **icmp** - (Optional) Specifies that the rule applies to ICMP traffic.
  - **type** - (Optional) Specifies that the rule applies to ICMP type traffic.
  - **code** - (Optional) Specifies that the rule applies to ICMP code traffic.
- **igmp** - (Optional) Specifies that the rule applies to IGMP traffic.
  - **type** - (Optional) Specifies that the rule applies to IGMP type traffic.
- **tcp** - Specifies that the rule applies to TCP traffic.
  - **src_port_mask** - (Optional) Specifies the TCP source port mask.
    - **<hex 0x0-0xffff>** - Enter the source TCP port mask here.
  - **dst_port_mask** - (Optional) Specifies the TCP destination port mask.
    - **<hex 0x0-0xffff>** - Enter the destination TCP port mask here.
  - **flag_mask** - (Optional) Specifies the TCP flag field mask.
    - **all** - Specifies that the TCP flag field mask will be set to all.
    - **urg** - (Optional) Specifies that the TCP flag field mask will be set to urg.
    - **ack** - (Optional) Specifies that the TCP flag field mask will be set to ack.
    - **psh** - (Optional) Specifies that the TCP flag field mask will be set to psh.
    - **rst** - (Optional) Specifies that the TCP flag field mask will be set to rst.
    - **syn** - (Optional) Specifies that the TCP flag field mask will be set to syn.
    - **fin** - (Optional) Specifies that the TCP flag field mask will be set to fin.
- **udp** - (Optional) Specifies that the rule applies to UDP traffic.
  - **src_port_mask** - (Optional) Specifies the UDP source port mask.
    - **<hex 0x0-0xffff>** - Enter the source UDP port mask here.
  - **dst_port_mask** - (Optional) Specifies the UDP destination port mask.
    - **<hex 0x0-0xffff>** - Enter the destination UDP port mask here.
- **protocol_id_mask** - (Optional) Specifies that the rule applies to the IP protocol ID traffic.
  - **<hex 0x0-0xff>** - Enter the IP protocol ID mask here.
  - **user_define_mask** - (Optional) Specifies that the rule applies to the IP protocol ID and the mask options behind the first 4 bytes of the IP payload.
    - **<hex 0x0-0xffffffff>** - Enter the user-defined IP protocol ID mask here.

packet_content_mask - Specifies the frame content mask, there are 5 offsets in maximum could be configured. Each offset presents 16 bytes, the range of mask of frame is 80 bytes (5 offsets) in the first 80 bytes of the frame.
- **offset_0-15** - (Optional) Specifies that the mask pattern offset of the frame will be between 0 and 15.

<hex 0x0-0xffffffff> - Enter the mask pattern offset of the frame between 0 and 15 here.
offset_16-31 - (Optional) Specifies that the mask pattern offset of the frame will be between 16 and 31.
<hex 0x0-0xffffffff> - Enter the mask pattern offset of the frame between 16 and 31 here.
offset_32-47 - (Optional) Specifies that the mask pattern offset of the frame will be between 32 and 47.
<hex 0x0-0xffffffff> - Enter the mask pattern offset of the frame between 32 and 47 here.
offset_48-63 - (Optional) Specifies that the mask pattern offset of the frame will be between 48 and 63.
<hex 0x0-0xffffffff> - Enter the mask pattern offset of the frame between 48 and 63 here.
offset_64-79 - (Optional) Specifies that the mask pattern offset of the frame will be between 64 and 79.
<hex 0x0-0xffffffff> - Enter the mask pattern offset of the frame between 64 and 79 here.

ipv6 - Specifies IPv6 filtering mask.
class - (Optional) Specifies the IPv6 class.
flowlabel - (Optional) Specifies the IPv6 flow label.
source_ipv6_mask - (Optional) Specifies an IPv6 source submask.
<ipv6mask> - Enter the IPv6 source submask here.
destination_ipv6_mask - (Optional) Specifies an IPv6 destination submask.
<ipv6mask> - Enter the IPv6 destination submask here.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To create CPU access list rules:

```
DGS-3000-28XMP:admin# create cpu access_profile profile_id 1 ethernet vlan source_mac 00-00-
00-00-00-01 destination_mac 00-00-00-00-00-02 802.1p ethernet_type
Command: create cpu access_profile profile_id 1 ethernet vlan source_mac 00-00-00-00-00-01
destination_mac 00-00-00-00-00-02 802.1p ethernet_type

Success.

DGS-3000-28XMP:admin# create cpu access_profile profile_id 2 ip vlan source_ip_mask 20.0.0.0
destination_ip_mask 10.0.0.0 dscp icmp type code
Command: create cpu access_profile profile_id 2 ip vlan source_ip_mask 20.0.0.0
destination_ip_mask 10.0.0.0 dscp icmp type code

Success.

DGS-3000-28XMP:admin#
```

21-2 delete cpu access_profile

Description

This command is used to delete CPU access list rules.

Format

delete cpu access_profile [profile_id <value 1-5> | all]

Parameters

profile_id - Specifies the index of access list profile.
- **<value 1-5>** - Enter the profile ID value here. This value must be between 1 and 5.
- **all** - Specifies that all the access list profiles will be deleted.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete CPU access list rules:

```
DGS-3000-28XMP:admin# delete cpu access_profile profile_id 1
Command: delete cpu access_profile profile_id 1

Success.

DGS-3000-28XMP:admin#
```

21-3 config cpu access_profile profile_id

Description

This command is used to configure a CPU access list entry.

Format

config cpu access_profile profile_id <value 1-5> [add access_id [auto_assign | <value 1-100>] [ethernet {[vlan <vlan_name 32> | vlan_id <vlanid 1-4094>] | source_mac <macaddr> | destination_mac <macaddr> | 802.1p <value 0-7> | ethernet_type <hex 0x0-0xffff>} | ip {[vlan <vlan_name 32> | vlan_id <vlanid 1-4094>] | 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> | flag [all | {urg | ack | psh | rst | syn | fin}]} | udp {src_port <value 0-65535> | dst_port <value 0-65535>} | protocol_id <value 0-255> {user_define <hex 0x0-0xffffffff>}]} | 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>} | ipv6 {class <value 0-255> | flowlabel <hex 0x0-0xfffff> | source_ipv6 <ipv6addr> | destination_ipv6 <ipv6addr>}] port [<portlist> | all] [permit | deny] {time_range <range_name 32>} | delete access_id <value 1-100>]

Parameters

<value 1-5> - Enter the profile ID value here. This value must be between 1 and 5.

add - Specifies that a profile or a rule will be added.
- **access_id** - Specifies the index of the access list entry. The range of this value is 1-100.
  - **auto_assign** - Specifies that the access ID will automatically be assigned.
  - **<value 1-100>** - Enter the access ID here. This value must be between 1 and 100.

ethernet - Specifies that the profile type will be Ethernet.
- **vlan** - (Optional) Specifies the VLAN name used.
  - **<vlan_name 32>** - Enter the name of the VLAN here. This name can be up to 32 characters long.

vlan_id - (Optional) Specifies the VLAN ID used.
<vlanid 1-4094> - Enter the VLAN ID used here.
source_mac - (Optional) Specifies the source MAC address.
<macaddr> - Enter the source MAC address used for this configuration here.
destination_mac - (Optional) Specifies the destination MAC.
<macaddr> - Enter the destination MAC address used for this configuration here.
802.1p - (Optional) Specifies the value of the 802.1p priority tag.
<value 0-7> - Enter the 802.1p priority tag value here. This value must be between 0 and 7.
ethernet_type - (Optional) Specifies the Ethernet type.
<hex 0x0-0xffff> - Enter the Ethernet type value here.

ip - Specifies that the profile type will be IP.
vlan - (Optional) Specifies the VLAN name used.
<vlan_name 32> - Enter the name of the VLAN here. This name can be up to 32 characters long.
vlan_id - (Optional) Specifies the VLAN ID used.
<vlanid 1-4094> - Enter the VLAN ID used here.
source_ip - (Optional) Specifies an IP source address.
<ipaddr> - Enter the source IP address used for this configuration here.
destination_ip - (Optional) Specifies an IP destination address.
<ipaddr> - Enter the destination IP address used for this configuration here.
dscp - (Optional) Specifies the value of DSCP, the value can be configured 0 to 63.
<value 0-63> - Enter the DSCP value used here.
icmp - (Optional) Specifies that the rule applies to ICMP traffic.
type - (Optional) Specifies that the rule applies to the value of ICMP type traffic.
<value 0-255> - Enter the ICMP type value here. This value must be between 0 and 255.
code - (Optional) Specifies that the rule applies to the value of ICMP code traffic.
<value 0-255> - Enter the ICMP code value here. This value must be between 0 and 255.
igmp - (Optional) Specifies that the rule applies to IGMP traffic.
type - (Optional) Specifies that the rule applies to the value of IGMP type traffic.
<value 0-255> - Enter the IGMP type value here. This value must be between 0 and 255.
tcp - (Optional) Specifies that the rule applies to TCP traffic.
src_port - (Optional) Specifies that the rule applies the range of TCP source port.
<value 0-65535> - Enter the source port value here. This value must be between 0 and 65535.
dst_port - (Optional) Specifies the range of TCP destination port range.
<value 0-65535> - Enter the destination port value here. This value must be between 0 and 65535.
flag - (Optional) Specifies the TCP flag fields .
all - Specifies that the TCP flag field mask will be set to all.
urg - (Optional) Specifies that the TCP flag field mask will be set to urg.
ack - (Optional) Specifies that the TCP flag field mask will be set to ack.
psh - (Optional) Specifies that the TCP flag field mask will be set to psh.
rst - (Optional) Specifies that the TCP flag field mask will be set to rst.
syn - (Optional) Specifies that the TCP flag field mask will be set to syn.
fin - (Optional) Specifies that the TCP flag field mask will be set to fin.
udp - Specifies that the rule applies to UDP traffic.
src_port - (Optional) Specifies the range of UDP source port range.
<value 0-65535> - Enter the source port value here. This value must be between 0 and 65535.
dst_port - (Optional) Specifies the range of UDP destination port mask.
<value 0-65535> - Enter the destination port value here. This value must be between 0 and 65535.
protocol_id - Specifies that the rule applies to the value of IP protocol ID traffic.
<value 0-255> - Enter the protocol ID value here. This value must be between 0 and 255.
user_define - (Optional) Specifies that the rule applies to the IP protocol ID and the mask options behind

the first 4 bytes of the IP payload. **<hex 0x0-0xffffffff>** - Enter the user-defined IP protocol ID mask here.
packet_content - Specifies the frame content pattern, there are 5 offsets in maximum could be configure. Each offset presents 16 bytes, the range of content of frame is 80 bytes(5 offsets) in the first 80 bytes of the frame. **offset_0-15** - (Optional) Specifies that the mask pattern offset of the frame will be between 0 and 15. **<hex 0x0-0xffffffff>** - Enter the mask pattern offset of the frame between 0 and 15 here. **offset_16-31** - (Optional) Specifies that the mask pattern offset of the frame will be between 16 and 31. **<hex 0x0-0xffffffff>** - Enter the mask pattern offset of the frame between 16 and 31 here. **offset_32-47** - (Optional) Specifies that the mask pattern offset of the frame will be between 32 and 47. **<hex 0x0-0xffffffff>** - Enter the mask pattern offset of the frame between 32 and 47 here. **offset_48-63** - (Optional) Specifies that the mask pattern offset of the frame will be between 48 and 63. **<hex 0x0-0xffffffff>** - Enter the mask pattern offset of the frame between 48 and 63 here. **offset_64-79** - (Optional) Specifies that the mask pattern offset of the frame will be between 64 and 79. **<hex 0x0-0xffffffff>** - Enter the mask pattern offset of the frame between 64 and 79 here.
ipv6 - Specifies the rule applies to IPv6 fields. **class** - (Optional) Specifies the value of IPv6 class. **<value 0-255>** - Enter the IPv6 class value here. This value must be between 0 and 255. **flowlabel** - (Optional) Specifies the value of IPv6 flow label. **<hex 0x0-0xffff>** - Enter the IPv6 flow label here. **source_ipv6** - (Optional) Specifies the value of IPv6 source address. **<ipv6addr>** - Enter the IPv6 source address used for this configuration here. **destination_ipv6** - (Optional) Specifies the value of IPv6 destination address. **<ipv6addr>** - Enter the IPv6 destination address used for this configuration here.
port - Specifies the list of ports to be included in this configuration. **<portlist>** - Enter a list of ports used for the configuration here. **all** - Specifies that all the ports will be used for this configuration.
permit - Specifies that the packets that match the access profile are permitted by the Switch.
deny - Specifies that the packets that match the access profile are filtered by the Switch.
time_range - (Optional) Specifies the name of this time range entry. **<range_name 32>** - Enter the time range here.
delete - Specifies to delete a rule from the profile ID entered. **access_id** - Specifies the index of access list entry. The range of this value is 1-100. **<value 1-100>** - Enter the access ID here. This value must be between 1 and 100.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure CPU access list entry:

```
DGS-3000-28XMP:admin# config cpu access_profile profile_id 1 add access_id 1 ip
vlan default  source_ip 20.2.2.3 destination_ip 10.1.1.252 dscp 3 icmp type 11 code
32 port 1 deny
Command: config cpu access_profile profile_id 1 add access_id 1 ip vlan default
source_ip 20.2.2.3 destination_ip 10.1.1.252 dscp 3 icmp type 11 code 32 port 1
deny

Success.

DGS-3000-28XMP:admin#
```

21-4 enable cpu interface filtering

Description

This command is used to enable CPU interface filtering control.

Format

enable cpu_interface_filtering

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable cpu_interface_filtering:

```
DGS-3000-28XMP:admin# enable cpu_interface_filtering
Command: enable cpu_interface_filtering

Success.

DGS-3000-28XMP:admin#
```

21-5 disable cpu interface filtering

Description

This command is used to disable CPU interface filtering control.

Format

disable cpu_interface_filtering

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To disable cpu_interface_filtering:

```
DGS-3000-28XMP:admin# disable cpu_interface_filtering
Command: disable cpu_interface_filtering

Success.

DGS-3000-28XMP:admin#
```

21-6 show cpu access_profile

Description

This command is used to display the current access list table.

Format

show cpu access_profile {profile_id <value 1-5>}

Parameters

profile_id - (Optional) Specifies the index of the access list profile.
<value 1-5> - Enter the profile ID used here. This value must be between 1 and 5.

Restrictions

None.

Example

To display current CPU access list table:

```
DGS-3000-28XMP:admin# show cpu access_profile
Command: show cpu access_profile

CPU Interface Filtering State: Disabled

CPU Interface Access Profile Table

Total Unused Rule Entries : 500
Total Used Rule Entries   : 0

================================================================================
Profile ID: 1     Type: Ethernet

MASK on
    VLAN            : 0xFFF
    Source MAC      : 00-00-00-00-00-01
    Destination MAC : 00-00-00-00-00-02
    802.1p
    Ethernet Type

Unused Rule Entries: 100
================================================================================


================================================================================
Profile ID: 2     Type: IPv4

MASK on
    VLAN            : 0xFFF
    Source IP       : 20.0.0.0
    Dest IP         : 10.0.0.0
    DSCP
    ICMP
    Type
    Code

Unused Rule Entries: 100
================================================================================



DGS-3000-28XMP:admin#
```

Chapter 22 Debug Software Command List

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

22-1 debug error_log

Description

This command is used to dump, clear or upload the software error log to a TFTP server.

Format

debug error_log [dump | clear | upload_toTFTP {<ipaddr> <path_filename 64>}]

Parameters

dump - Specifies to display the debug message of the debug log.
clear - Specifies to clear the debug log.
upload_toTFTP - Specifies to upload the debug log to a TFTP server specified by IP address. **<ipaddr>** - (Optional) Enter the IPv4 address of the TFTP server. **<path_filename 64>** - (Optional) Enter the DOS pathname on the TFTP server. It can be a relative pathname or an absolute pathname. This value can be up to 64 characters long.

Restrictions

Only Administrators can issue this command.

Example

To dump the error log:

```
DGS-3000-28XMP:admin# debug error_log dump
Command: debug error_log dump

********************************************************************************
# debug log: 1
# level: fatal
# clock: 10000ms
# time : 2009/03/11 13:00:00

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

Current TASK : bcmARL.0

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

To clear the error log:

```
DGS-3000-28XMP:admin# debug error_log clear
Command: debug error_log clear

Success.

DGS-3000-28XMP:admin#
```

To upload the error log to TFTP server:

```
DGS-3000-28XMP:admin# debug error_log upload_toTFTP 10.0.0.90 debug-log.txt
Command: debug error_log upload_toTFTP 10.0.0.90 debug-log.txt

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

DGS-3000-28XMP:admin#
```

22-2 debug buffer

Description

This command is used to show the debug buffer's state, or dump, clear, or upload the debug buffer to a TFTP server.

Format

debug buffer [utilization | dump | clear | upload_toTFTP <ipaddr> <path_filename 64>]

Parameters

utilization - Specifies to display the debug buffer's state.
dump - Specifies to display the debug message in the debug buffer.
clear - Specifies to clear the debug buffer.
upload_toTFTP - Specifies to upload the debug buffer to a TFTP server specified by IP address. **<ipaddr>** - Enter the IPv4 address of the TFTP server. **<path_filename 64>** - Enter the DOS pathname on the TFTP server. It can be a relative pathname or an absolute pathname. This value can be up to 64 characters long.

Restrictions

Only Administrators can issue this command.

Example

To show the debug buffer's state:

```
DGS-3000-28XMP:admin# debug buffer utilization
Command: debug buffer utilization

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

DGS-3000-28XMP:admin#
```

To clear the debug buffer:

```
DGS-3000-28XMP:admin# debug buffer clear
Command: debug buffer clear

Success.

DGS-3000-28XMP:admin#
```

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

```
DGS-3000-28XMP:admin# debug buffer upload_toTFTP 10.0.0.90 debugcontent.txt
Command: debug buffer upload_toTFTP 10.0.0.90 debugcontent.txt

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

DGS-3000-28XMP:admin#
```

22-3 debug output

Description

This command is used to set a specified module's debug message output to debug buffer or local console. If the user uses the command in a Telnet session, the error message also is output to the local console.

Format

debug output [module <module_list> | all] [buffer | console | monitor]

Parameters

module - Specifies the module list. **<module_list>** - Enter the module list here. **all** - Specifies to the control output method of all modules.
buffer - Specifies to direct the debug message of the module output to debug buffer. This is the default option.
console - Specifies to direct the debug message of the module output to local console.
monitor - Specifies to direct the debug message of the module output to SSH/Telnet.

Restrictions

Only Administrators can issue this command.

Example

To set all module debug message outputs to local console:

```
DGS-3000-28XMP:admin# debug output all console
Command: debug output all console

Success.

DGS-3000-28XMP:admin#
```

22-4 debug config error_reboot

Description

This command is used to set if the Switch needs to be rebooted when a fatal error occurs. When the error occurs, the watchdog timer will be disabled by the system first, and then all debug information will be saved in NVRAM. If the error_reboot is enabled, the watchdog shall be enabled after all information is stored into NVRAM.

Format

debug config error_reboot [enable | disable]

Parameters

enable - Specifies to reboot when a fatal error happens.
disable - Specifies that the Switch will not reboot when a fatal error happens, system will hang-up for debug and enter the debug shell mode for debug.

Restrictions

Only Administrators can issue this command.

Example

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

```
DGS-3000-28XMP:admin# debug config error_reboot disable
Command: debug config error_reboot disable

Success.

DGS-3000-28XMP:admin#
```

22-5 debug config state

Description

This command is used to set the state of the debug.

Format

debug config state [enable | disable]

Parameters

enable - Specifies to enable the debug state.
disable - Specifies to disable the debug state.

Restrictions

Only Administrators can issue this command.

Example

To set the debug state to disabled:

```
DGS-3000-28XMP:admin# debug config state disable
Command: debug config state disable

Success.

DGS-3000-28XMP:admin#
```

22-6 debug show error_reboot state

Description

This command is used to display debug error reboot state.

Format

debug show error_reboot state

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To show the debug error reboot state:

```
DGS-3000-28XMP:admin# debug show error_reboot state
Command: debug show error_reboot state

Error Reboot: Enabled

DGS-3000-28XMP:admin#
```

22-7 debug show status

Description

This command is used to display the specified module's debug status.

Format

debug show status {module <module_list>}

Parameters

module – (Optional) Specifies the module list.
<module_list> - Enter the module list.

Restrictions

Only Administrators can issue this command.

Example

To show the specified module's debug state:

```
DGS-3000-28XMP:admin# debug show status module MSTP
Command: debug show status module MSTP

Debug Global State  : Enabled

MSTP                : Disabled

DGS-3000-28XMP:admin#
```

To show the debug state:

```
DGS-3000-28XMP:admin#debug show status
Command: debug show status

Debug Global State  : Enabled

MSTP                : Disabled
IMPB                : Disabled
DHCPv6_RELAY        : Disabled

DGS-3000-28XMP:admin#
```

Chapter 23 DHCP Local Relay Command List

config dhcp_local_relay vlan <vlan_name 32> state [enable | disable]
config dhcp_local_relay vlan vlanid <vlan_id> state [enable | disable]
config dhcp_local_relay option_82 circuit_id [default | vendor1]
config dhcp_local_relay option_82 ports <portlist> policy [replace | drop | keep]
config dhcp_local_relay option_82 remote_id [default | user_define <desc 32>]
enable dhcp_local_relay
disable dhcp_local_relay
show dhcp_local_relay
show dhcp_local_relay option_82 ports {<portlist>}

23-1 config dhcp_local_relay vlan

Description

This command is used to enable or disable the DHCP local relay function for the specified VLAN name.

When DHCP local relay is enabled for the VLAN, the DHCP packet will be relayed in a broadcast way without changing the source MAC address and gateway address. DHCP Option 82 will be automatically added.

Format

config dhcp_local_relay vlan <vlan_name 32> state [enable | disable]

Parameters

<vlan_name 32> - Enter the VLAN name for which the DHCP local relay function will be enabled. This name can be up to 32 characters long.
state - Specifies to enable or disable DHCP local relay for specified VLAN. **enable** - Specifies that the DHCP local relay function will be enabled. **disable** - Specifies that the DHCP local relay function will be disabled.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable DHCP local relay for the default VLAN:

```
DGS-3000-28XMP:admin# config dhcp_local_relay vlan default state enable
Command: config dhcp_local_relay vlan default state enable

Success.

DGS-3000-28XMP:admin#
```

23-2 config dhcp_local_relay vlan vlanid

Description

This command is used to enable or disable DHCP local relay function for specified VLAN ID.

Format

config dhcp_local_relay vlan vlanid <vlan_id> state [enable | disable]

Parameters

vlanid - Specifies the VLAN ID for which the DHCP local relay function will be enabled. **<vlan_id>** - Enter the VLAN ID used here.
state - Specifies to enable or disable DHCP local relay for the specified VLAN. **enable** - Specifies that the DHCP local relay function will be enabled. **disable** - Specifies that the DHCP local relay function will be disabled.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable DHCP local relay for the default VLAN:

```
DGS-3000-28XMP:admin# config dhcp_local_relay vlan vlanid 1 state enable
Command: config dhcp_local_relay vlan vlanid 1 state enable

Success.

DGS-3000-28XMP:admin#
```

23-3 config dhcp_local_relay option_82 circuit_id

Description

This command is used to configure the circuit ID of DHCP relay agent information Option 82 of the Switch.

Format

config dhcp_local_relay option_82 circuit_id [default | vendor1]

Parameters

default – Specifies the circuit ID of the DHCP relay agent to default.
vendor1 - Specifies the circuit ID of the DHCP relay agent to vendor1.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the circuit ID of DHCP relay agent as default:

```
DGS-3000-28XMP:admin# config dhcp_local_relay option_82 circuit_id default
Command: config dhcp_local_relay option_82 circuit_id default

Success.

DGS-3000-28XMP:admin#
```

23-4 config dhcp_local_relay option_82 ports

Description

This command is used to configure the settings of the specified ports for the policy of the Option 82.

Format

config dhcp_local_relay option_82 ports <portlist> policy [replace | drop | keep]

Parameters

<portlist> - Enter a list of ports to be configured.
policy - Specifies how to process the packets coming from the client side which have the Option 82 field. **replace** - Specifies to replace the existing Option 82 field in the packet. **drop** - Specifies to discard if the packet has the Option 82 field. **keep** - Specifies to retain the existing Option 82 field in the packet.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure port 1 to 5 for the policy of the Option 82:

```
DGS-3000-28XMP:admin# config dhcp_local_relay option_82 ports 1-5 policy keep
Command: config dhcp_local_relay option_82 ports 1-5 policy keep

Success.

DGS-3000-28XMP:admin#
```

23-5 config dhcp_local_relay option_82 remote_id

Description

This command is used to configure the remote ID.

Format

config dhcp_local_relay option_82 remote_id [default | user_define <desc 32>]

Parameters

default - Specifies to use the Switch's system MAC address as the remote ID.
user_define - Specifies to use the user-defined string as the remote ID. **<desc 32>** - Enter the maximum of 32 characters. Spaces are allowed in the string.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the remote ID:

```
DGS-3000-28XMP:admin# config dhcp_local_relay option_82 remote_id user_define D-Lin
k L2Switch
Command: config dhcp_local_relay option_82 remote_id user_define D-Link L2Switch

Success.

DGS-3000-28XMP:admin#
```

23-6 enable dhcp_local_relay

Description

This command is used to globally enable the DHCP local relay function on the Switch.

Format

enable dhcp_local_relay

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable the DHCP local relay function:

```
DGS-3000-28XMP:admin# enable dhcp_local_relay
Command: enable dhcp_local_relay

Success.

DGS-3000-28XMP:admin#
```

23-7 disable dhcp_local_relay

Description

This command is used to globally disable the DHCP local relay function on the Switch.

Format

disable dhcp_local_relay

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To disable the DHCP local relay function:

```
DGS-3000-28XMP:admin# disable dhcp_local_relay
Command: disable dhcp_local_relay

Success.

DGS-3000-28XMP:admin#
```

23-8 show dhcp_local_relay

Description

This command is used to display the current DHCP local relay configuration.

Format

show dhcp_local_relay

Parameters

None.

Restrictions

None.

Example

To display the DHCP local relay status:

```
DGS-3000-28XMP:admin# show dhcp_local_relay
Command: show dhcp_local_relay

DHCP/BOOTP Local Relay Status         : Disabled
DHCP/BOOTP Local Relay VID List       : 1

DHCP Relay Agent Information Option 82 Circuit ID : Default
DHCP Relay Agent Information Option 82 Remote ID : D-Link L2Switch


DGS-3000-28XMP:admin#
```

23-9 show dhcp_local_relay option_82 ports

Description

This command is used to display the current DHCP local relay Option 82 configuration of each port.

Format

show dhcp_local_relay option_82 ports {<portlist>}

Parameters

<portlist> - (Optional) Enter a list of ports to be displayed.

Restrictions

None.

Example

To display the DHCP local relay Option 82 configuration of port 1 to 5:

```
DGS-3000-28XMP:admin# show dhcp_local_relay option_82 ports 1-5
Command: show dhcp_local_relay option_82 ports 1-5

Port  Option 82
      Policy
----  ---------
1     keep
2     keep
3     keep
4     keep
5     keep


DGS-3000-28XMP:admin#
```

Chapter 24 DHCP Relay Command List

config dhcp_relay {hops <int 1-16> | time <sec 0-65535>}
config dhcp_relay add ipif <ipif_name 12> <ipaddr>
config dhcp_relay add vlanid <vlan_id_list> <ipaddr>
config dhcp_relay delete ipif <ipif_name 12> <ipaddr>
config dhcp_relay delete vlanid <vlan_id_list> <ipaddr>
config dhcp_relay option_82 {state [enable | disable] | check [enable | disable] | policy [replace | drop | keep] | remote_id [default | user_define <desc 32>]}(1)
config dhcp_relay option_82 circuit_id [default | vendor1]
enable dhcp_relay
disable dhcp_relay
show dhcp_relay {ipif <ipif_name 12>}
config dhcp_relay option_60 state [enable | disable]
config dhcp_relay option_60 add string <multiword 255> relay <ipaddr> [exact-match | partial-match]
config dhcp_relay option_60 default [relay <ipaddr> | mode [relay | drop]]
config dhcp_relay option_60 delete [string <multiword 255> {relay <ipaddr>} | ipaddress <ipaddr> | all | default {<ipaddr>}]
show dhcp_relay option_60 {[string <multiword 255> | ipaddress <ipaddr> | default]}
config dhcp_relay option_61 state [enable | disable]
config dhcp_relay option_61 add [mac_address <macaddr> | string <multiword 255>] [relay <ipaddr> | drop]
config dhcp_relay option_61 default [relay <ipaddr> | drop]
config dhcp_relay option_61 delete [mac_address <macaddr> | string <multiword 255> | all]
show dhcp_relay option_61

24-1 config dhcp_relay

Description

This command is used to configure the DHCP relay feature of the Switch.

Format

config dhcp_relay {hops <int 1-16> | time <sec 0-65535>}

Parameters

hops - (Optional) Specifies the maximum number of relay hops that the DHCP/BOOTP packets can cross. The range is 1 to 16. The default value is 4. The DHCP packet will be dropped when the relay hop count in the received packet is equal to or greater than this setting. **<int 1-16>** - Enter the maximum number of relay hops here. This value must be between 1 and 16.
time - (Optional) The time field in the DHCP packet must be equal to or greater than this setting to be relayed by the router. The default value is 0. **<sec 0-65535>** - Enter the relay time here. This value must be between 0 and 65535 seconds.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the DHCP relay hops and time parameters:

```
DGS-3000-28XMP:admin# config dhcp_relay hops 4 time 2
Command: config dhcp_relay hops 4 time 2

Success.

DGS-3000-28XMP:admin#
```

24-2 config dhcp_relay add ipif

Description

This command is used to add an IP destination address of the DHCP server for relay of DHCP/BOOTP packets.

Format

config dhcp_relay add ipif <ipif_name 12> <ipaddr>

Parameters

<ipif_name 12> - Enter the IP interface name used here. This name can be up to 12 characters long.
<ipaddr> - Enter the DHCP/BOOTP server IP address.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

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

```
DGS-3000-28XMP:admin# config dhcp_relay add ipif System 10.43.21.12
Command: config dhcp_relay add ipif System 10.43.21.12

Success.

DGS-3000-28XMP:admin#
```

24-3 config dhcp_relay add vlanid

Description

This command is used to add an IP address as a destination to forward (relay) DHCP/BOOTP packets. If there is an IP interface in the VLAN and it has configured a DHCP server at the interface level, then the configuration at the

interface level has higher priority. In this case, the DHCP server configured on the VLAN will not be used to forward the DHCP packets.

Format

config dhcp_relay add vlanid <vlan_id_list> <ipaddr>

Parameters

<vlan_id_list> - Enter the VLAN ID list used for this configuration here.
<ipaddr> - Enter the DHCP/BOOTP server IP address used here.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To add a DHCP/BOOTP server 10.43.21.12 to VLAN 1 to 10:

```
DGS-3000-28XMP:admin# config dhcp_relay add vlanid 1-10 10.43.21.12
Command: config dhcp_relay add vlanid 1-10 10.43.21.12

Success.

DGS-3000-28XMP:admin#
```

24-4 config dhcp_relay delete

Description

This command is used to delete one of the IP destination addresses in the Switch's relay table.

Format

config dhcp_relay delete ipif <ipif_name 12> <ipaddr>

Parameters

<ipif_name 12> - Enter the IP interface name used here. This name can be up to 12 characters long.
<ipaddr> - Enter the DHCP/BOOTP server IP address.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

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

```
DGS-3000-28XMP:admin# config dhcp_relay delete ipif System 10.43.21.12
Command: config dhcp_relay delete ipif System 10.43.21.12

Success.

DGS-3000-28XMP:admin#
```

24-5 config dhcp_relay delete vlanid

Description

This command is used to delete an IP address as a destination to forward (relay) DHCP/BOOTP packets.

Format

config dhcp_relay delete vlanid <vlan_id_list> <ipaddr>

Parameters

<vlan_id_list> - Enter the VLAN ID list used for this configuration here.
<ipaddr> - Enter the DHCP/BOOTP server IP address used here.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete a DHCP/BOOTP server 10.43.21.12 from VLAN 2 and VLAN 3:

```
DGS-3000-28XMP:admin# config dhcp_relay delete vlanid 2-3 10.43.21.12
Command: config dhcp_relay delete vlanid 2-3 10.43.21.12

Success.

DGS-3000-28XMP:admin#
```

24-6 config dhcp_relay option_82

Description

This command is used to configure the processing of DHCP Option 82 for the DHCP relay function.

Format

config dhcp_relay option_82 {state [enable | disable] | check [enable | disable] | policy [replace | drop | keep] | remote_id [default | user_define <desc 32>]}(1)

Parameters

state - When the state is enabled, the DHCP packet will be inserted with the Option 82 field before being relayed to server. The DHCP packet will be processed based on the behavior defined in check and policy setting.

When the state is disabled, the DHCP packet will be relayed directly to server without further check and processing on the packet. The default setting is disabled.

enable - Specifies that the Option 82 processing will be enabled.

disable - Specifies that the Option 82 processing will be disabled.

check - When the state is enabled, For packets coming from client side, the packet should not have the Option 82's field. If the packet has this option field, it will be dropped. The default setting is disabled.

enable - Specifies that checking will be enabled.

disable - Specifies that checking will be disabled.

policy - Specifies the policy used. This option takes effect only when the check status is disabled. The default setting is set to 'replace'.

replace - Specifies to replace the existing Option 82 field in the packet. The Switch will use its own Option 82 value to replace the old Option 82 value in the packet.

drop - Specifies to discard if the packet has the Option 82 field. If the packet, that comes from the client side, contains an Option 82 value, the packet will be dropped. If the packet, that comes from the client side, doesn't contain an Option 82 value, it will insert its own Option 82 value into the packet.

keep - Specifies to retain the existing Option 82 field in the packet. If the packet, that comes from the client side, contains an Option 82 value, the old Option 82 value will be kept. If the packet, that comes from the client side, doesn't contain an Option 82 value, it will insert its own Option 82 value into the packet.

remote_id - Specifies the content in Remote ID sub-option.

default - Use switch's system MAC address as remote ID.

user_define - Use a user-defined string as remote ID. Spaces are allowed in the string.

<desc 32> - Enter the user-defined description here. This value can be up to 32 characters long.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure DHCP relay Option 82:

```
DGS-3000-28XMP:admin# config dhcp_relay option_82 state enable
Command: config dhcp_relay option_82 state enable

Success.

DGS-3000-28XMP:admin# config dhcp_relay option_82 check disable
Command: config dhcp_relay option_82 check disable

Success.

DGS-3000-28XMP:admin# config dhcp_relay option_82 policy replace
Command: config dhcp_relay option_82 policy replace

Success.

DGS-3000-28XMP:admin# config dhcp_relay option_82 remote_id user_define “D-Link L2 Switch”
Command: config dhcp_relay option_82 remote_id user_define "D-Link L2 Switch"

Success.

DGS-3000-28XMP:admin#
```

24-7 config dhcp_relay option_82 circuit_id

Description

This command is used to configure the circuit ID of DHCP relay agent information Option 82 of the Switch.

Format

config dhcp_relay option_82 circuit_id [default | vendor1]

Parameters

default – Specifies the circuit ID of DHCP relay agent to default. The default circuit ID includes the incoming VLAN ID of the DHCP client packet, the module value of 0, and the number of the port on the Switch that receives the DHCP client packet.
vendor1 - Specifies the circuit ID of DHCP relay agent to vendor1.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the circuit ID as default:

```
DGS-3000-28XMP:admin# config dhcp_relay option_82 circuit_id default
Command: config dhcp_relay option_82 circuit_id default

Success.

DGS-3000-28XMP:admin#
```

24-8 enable dhcp_relay

Description

This command is used to enable the DHCP relay function on the Switch.

Format

enable dhcp_relay

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable the DHCP relay function.

```
DGS-3000-28XMP:admin# enable dhcp_relay
Command: enable dhcp_relay

Success.

DGS-3000-28XMP:admin#
```

24-9 disable dhcp_relay

Description

This command is used to disable the DHCP relay function on the Switch.

Format

disable dhcp_relay

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To disable the DHCP relay function:

```
DGS-3000-28XMP:admin# disable dhcp_relay
Command: disable dhcp_relay

Success.

DGS-3000-28XMP:admin#
```

24-10 show dhcp_relay

Description

This command is used to display the current DHCP relay configuration.

Format

show dhcp_relay {ipif <ipif_name 12>}

Parameters

ipif - (Optional) Specifies the IP interface name. **<ipif_name 12>** - Enter the IP interface name used here. This name can be up to 12 characters long.
If no parameter is specified , the DHCP relay configuration associated with all IP interfaces will be displayed.

Restrictions

None.

Example

To display DHCP relay configuration:

```
DGS-3000-28XMP:admin#show dhcp_relay
Command: show dhcp_relay

DHCP/BOOTP Relay Status         : Enabled
DHCP/BOOTP Hops Count Limit     : 4
DHCP/BOOTP Relay Time Threshold : 0
DHCP Vendor Class Identifier Option 60 State: Disabled
DHCP Client Identifier Option 61 State: Disabled
DHCP Relay Agent Information Option 82 State  : Enabled
DHCP Relay Agent Information Option 82 Check  : Disabled
DHCP Relay Agent Information Option 82 Policy : Replace
DHCP Relay Agent Information Option 82 Circuit ID : Default
DHCP Relay Agent Information Option 82 Remote ID : User Define( "D-Link L2 Switch" )

Interface    Server 1        Server 2        Server 3        Server 4
------------ --------------- --------------- --------------- ---------------
System       10.43.21.12

Server           VLAN ID List
---------------  ------------------------------------------------------------
10.43.21.12      1


DGS-3000-28XMP:admin#
```

24-11 config dhcp_relay option_60 state

Description

This command is used to decide whether DHCP relay will process the DHCP Option 60 or not.

When option_60 is enabled, if the packet does not have Option 60, then the relay servers cannot be determined based on Option 60. The relay servers will be determined based on either Option 61 or per IPIF configured servers.

If the relay servers are determined based on Option 60 or Option 61, then IPIF configured servers will be ignored.

If the relay servers are not determined either by Option 60 or Option 61, then IPIF configured servers will be used to determine the relay servers.

Format

config dhcp_relay option_60 state [enable | disable]

Parameters

enable - Specifies that the Option 60 rule will be enabled.
disable - Specifies that the Option 60 rule will be disabled.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the state of dhcp_relay Option 60:

```
DGS-3000-28XMP:admin# config dhcp_relay option_60 state enable
Command: config dhcp_relay option_60 state enable

Success

DGS-3000-28XMP:admin#
```

24-12 config dhcp_relay option_60 add string

Description

This command is used to configure the Option 60 relay rules. Different strings can be specified within the same relay server, and the same string can be specified with multiple relay servers.

The system will relay the packet to all the matching servers.

Format

config dhcp_relay option_60 add string <multiword 255> relay <ipaddr> [exact-match | partial-match]

Parameters

<multiword 255> - Enter the string value here. This value can be up to 255 characters long.
relay - Specifies a relay server IP address. **<ipaddr>** - Enter the IP address used for this configuration here.
exact-match - Specifies that the Option 60 string in the packet must fully match with the specified string.
partial-match - Specifies that the Option 60 string in the packet only needs a partial match with the specified string.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the DHCP relay Option 60 option:

```
DGS-3000-28XMP:admin# config dhcp_relay option_60 add string "abc" relay 10.90.90.1 exact-
match
Command: config dhcp_relay option_60 add string "abc" relay 10.90.90.1 exact-match

Success.

DGS-3000-28XMP:admin#
```

24-13 config dhcp_relay option_60 default

Description

This command is used to configure the DHCP relay Option 60 default drop option.

When there are no match servers found for the packet based on Option 60, the relay servers will be determined by the default relay server setting.

When drop is specified, the packet with no matching rules found will be dropped without further process.

When relay is specified, the packet will be processed further based on Option 61. The final relay servers will be the union of Option 60 default relay servers and the relay servers determined by Option 61.

Format

config dhcp_relay option_60 default [relay <ipaddr> | mode [relay | drop]]

Parameters

relay - Specifies the IP address used for the DHCP relay forward function. **<ipaddr>** - Enter the IP address used for this configuration here.
mode - Specifies the DHCP relay Option 60 mode. **relay** - Specifies that the packet will be relayed based on the relay rules. **drop** - Specifies to drop the packet that has no matching Option 60 rules.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the DHCP relay Option 60 default drop option:

```
DGS-3000-28XMP:admin# config dhcp_relay option_60 default mode drop
Command: config dhcp_relay option_60 default mode drop

Success.

DGS-3000-28XMP:admin#
```

24-14 config dhcp_relay option_60 delete

Description

This command is used to delete DHCP relay Option 60 entry.

Format

config dhcp_relay option_60 delete [string <multiword 255> {relay <ipaddr>} | ipaddress <ipaddr> | all | default {<ipaddr>}]

Parameters

string - Specifies the DHCP Option 60 string. All entries that match the specified string will be removed. This is

only applicable if the IP address is not specified.

<multiword 255> - Enter the DHCP Option 60 string to be removed here. This value can be up to 255 characters long.

relay - (Optional) Specifies to delete one entry, whose string and IP address are equal to the string and IP address specified by the user.

<ipaddr> - Enter the IP address used for this configuration here.

ipaddress - Specifies to delete all the entry whose IP address is equal to the specified IP address.

<ipaddr> - Enter the IP address used for this configuration here.

all - Specifies to delete all the entries. Default relay servers are excluded.

default - Specifies to delete the default relay IP address that is specified by the user.

<ipaddr> - (Optional) Enter the IP address used for this configuration here.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete the DHCP relay Option 60 string called ‘abc’:

```
DGS-3000-28XMP:admin# config dhcp_relay option_60 delete string "abc" relay 10.90.90.1
Command: config dhcp_relay option_60 delete string "abc" relay 10.90.90.1

Success.

DGS-3000-28XMP:admin#
```

24-15 show dhcp_relay option_60

Description

This command is used to show DHCP relay Option 60 entries specified by the user.

Format

show dhcp_relay option_60 {[string <multiword 255> | ipaddress <ipaddr> | default]}

Parameters

string - (Optional) Specifies to display the entry that contains this string.

<multiword 255> - Enter the string here. This value can be up to 255 characters long.

ipaddress - (Optional) Specifies to display the entry whose IP address equals the specified IP address.

<ipaddr> - Enter the IP address here.

default - (Optional) Specifies to display the default behavior of DHCP relay Option 60.

If no parameter is specified then all the DHCP Option 60 entries will be displayed.

Restrictions

None.

Example

To show DHCP Option 60 information:

```
DGS-3000-28XMP:admin# show dhcp_relay option_60
Command: show dhcp_relay option_60

Default Processing Mode: Drop

Default Servers:

Matching Rules:

String                          Match Type            IP Address
-------                         ---------             ---------
abc                             Exact Match           10.90.90.1

Total Entries : 1

DGS-3000-28XMP:admin#
```

24-16 config dhcp_relay option_61 state

Description

This command is used to decide whether the DHCP relay will process the DHCP Option 61 or not.

When Option 61 is enabled, if the packet does not have Option 61, then the relay servers cannot be determined based on Option 61.

If the relay servers are determined based on Option 60 or Option 61, then IPIF configured servers will be ignored.

If the relay servers are not determined either by Option 60 or Option 61, then IPIF configured servers will be used to determine the relay servers.

Format

config dhcp_relay option_61 state [enable | disable]

Parameters

enable - Specifies to enable the function DHCP relay use Option 61 ruler to relay DHCP packets.
disable - Specifies to disable the function DHCP relay use Option 61 ruler to relay DHCP packets.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the state of DHCP relay Option 61:

```
DGS-3000-28XMP:admin# config dhcp_relay option_61 state enable
Command: config dhcp_relay option_61 state enable

Success

DGS-3000-28XMP:admin#
```

24-17 config dhcp_relay option_61 add

Description

This command is used to add a rule to determine the relay server based on Option 61. The match rule can be based on either MAC address or a user-specified string. Only one relay server can be specified for a MAC-address or a string.

If relay servers are determined based on Option 60, and one relay server is determined based on Option 61, the final relay servers will be the union of these two sets of the servers.

Format

config dhcp_relay option_61 add [mac_address <macaddr> | string <multiword 255>] [relay <ipaddr> | drop]

Parameters

mac_address - Specifies the client's client-ID which is the hardware address of the client. **<macaddr>** - Enter the client's MAC address here.
string - Specifies the client's client-ID, which is specified by the administrator. **<multiword 255>** - Enter the client's description here. This value can be up to 255 characters long.
relay - Specifies to relay the packet to an IP address. **<ipaddr>** - Enter the IP address used for this configuration here.
drop - Specifies to drop the packet.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the DHCP relay Option 61 function:

```
DGS-3000-28XMP:admin# config dhcp_relay option_61 add mac_address 00-11-22-33-44-55 drop
Command: config dhcp_relay option_61 add mac_address 00-11-22-33-44-55 drop

Success

DGS-3000-28XMP:admin#
```

24-18 config dhcp_relay option_61 default

Description

This command is used to configure the default ruler for Option 61.

Format

config dhcp_relay option_61 default [relay <ipaddr> | drop]

Parameters

relay - Specifies to relay the packet that has no option 61 matching rules to an IP address. **<ipaddr>** - Enter the IP address used for this configuration here.
drop - Specifies to drop the packet that have no Option 61 matching rules.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the DHCP relay Option 61 function:

```
DGS-3000-28XMP:admin# config dhcp_relay option_61 default drop
Command: config dhcp_relay option_61 default drop

Success

DGS-3000-28XMP:admin#
```

24-19 config dhcp_relay option_61 delete

Description

This command is used to delete an Option 61 rule.

Format

config dhcp_relay option_61 delete [mac_address <macaddr> | string <multiword 255> | all]

Parameters

mac_address - Specifies the entry with the specified MAC address will be deleted. **<macaddr>** - Enter the MAC address here.
string - Specifies the entry with the specified string will be deleted. **<multiword 255>** - Enter the string value here. This value can be up to 255 characters long.
all - Specifies that all rules excluding the default rule will be deleted.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To remove a DHCP relay Option 61 entry:

```
DGS-3000-28XMP:admin# config dhcp_relay option_61 delete mac_address 00-11-22-33-44-55
Command: config dhcp_relay option_61 delete mac_address 00-11-22-33-44-55

Success

DGS-3000-28XMP:admin#
```

24-20 show dhcp_relay option_61

Description

This command is used to show all rules for Option 61.

Format

show dhcp_relay option_61

Parameters

None.

Restrictions

None.

Example

To display DHCP relay rules for Option 61:

```
DGS-3000-28XMP:admin# show dhcp_relay option_61
Command: show dhcp_relay option_61

Default Relay Rule:Drop

Matching Rules:

Client-ID                    Type               Relay Rule
-----------                  ----               ---------
00-11-22-33-44-55            MAC Address        Drop


Total Entries : 1


DGS-3000-28XMP:admin#
```

Chapter 25 DHCP Server Command List

enable dhcp_server
disable dhcp_server
create dhcp excluded_address begin_address <ipaddr> end_address <ipaddr>
create dhcp pool <pool_name 12>
create dhcp pool manual_binding <pool_name 12> <ipaddr> hardware_address <macaddr> {type [ethernet | ieee802]}
config dhcp pool network_addr <pool_name 12> <network_address>
config dhcp pool domain_name <pool_name 12> {<domain_name 64>}
config dhcp pool dns_server <pool_name 12> {<ipaddr>} {<ipaddr>} {<ipaddr>}
config dhcp pool netbios_name_server <pool_name 12> {<ipaddr>} {<ipaddr>} {<ipaddr>}
config dhcp pool netbios_node_type <pool_name 12> [broadcast | peer_to_peer | mixed | hybrid]
config dhcp pool default_router <pool_name 12> {<ipaddr>} {<ipaddr>} {<ipaddr>}
config dhcp pool lease <pool_name 12> [<day 0-365> <hour 0-23> <minute 0-59> | infinite]
config dhcp pool boot_file <pool_name 12> {<file_name 64>}
config dhcp pool next_server <pool_name 12> {<ipaddr>}
config dhcp ping_packets <number 0-10>
config dhcp ping_timeout <millisecond 10-2000>
clear dhcp binding [<pool_name 12> [<ipaddr> | all] | all]
clear dhcp conflict_ip [<ipaddr> | all]
delete dhcp excluded_address [begin_address <ipaddr> end_address <ipaddr> | all]
delete dhcp pool [<pool_name 12> | all]
delete dhcp pool manual_binding <pool_name 12> [<ipaddr> | all]
show dhcp excluded_address
show dhcp binding {<pool_name 12>}
show dhcp pool {<pool_name 12>}
show dhcp pool manual_binding {<pool_name 12>}
show dhcp_server
show dhcp conflict_ip {<ipaddr>}

25-1 enable dhcp_server

Description

This command is used to enable the DHCP server to distribute IP addresses, subnet masks, gateway addresses, and DNS server addresses to your network.

NOTE: The DHCP server, DHCP client, DHCP relay and the DHCP local relay features are mutually exclusive. This means that if one of these features are enabled on an interface, the other three features mentioned cannot be enabled on that interface.

Format

enable dhcp_server

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable DHCP server:

```
DGS-3000-28XMP:admin#enable dhcp_server
Command: enable dhcp_server

Success.

DGS-3000-28XMP:admin#
```

25-2 disable dhcp_server

Description

This command is used to disable the DHCP server function on the switch.

Format

disable dhcp_server

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To disable the Switch's DHCP server:

```
DGS-3000-28XMP:admin#disable dhcp_server
Command: disable dhcp_server

Success.

DGS-3000-28XMP:admin#
```

25-3 create dhcp excluded_address begin_address

Description

This command is used to create a DHCP server exclude address. The DHCP server assumes that all IP addresses in a DHCP pool subnet are available for assigning to DHCP clients. Use this command to specify the IP address that the DHCP server should not assign to clients. This command can be used multiple times in order to define multiple groups of excluded addresses.

Format

create dhcp excluded_address begin_address <ipaddr> end_address <ipaddr>

Parameters

<ipaddr> - Enter the starting address of the IP address range.
end_address - Specifies the ending address of the IP address range. **<ipaddr>** - Enter the ending address of the IP address range.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To specify the IP address that DHCP server should not assign to clients:

```
DGS-3000-28XMP:admin#create dhcp excluded_address begin_address 10.10.10.1 end_address
10.10.10.10
Command: create dhcp excluded_address begin_address 10.10.10.1 end_address 10.10.10.10

Success.

DGS-3000-28XMP:admin#
```

25-4 create dhcp pool

Description

This command is used to create a DHCP pool by specifying a name. After creating a DHCP pool, use other DHCP pool configuration commands to configure parameters for the pool.

Format

create dhcp pool <pool_name 12>

Parameters

<pool_name 12> - Enter the name of the DHCP pool.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To create a DHCP pool:

```
DGS-3000-28XMP:admin#create dhcp pool engineering
Command: create dhcp pool engineering

Success.

DGS-3000-28XMP:admin#
```

25-5 create dhcp pool manual_binding

Description

This command is used to specify the distinct identification of the client in dotted-hexadecimal notation or hardware address.

An address binding is a mapping between the IP address and MAC address of a client. The IP address of a client can be assigned manually by an administrator or assigned automatically from a pool by a DHCP server.

The IP address specified in the manual binding entry must be in a range within that the network uses for the DHCP pool. If the user specifies a conflict IP address, an error message will be returned. If a number of manual binding entries are created, and the network address for the pool is changed such that conflicts are generated, those manual binding entries which conflict with the new network address will be automatically deleted.

Format

create dhcp pool manual_binding <pool_name 12> <ipaddr> hardware_address <macaddr> {type [ethernet | ieee802]}

Parameters

<pool_name 12> - Enter the DHCP pool name.
<ipaddr> - Enter the IP address which will be assigned to a specified client.
hardware_address - Specifies the hardware MAC address. **<macaddr>** - Enter the MAC address here.
type - (Optional) Specifies the DHCP pool manual binding type. If it's not specified, the type will be “ethernet". **ethernet** - Specifies Ethernet type. **ieee802** - Specifies IEEE 802 type.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure manual bindings:

```
DGS-3000-28XMP:admin#create dhcp pool manual_binding engineering 10.10.10.2 hardware_address
00-80-C8-02-02-02 type ethernet
Command: create dhcp pool manual_binding engineering 10.10.10.2 hardware_address 00-80-C8-
02-02-02 type ethernet

Success.

DGS-3000-28XMP:admin#
```

25-6 config dhcp pool network_addr

Description

This command is used to specify the network for the DHCP pool. The addresses in the network are free to be assigned to the DHCP client. The prefix length specifies the number of bits that comprise the address prefix. The prefix is an alternative way of specifying the network mask of the client. The prefix length must be preceded by a forward slash (/). When the DHCP server receives a request from the client, the server will automatically find a pool to allocate the address. If the request is relayed to the server by the intermediate device, the server will match the gateway IP address carried in the packet against the network of each DHCP pool. The pool which has the longest match will be selected. If the request packet is not through relay, then the server will match the IP address of the IPIF that received the request packet against the network of each DHCP pool.

Format

config dhcp pool network_addr <pool_name 12> <network_address>

Parameters

<pool_name 12> - Enter the DHCP pool name.
<network_address> - Enter the IP address that the DHCP server may assign to clients.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the address range of the DHCP address pool:

```
DGS-3000-28XMP:admin#config dhcp pool network_addr engineering 10.10.10.0/24
Command: config dhcp pool network_addr engineering 10.10.10.0/24

Success.

DGS-3000-28XMP:admin#
```

25-7 config dhcp pool domain_name

Description

This command is used to specify the domain name for the client if the server allocates the address for the client from this pool. The domain name configured here will be used as the default domain name by the client. By default, the domain name is empty. If the domain name is empty, the domain name information will not be provided to the client.

Format

config dhcp pool domain_name <pool_name 12> {<domain_name 64>}

Parameters

<pool_name 12> - Enter the DHCP pool name.
<domain_name 64> - (Optional) Enter the domain name of the client.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the domain name option of the DHCP pool:

```
DGS-3000-28XMP:admin#config dhcp pool domain_name engineering abc.com
Command: config dhcp pool domain_name engineering abc.com

Success.

DGS-3000-28XMP:admin#
```

25-8 config dhcp pool dns_server

Description

This command is used to specify the IP address of a DNS server that is available to a DHCP client. Up to three IP addresses can be specified on one command line. If DNS server is not specified, the DNS server information will not be provided to the client. If this command is input twice for the same pool, the second command will overwrite the first command.

Format

config dhcp pool dns_server <pool_name 12> {<ipaddr>} {<ipaddr>} {<ipaddr>}

Parameters

<pool_name 12> - Enter the DHCP pool name.
<ipaddr> - (Optional) Enter the IP address of the DNS server. Up to three IP addresses can be specified on one command line.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the IP address of the DNS server:

```
DGS-3000-28XMP:admin#config dhcp pool dns_server engineering 10.10.10.1
Command: config dhcp pool dns_server engineering 10.10.10.1

Success.

DGS-3000-28XMP:admin#
```

25-9 config dhcp pool netbios_name_server

Description

This command is used to specify the NetBIOS WINS server that is available to a Microsoft DHCP client. Up to three IP addresses can be specified on one command line.

Windows Internet Naming Service (WINS) is a name resolution service that Microsoft DHCP clients use to correlate host names to IP addresses within a general grouping of networks. If a NetBIOS name server is not specified, the NetBIOS name server information will not be provided to the client. If this command is input twice for the same pool, the second command will overwrite the first command.

Format

config dhcp pool netbios_name_server <pool_name 12> {<ipaddr>} {<ipaddr>} {<ipaddr>}

Parameters

<pool_name 12> - Enter the DHCP pool name.
<ipaddr> - (Optional) Enter the IP address of the WINS server. Up to three IP addresses can be specified on one command line.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure a WINS server IP address:

```
DGS-3000-28XMP:admin#config dhcp pool netbios_name_server engineering 10.10.10.5
Command: config dhcp pool netbios_name_server engineering 10.10.10.5

Success.

DGS-3000-28XMP:admin#
```

25-10 config dhcp pool netbios_node_type

Description

This command is used to specify the NetBIOS node type for a Microsoft DHCP client.

The NetBIOS node type for Microsoft DHCP clients can be one of four settings: broadcast, peer-to-peer, mixed, or hybrid. Use this command to configure a NetBIOS over TCP/IP device that is described in RFC 1001/1002. By default, the NetBIOS node type is broadcast.

Format

config dhcp pool netbios_node_type <pool_name 12> [broadcast | peer_to_peer | mixed | hybrid]

Parameters

<pool_name 12> - Enter the DHCP pool name.
broadcast - Specifies the NetBIOS node type for Microsoft DHCP clients as broadcast.
peer_to_peer - Specifies the NetBIOS node type for Microsoft DHCP clients as peer_to_peer.
mixed - Specifies the NetBIOS node type for Microsoft DHCP clients as mixed.
hybrid - Specifies the NetBIOS node type for Microsoft DHCP clients as hybrid.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the NetBIOS node type:

```
DGS-3000-28XMP:admin#config dhcp pool netbios_node_type engineering hybrid
Command: config dhcp pool netbios_node_type engineering hybrid

Success.

DGS-3000-28XMP:admin#
```

25-11 config dhcp pool default_router

Description

This command is used to specify the IP address of the default router for a DHCP client. Up to three IP addresses can be specified on one command line.

After a DHCP client has booted, the client begins sending packets to its default router. The IP address of the default router should be on the same subnet as the client. If the default router is not specified, the default router information will not be provided to the client. If this command is input twice for the same pool, the second command will overwrite the first command. The default router must be within the range the network defined for the DHCP pool.

Format

config dhcp pool default_router <pool_name 12> {<ipaddr>} {<ipaddr>} {<ipaddr>}

Parameters

<pool_name 12> - Enter the DHCP pool name.
<ipaddr> - (Optional) Enter the IP address of the default router. Up to three IP addresses can be specified on one command line.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the default router:

```
DGS-3000-28XMP:admin#config dhcp pool default_router engineering 10.10.10.10
Command: config dhcp pool default_router engineering 10.10.10.10

Success.

DGS-3000-28XMP:admin#
```

25-12 config dhcp pool lease

Description

This command is used to specify the duration of the DHCP pool lease.

By default, each IP address assigned by a DHCP server comes with a one-day lease, which is the amount of time that the address is valid.

Format

config dhcp pool lease <pool_name 12> [<day 0-365> <hour 0-23> <minute 0-59> | infinite]

Parameters

<pool_name 12> - Enter the DHCP pool's name.
<day 0-365> - Enter the number of days of the lease.
<hour 0-23> - Enter the number of hours of the lease.
<minute 0-59> - Enter the number of minutes of the lease.
infinite - Specifies a lease of unlimited duration.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the lease of a pool:

```
DGS-3000-28XMP:admin#config dhcp pool lease engineering infinite
Command: config dhcp pool lease engineering infinite

Success.

DGS-3000-28XMP:admin#
```

25-13 config dhcp pool boot_file

Description

This command is used to specify the name of the file that is used as a boot image.

The boot file is used to store the boot image for the client. The boot image is generally the operating system the client uses to load. If this command is input twice for the same pool, the second command will overwrite the first command. If the bootfile is not specified, the boot file information will not be provided to the client.

Format

config dhcp pool boot_file <pool_name 12> {<file_name 64>}

Parameters

<pool_name 12> - Enter the DHCP pool name.
<file_name 64> - (Optional) Enter the file name of the boot image.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the boot file:

```
DGS-3000-28XMP:admin#config dhcp pool boot_file engineering boot.had
Command: config dhcp pool boot_file engineering boot.had

Success.

DGS-3000-28XMP:admin#
```

25-14 config dhcp pool next_server

Description

This command is used by the DHCP client boot process, typically a TFTP server. If next server information is not specified, it will not be provided to the client. If this command is input twice for the same pool, the second command will overwrite the first command.

Format

config dhcp pool next_server <pool_name 12> {<ipaddr>}

Parameters

<pool_name 12> - Enter the DHCP pool name.
<ipaddr> - (Optional) Enter the IP address of the next server.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the next server:

```
DGS-3000-28XMP:admin#config dhcp pool next_server engineering 192.168.0.1
Command: config dhcp pool next_server engineering 192.168.0.1

Success.

DGS-3000-28XMP:admin#
```

25-15 config dhcp ping_packets

Description

This command is used to specify the number of ping packets the DHCP server sends to an IP address before assigning this address to a requesting client.

By default, the DHCP server pings a pool address twice before assigning the address to a DHCP client. If the ping is unanswered, the DHCP server assumes (with a high probability) that the address is not in use and assigns the address to the requesting client. If the ping is answered, the server will discard the current IP address and try another IP address.

Format

config dhcp ping_packets <number 0-10>

Parameters

<number 0-10> - Enter the number of ping packets. 0 means there is no ping test. The default value is 2.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure ping packets:

```
DGS-3000-28XMP:admin#config dhcp ping_packets 4
Command: config dhcp ping_packets 4

Success.

DGS-3000-28XMP:admin#
```

25-16 config dhcp ping_timeout

Description

This command is used to specify the amount of time the DHCP server must wait before timing out a ping packet.

Format

config dhcp ping_timeout <millisecond 10-2000>

Parameters

<millisecond 10-2000> - Enter the amount of time the DHCP server must wait before timing out a ping packet. The default value is 100.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the time out value for ping packets:

```
DGS-3000-28XMP:admin#config dhcp ping_timeout 500
Command: config dhcp ping_timeout 500

Success.

DGS-3000-28XMP:admin#
```

25-17 clear dhcp binding

Description

This command is used to clear a binding entry or all binding entries in a pool or clears all binding entries in all pools. Note that this command will not clear the dynamic binding entry which matches a manual binding entry.

Format

clear dhcp binding [<pool_name 12> [<ipaddr> | all] | all]

Parameters

<pool_name 12> - Enter the DHCP pool name to clear.
<ipaddr> - Enter the IP address to clear.
all - Specifies to clear all IP addresses for the specified pool.

all - Specifies to clear all binding entries in all pools

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To clear dynamic binding entries in the pool named “engineering”:

```
DGS-3000-28XMP:admin#clear dhcp binding engineering 10.48.74.121
Command: clear dhcp binding engineering 10.48.74.121

Success.

DGS-3000-28XMP:admin#
```

25-18 clear dhcp conflict_ip

Description

This command is used to clear an entry or all entries from the conflict IP database.

Format

clear dhcp conflict_ip [<ipaddr> | all]

Parameters

<ipaddr> - Enter the IP address to be cleared.
all - Specifies that all IP addresses will be cleared.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To clear an IP address 10.20.3.4 from the conflict database:

```
DGS-3000-28XMP:admin#clear dhcp conflict_ip 10.20.3.4
Command: clear dhcp conflict_ip 10.20.3.4

Success.

DGS-3000-28XMP:admin#
```

25-19 delete dhcp excluded_address

Description

This command is used to delete a DHCP server exclude address.

Format

delete dhcp excluded_address [begin_address <ipaddr> end_address <ipaddr> | all]

Parameters

begin_address - Specifies the starting address of the IP address range. **<ipaddr>** - Enter the starting address of the IP address range. **end_address** - Specifies the ending address of the IP address range. **<ipaddr>** - Enter the ending address of the IP address range.
all - Specifies to delete all IP addresses.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete a DHCP server exclude address:

```
DGS-3000-28XMP:admin#delete dhcp excluded_address begin_address 10.10.10.1 end_address
10.10.10.10
Command: delete dhcp excluded_address begin_address 10.10.10.1 end_address 10.10.10.10

Success.

DGS-3000-28XMP:admin#
```

25-20 delete dhcp pool

Description

This command is used to delete a DHCP pool.

Format

delete dhcp pool [<pool_name 12> | all]

Parameters

<pool_name 12> - Enter the name of the DHCP pool.
all - Specifies to delete all the DHCP pools.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete a DHCP pool:

```
DGS-3000-28XMP:admin#delete dhcp pool engineering
Command: delete dhcp pool engineering

Success.

DGS-3000-28XMP:admin#
```

25-21 delete dhcp pool manual_binding

Description

This command is used to delete DHCP server manual binding.

Format

delete dhcp pool manual_binding <pool_name 12> [<ipaddr> | all]

Parameters

<pool_name 12> - Enter the DHCP pool name.
<ipaddr> - Enter the IP address which will be assigned to a specified client.
all - Specifies to delete all IP addresses.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete DHCP server manual binding:

```
DGS-3000-28XMP:admin#delete dhcp pool manual_binding engineering 10.10.10.1
Command: delete dhcp pool manual_binding engineering 10.10.10.1

Success.

DGS-3000-28XMP:admin#
```

25-22 show dhcp excluded_address

Description

This command is used to display the groups of IP addresses which are excluded from being a legal assigned IP address.

Format

show dhcp excluded_address

Parameters

None.

Restrictions

None.

Example

To display the DHCP server excluded addresses:

```
DGS-3000-28show dhcp excluded_address
Command: show dhcp excluded_address

 Index  Begin Address    End Address
 -----  ------------     ------------
  1     192.168.0.1      192.168.0.100
  2     10.10.10.1       10.10.10.10

 Total Entries: 2


DGS-3000-28XMP:admin#
```

25-23 show dhcp binding

Description

This command is used to display dynamic binding entries.

Format

show dhcp binding {<pool_name 12>}

Parameters

<pool_name 12> - (Optional) Enter a DHCP pool name.

Restrictions

None.

Example

To display dynamic binding entries for “engineering”:

```
DGS-3000-28XMP:admin#show dhcp binding engineering
Command: show dhcp binding engineering

Pool Name    IP Address      Hardware Address  Type     Status    Lifetime
------------ --------------- ----------------- -------- --------- -------------
engineering  192.168.0.1     00-80-C8-08-13-88 Ethernet Manual    86400
engineering  192.168.0.2     00-80-C8-08-13-99 Ethernet Automatic 86400
engineering  192.168.0.3     00-80-C8-08-13-A0 Ethernet Automatic 86400
engineering  192.168.0.4     00-80-C8-08-13-B0 Ethernet Automatic 86400

 Total Entries: 0

DGS-3000-28XMP:admin#
```

25-24 show dhcp pool

Description

This command is used to display the information for DHCP pool. If pool name is not specified, information for all pools will be displayed.

Format

show dhcp pool {<pool_name 12>}

Parameters

<pool_name 12> - (Optional) Enter the DHCP pool name.

Restrictions

None.

Example

To display the current DHCP pool information for “engineering”:

```
DGS-3000-28XMP:admin#show dhcp pool engineering
Command: show dhcp pool engineering

 Pool Name              :engineering
 Network Address        :10.10.10.0/24
 Domain Name            :abc.com
 DNS Server             :10.10.10.1
 NetBIOS Name Server    :10.10.10.5
 NetBIOS Node Type      :Hybrid
 Default Router         :10.10.10.10
 Pool Lease             :Infinite
 Boot File              :boot.had
 Next Server            :192.168.0.1


 Total Entries: 1


DGS-3000-28XMP:admin#
```

25-25 show dhcp pool manual_binding

Description

This command is used to display the configured manual binding entries.

Format

show dhcp pool manual_binding {<pool_name 12>}

Parameters

<pool_name 12> - (Optional) Enter the DHCP pool name.

Restrictions

None.

Example

To display the configured manual binding entries:

```
DGS-3000-28XMP:admin#show dhcp pool manual_binding
Command: show dhcp pool manual_binding

 Pool Name    IP Address             Hardware Address              Type
 ---------    ---------              ------------------------      ---------
 engineering  10.10.10.20            00-11-22-33-44-55             ethernet

  Total Entries: 1


DGS-3000-28XMP:admin#
```

25-26 show dhcp_server

Description

This command is used to display the current DHCP server configuration.

Format

show dhcp_server

Parameters

None.

Restrictions

None.

Example

To display the DHCP server status:

```
DGS-3000-28XMP:admin#show dhcp_server
Command: show dhcp_server

  DHCP Server Global State: Enabled
  Ping Packet Number      : 4
  Ping Timeout            : 500 ms


DGS-3000-28XMP:admin#
```

25-27 show dhcp conflict_ip

Description

This command is used to display the IP address that has been identified as being in conflict.

The DHCP server will use ping packet to determine whether an IP address is conflicting with other hosts before binding this IP. The IP address which has been identified in conflict will be moved to the conflict IP database. The system will not attempt to bind the IP address in the conflict IP database unless the user clears it from the conflict IP database.

Format

show dhcp conflict_ip {<ipaddr>}

Parameters

<ipaddr> - (Optional) Enter the IP address to be displayed.

Restrictions

None.

Example

To display the entries in the DHCP conflict IP database:

```
DGS-3000-28XMP:admin#show dhcp conflict_ip
Command: show dhcp conflict_ip

  IP Address           Detection Method      Detection Time
 ------------          ----------------      ----------------
 172.16.1.32           Ping                  2007/08/30 17:06:59
 172.16.1.32           Gratuitous ARP        2007/09/10 19:38:01

 Total Entries: 2

DGS-3000-26TC:admin#
```

Chapter 26 DHCP Server Screening Command List

create filter dhcpv6_server permit sip <ipv6addr> ports [<portlist> | all]
create filter icmpv6_ra_all_node permit sip <ipv6addr> ports [<portlist> | all]
config filter dhcp_server [add permit server_ip <ipaddr> {client_mac <macaddr>} ports [<portlist> | all] | delete permit server_ip <ipaddr> {client_mac <macaddr>} ports [<portlist> | all] | ports [<portlist> | all] {vlanid <vid_list>} state [enable | disable] | illegal_server_log_suppress_duration [1min | 5min | 30min] | trap [enable | disable] | log [enable | disable]]
config filter dhcpv6_server ports [<portlist> | all] {vlanid <vid_list>} state [enable | disable]
config filter dhcpv6_server trap [enable | disable]
config filter dhcpv6_server log [enable | disable]
config filter icmpv6_ra_all_node ports [<portlist> | all] state [enable | disable]
config filter icmpv6_ra_all_node trap [enable | disable]
config filter icmpv6_ra_all_node log [enable | disable]
delete filter dhcpv6_server permit sip <ipv6addr>
delete filter icmpv6_ra_all_node permit sip <ipv6addr>
show filter dhcp_server {ports <portlist>}
show filter dhcpv6_server {ports <portlist>}
show filter icmpv6_ra_all_node

26-1 create filter dhcpv6_server permit sip

Description

This command is used to create a permit entry for DHCPv6 server filtering. The specific DHCPv6 server packets, with the source IPv6 address, will be forwarded on the specified port(s).

Format

create filter dhcpv6_server permit sip <ipv6addr> ports [<portlist> | all]

Parameters

<ipv6addr> - Enter the source address of the entry which will be created into the Filter DHCPv6 server forward list.
ports - Specifies the list of ports used for this configuration. **<portlist>** - Enter the list of ports, used for this configuration, here. **all** - Specifies that all ports will be used for this configuration.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To create a Filter DHCPv6 server permit entry on port 5:

```
DGS-3000-28XMP:admin#create filter dhcpv6_server permit sip 2200::5 ports 5
Command: create filter dhcpv6_server permit sip 2200::5 ports 5

Success.

DGS-3000-28XMP:admin#
```

26-2 create filter icmpv6_ra_all_node permit sip

Description

This command is used to create a permit entry. The specific ICMPv6 RA All-nodes packets with source IPv6 address can be forwarded on the specified port(s).

Format

create filter icmpv6_ra_all_node permit sip <ipv6addr> ports [<portlist> | all]

Parameters

<ipv6addr> - Enter the source address of entry which will be created into the Filter ICMPv6 RA All-nodes forward list.
ports - Specifies a list of ports which apply to icmpv6_ra_all_node permit entry. **<portlist>** - Enter a range of ports that the permit entry will apply to. **all** - Specifies all the existing ports that apply to the permit entry.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To create a filter ICMPv6 RA All-nodes permit entry on port 5:

```
DGS-3000-28XMP:admin#create filter icmpv6_ra_all_node permit sip 2200::5 ports 5
Command: create filter icmpv6_ra_all_node permit sip 2200::5 ports 5

Success.

DGS-3000-28XMP:admin#
```

26-3 config filter dhcp_server

Description

This command is used to configure DHCP server screening.

With DHCP server screening function, illegal DHCP server packets will be filtered. This command is used to configure the state of the DHCP server packet filtering function and to add/delete the DHCP server binding entry.

This command is useful for projects that support per-port control of the DHCP server screening function. The filter can be based on the DHCP server IP address.

The command has two purposes: To specify to filter all DHCP server packets on the specific port and to specify to allow some DHCP server packets with pre-defined server IP addresses. With this function, we can restrict the DHCP server to service specific DHCP clients. This is useful when two DHCP servers are present on the network, one of them provides the private IP address, and one of them provides the IP address.

Enabling filtering of the DHCP server port state will create one access profile and create one access rule per port (UDP port = 67). Filter commands in this file will share the same access profile.

Addition of a permit DHCP entry will create one access profile and create one access rule. Filtering commands in this file will share the same access profile.

Format

config filter dhcp_server [add permit server_ip <ipaddr> {client_mac <macaddr>} ports [<portlist> | all] | delete permit server_ip <ipaddr> {client_mac <macaddr>} ports [<portlist> | all] | ports [<portlist> | all] {vlanid <vid_list>} state [enable | disable] | illegal_server_log_suppress_duration [1min | 5min | 30min] | trap [enable | disable] | log [enable | disable]]

Parameters

add - Specifies to add a DHCP filter.
- **permit** - Specifies a permission DHCP filter.
  - **server_ip** - Specifies the IP address of the DHCP server to be filtered.
    - **<ipaddr>** - Enter the DHCP server IP address here.
  - **client_mac** - (Optional) Specifies the MAC address of the DHCP client.
    - **<macaddr>** - Enter the DHCP client MAC address here.
  - **ports** - Specifies the port number of filter DHCP server.
    - **<portlist>** - Enter the list of ports to be configured here.
    - **all** - Specifies that all the port will be used for this configuration.

delete - Specifies to delete the DHCP filter.
- **permit** - Specifies the permission DHCP filter.
  - **server_ip** - Specifies the IP address of the DHCP server to be filtered.
    - **<ipaddr>** - Enter the DHCP server IP address here.
  - **client_mac** - (Optional) Specifies the MAC address of the DHCP client.
    - **<macaddr>** - Enter the DHCP client MAC address here.
  - **ports** - Specifies the port number of filter DHCP server.
    - **<portlist>** - Enter the list of ports to be configured here.
    - **all** - Specifies that all the port will be used for this configuration.

ports - Specifies the port number of filter DHCP server.
- **<portlist>** - Enter the list of ports to be configured here.
- **all** - Specifies that all the port will be used for this configuration.
- **vlanid** - (Optional) Specifies VLAN IDs. When ports are enabled and the VLAN is specified, ingress DHCP server packets containing the enabled VLAN ID will be checked. Packets not containing the enabled VLAN ID will be bypassed. When ports are enabled and the VLAN is not specified, all ingress DHCPv6 server packets will be checked.
  - **<vid_list>** - Enter the list of VLANs to be configured here.
- **state** - Specifies to enable or disable the filter DHCP server state.
  - **enable** - Specifies that the filter DHCP server state will be enabled.
  - **disable** - Specifies that the filter DHCP server state will be disabled.

illegal_server_log_suppress_duration - Specifies the same illegal DHCP server IP address detected will be logged only once within the duration. The default value is 5 minutes.

1min - Specifies that illegal server log suppress duration value will be set to 1 minute.

5min - Specifies that illegal server log suppress duration value will be set to 5 minutes.

30min - Specifies that illegal server log suppress duration value will be set to 30 minutes.

trap - Specifies to enable or disable the trap function.

enable - Specifies to enable the trap function.

disable - Specifies to disable the trap function.

log - Specifies to enable or disable the log function.

enable - Specifies to enable the log function.

disable - Specifies to disable the log function.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To add an entry from the DHCP server filter list in the Switch's database:

```
DGS-3000-28XMP:admin#config filter dhcp_server add permit server_ip 10.1.1.1 client_mac 00-
00-00-00-00-01 port 1-26
Command: config filter dhcp_server add permit server_ip 10.1.1.1 client_mac 00-00-00-00-00-01
ports 1-26

Success.

DGS-3000-28XMP:admin#
```

26-4 config filter dhcpv6_server ports

Description

This command is used to configure the state of filter DHCPv6 server packets on the switch. The filter DHCPv6 server function is used to filter the DHCPv6 server packets on the specific port(s) and receive the trust packets from the specific source. This feature can be protected network usable when a malicious host sends the DHCPv6 server packets.

Format

config filter dhcpv6_server ports [<portlist> | all] {vlanid <vid_list>} state [enable | disable]

Parameters

<portlist> - Enter a range of ports to configure the Filter DHCPv6 server state.

all - Specifies all the existing ports on the switch for configuring the Filter DHCPv6 server state.

vlanid - (Optional) Specifies VLAN IDs. When ports are enabled and the VLAN is specified, ingress DHCPv6 server packets containing the enabled VLAN ID will be checked. Packets not containing the enabled VLAN ID will be bypassed. When ports are enabled and the VLAN is not specified, all ingress DHCPv6 server packets will be checked.

<vid_list> - Enter the list of VLANs to be configured here.

state - Specifies whether the port's filter DHCPv6 server function is enabled or disabled.

enable - Specifies that the filter option is enabled.

disable - Specifies that the filter option is disabled.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure enabling all port states:

```
DGS-3000-28XMP:admin#config filter dhcpv6_server ports all state enable
Command: config filter dhcpv6_server ports all state enable

Success.

DGS-3000-28XMP:admin#
```

26-5 config filter dhcpv6_server trap

Description

This command is used to enable or disable the filter DHCPv6 server trap state.

Format

config filter dhcpv6_server trap [enable | disable]

Parameters

enable - Specifies that the trap for the filter DHCPv6 server will be enabled. The trap for filter DHCPv6 server will be sent out.
disable - Specifies that the trap for the filter DHCPv6 server will be disabled.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable the filter DHCPv6 server trap state:

```
DGS-3000-28XMP:admin#config filter dhcpv6_server trap enable
Command: config filter dhcpv6_server trap enable

Success.

DGS-3000-28XMP:admin#
```

26-6 config filter dhcpv6_server log

Description

This command is used to enable or disable the Filter DHCPv6 server log state.

Format

config filter dhcpv6_server log [enable | disable]

Parameters

enable - Specifies that the log for the Filter DHCPv6 server will be enabled. The log for Filter DHCPv6 server will be generated.
disable - Specifies that the log for the Filter DHCPv6 server will be disabled.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable the Filter DHCPv6 Server log state:

```
DGS-3000-28XMP:admin#config filter dhcpv6_server log enable
Command: config filter dhcpv6_server log enable

Success.

DGS-3000-28XMP:admin#
```

26-7 config filter icmpv6_ra_all_node ports

Description

This command is used to configure the state of the filter ICMPv6 RA all-nodes packets on the switch. The filter ICMPv6 RA all-nodes function is used to filter the ICMPv6 RA all-nodes packets on the specific port(s) and receive the trust packets from the specific source. This feature can be protected network usable when a malicious host sends ICMPv6 RA all-nodes packets.

NOTE: It only needs to filter the packet of which the destination address is the all-nodes multicast address (FF02::1).

Format

config filter icmpv6_ra_all_node ports [<portlist> | all] state [enable | disable]

Parameters

<portlist> - Enter a range of ports for configuring the Filter icmpv6_ra_all_node state.
all - Specifies all the existing ports on the switch for configuring the Filter icmpv6_ra_all_node state.
state - Specifies whether the port's filter ICMPv6 RA all-nodes packets function is enabled or disabled. **enable** - Specifies that the filter ICMPv6 RA all-nodes packets function is be enabled. **disable** - Specifies that the filter ICMPv6 RA all-nodes packets function is be disabled.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable the filter ICMPv6 RA all-nodes state for port 1:

```
DGS-3000-28XMP:admin#config filter icmpv6_ra_all_node ports 1 state enable
Command: config filter icmpv6_ra_all_node ports 1 state enable

Success.

DGS-3000-28XMP:admin#
```

26-8 config filter icmpv6_ra_all_node trap

Description

This command is used to enable or disable the filter ICMPv6 RA all-nodes trap state. If the ICMPv6 RA all-nodes server trap state is disabled, no trap will be sent out.

Format

config filter icmpv6_ra_all_node trap [enable | disable]

Parameters

enable - Specifies that the trap for the filter ICMPv6 RA all-nodes will be enabled. The trap for filter ICMPv6 RA all-nodes will be sent out.
disable - Specifies that the trap for the filter ICMPv6 RA all-nodes will be disabled.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable the filter ICMPv6 RA all-nodes trap state:

```
DGS-3000-28XMP:admin#config filter icmpv6_ra_all_node trap enable
Command: config filter icmpv6_ra_all_node trap enable

Success.

DGS-3000-28XMP:admin#
```

26-9 config filter icmpv6_ra_all_node log

Description

This command is used to enable or disable the filter ICMPv6 RA All-nodes log state.

Format

config filter icmpv6_ra_all_node log [enable | disable]

Parameters

enable - Specifies that the log for the filter ICMPv6 RA will be enabled. The log for filter ICMPv6 RA all-nodes will be generated.
disable - Specifies that the log for the filter ICMPv6 RA will be disabled.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable the filter ICMPv6 RA all-nodes log state:

```
DGS-3000-28XMP:admin#config filter icmpv6_ra_all_node log enable
Command: config filter icmpv6_ra_all_node log enable

Success.

DGS-3000-28XMP:admin#
```

26-10 delete filter dhcpv6_server permit sip

Description

This command is used to delete a filter DHCPv6 server permit entry.

Format

delete filter dhcpv6_server permit sip <ipv6addr>

Parameters

<ipv6addr> - Enter the source IPv6 address of the entry here.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete permit entry from the filter DHCPv6 server forward list:

```
DGS-3000-28XMP:admin#delete filter dhcpv6_server permit sip 2200::4
Command: delete filter dhcpv6_server permit sip 2200::4

Success.

DGS-3000-28XMP:admin#
```

26-11 delete filter icmpv6_ra_all_node permit sip

Description

This command is used to delete a filter ICMPv6 RA all-nodes permit entry.

Format

delete filter icmpv6_ra_all_node permit sip <ipv6addr>

Parameters

<ipv6addr> - Enter the source IPv6 address of the entry which will be deleted in the filter ICMPv6 RA all-nodes forward list.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete permit entry from the filter ICMPv6 RA all-nodes forward list:

```
DGS-3000-28XMP:admin#delete filter icmpv6_ra_all_node permit sip 2200::4
Command: delete filter icmpv6_ra_all_node permit sip 2200::4

Success.

DGS-3000-28XMP:admin#
```

26-12 show filter dhcp_server

Description

This command is used to display the DHCP server filter list created on the Switch.

Format

show filter dhcp_server {ports <portlist>}

Parameters

ports - (Optional) Specifies the list of ports to be displayed.
<portlist> - Enter the list of ports.

Restrictions

None.

Example

To display the DHCP server/client filter list created on the Switch:

```
DGS-3000-28XMP:admin#show filter dhcp_server
Command: show filter dhcp_server

Enabled Ports:
Trap State: Disabled
Log  State: Disabled
Illegal Server Log Suppress Duration:5 minutes

Permit DHCP Server/Client Table:
Server IP Address Client MAC Address  Port
----------------- ------------------  --------------------
10.1.1.1          00-00-00-00-00-01   1-26
10.90.90.20       All Client MAC      1-20

 Total Entries: 2


DGS-3000-28XMP:admin#
```

To display the DHCP server/client configuration on port 1-5:

```
DGS-3000-28XMP:admin#show filter dhcp_server ports 1-5
Command: show filter dhcp_server ports 1-5


Ports  State    Enabled VLANs
------ -------- ----------------------------------------
1      Disabled -
2      Enabled  1
3      Enabled  1
4      Enabled  1
5      Enabled  1

DGS-3000-28XMP:admin#
```

26-13 show filter dhcpv6_server

Description

This command is used to display the filter DHCPv6 server information.

Format

show filter dhcpv6_server {ports <portlist>}

Parameters

ports - (Optional) Specifies the list of ports to be displayed.
<portlist> - Enter the list of ports.

Restrictions

None.

Example

To display filter DHCPv6 server information:

```
DGS-3000-28XMP:admin#show filter dhcpv6_server
Command: show filter dhcpv6_server

Enabled ports:1-28
Trap State: Enabled
Log  State: Enabled

Permit Source Address Table:
Source IP Address                       Port
--------------------------------------  ---------------
 2200::5                                 5

Total Entries:1

DGS-3000-28XMP:admin#
```

To display the DHCP server/client configuration on port 1-5:

```
DGS-3000-28XMP:admin#show filter dhcpv6_server ports 1-5
Command: show filter dhcpv6_server ports 1-5

Ports  State      Enabled VLANs
------ --------   --------------------------------
1      Enabled    1
2      Enabled    -
3      Enabled    -
4      Enabled    -
5      Enabled    -


DGS-3000-28XMP:admin#
```

26-14 show filter icmpv6_ra_all_node

Description

This command is used to display the filter ICMPv6 RA all-nodes information.

Format

show filter icmpv6_ra_all_node

Parameters

None.

Restrictions

None.

Example

To display filter ICMPv6 RA all-nodes information:

```
DGS-3000-28XMP:admin#show filter icmpv6_ra_all_node
Command: show filter icmpv6_ra_all_node

Enabled ports:1
Trap State: Enabled
Log  State: Enabled

Permit Source Address Table:
Source IP Address                       Port
--------------------------------------  ---------------
 2200::5                                 5

Total Entries:1

DGS-3000-28XMP:admin#
```

Chapter 27 DHCPv6 Relay Command List

enable dhcpv6_relay
enable dhcpv6_local_relay
disable dhcpv6_relay
disable dhcpv6_local_relay
config dhcpv6_relay [add | delete] ipif <ipif_name 12> <ipv6addr>
config dhcpv6_relay hop_count <value 1-32>
config dhcpv6_relay ipif [<ipif_name 12> | all] state [enable | disable]
config dhcpv6_local_relay vlan [<vlan_name 32> | vlanid <vlan_id>] state [enable | disable]
config dhcpv6_relay option_18 {state [enable | disable] | check [enable | disable] | interface_id [default | cid | vendor1 | vendor2]}(1)
config dhcpv6_relay option_37 {state [enable | disable] | check [enable | disable] | remote_id [default | cid_with_user_define <desc 128> | user_define <desc 128> | vendor1]}(1)
config dhcpv6_relay port [<portlist> | all] state [enable | disable]
show dhcpv6_relay {ipif <ipif_name 12>}
show dhcpv6_local_relay
show dhcpv6_relay port {<portlist>}
debug dhcpv6_relay state enable
debug dhcpv6_relay state disable
debug dhcpv6_relay output [buffer | console]
debug dhcpv6_relay packet [all | receiving | sending] state [enable | disable]
debug dhcpv6_relay hop_count state [enable | disable]

27-1 enable dhcpv6_relay

Description

This command is used to enable the DHCPv6 relay function on the Switch.

Format

enable dhcpv6_relay

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the DHCPv6 relay global state to enable:

```
DGS-3000-28XMP:admin#enable dhcpv6_relay
Command: enable dhcpv6_relay

Success.

DGS-3000-28XMP:admin#
```

27-2 disable dhcpv6_relay

Description

This command is used to disable the DHCPv6 relay function on the Switch.

Format

disable dhcpv6_relay

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the DHCPv6 relay global state to disable:

```
DGS-3000-28XMP:admin#disable dhcpv6_relay
Command: disable dhcpv6_relay

Success.

DGS-3000-28XMP:admin#
```

27-3 enable dhcpv6_local_relay

Description

This command is used to enable the DHCPv6 local relay function of the Switch.

Format

enable dhcpv6_local_relay

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the DHCPv6 local relay global state to enable:

```
DGS-3000-28XMP:admin#enable dhcpv6_local_relay
Command: enable dhcpv6_local_relay

Success.

DGS-3000-28XMP:admin#
```

27-4 disable dhcpv6_local_relay

Description

This command is used to disable the DHCPv6 local relay function of the switch

Format

disable dhcpv6_local_relay

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the DHCPv6 local relay global state to disable:

```
DGS-3000-28XMP:admin#disable dhcpv6_local_relay
Command: disable dhcpv6_local_relay

Success.

DGS-3000-28XMP:admin#
```

27-5 config dhcpv6_relay

Description

This command is used to add/delete an IPv6 address which is a destination to forward (relay) DHCPv6 packets.

Format

config dhcpv6_relay [add | delete] ipif <ipif_name 12> <ipv6addr>

Parameters

add - Specifies to add an IPv6 destination to the DHCPv6 relay table.
delete - Specifies to Delete an IPv6 destination from the DHCPv6 relay table.

ipif - Specifies the name of the IP interface in which DHCPv6 relay is to be enabled.
<ipif_name 12> - Enter the IP interface name here. This name can be up to 12 characters long.

<ipv6addr> - Enter the DHCPv6 server IP address.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To add a DHCPv6 server to the relay table:

```
DGS-3000-28XMP:admin#config dhcpv6_relay add ipif System 2001:DB8:1234:0:218:FEFF:FEFB:CC0E
Command: config dhcpv6_relay add ipif System 2001:DB8:1234::218:FEFF:FEFB:CC0E

Success.

DGS-3000-28XMP:admin#
```

27-6 config dhcpv6_relay hop_count

Description

This command is used to configure the DHCPv6 relay hop_count of the switch.

Format

config dhcpv6_relay hop_count <value 1-32>

Parameters

<value 1-32> - Enter the number of relay agents that have relayed this message. The default value is 4.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the maximum hops of a DHCPv6 relay packet could be transferred to 4:

```
DGS-3000-28XMP:admin#config dhcpv6_relay hop_count 4
Command: config dhcpv6_relay hop_count 4

Success.

DGS-3000-28XMP:admin#
```

27-7 config dhcpv6_relay ipif

Description

This command is used to configure the DHCPv6 relay state of one specific interface or all interfaces.

Format

config dhcpv6_relay ipif [<ipif_name 12> | all] state [enable | disable]

Parameters

<ipif_name 12> - Enter the IP interface name used here. This name can be up to 12 characters long.
all - Specifies that all the configured IP interfaces will be used.
state - Specifies to enable or disable the DHCPv6 relay state. **enable** - Specifies to enable the DHCPv6 relay state of the interface. **disable** - Specifies to disable the DHCPv6 relay state of the interface.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the DHCPv6 relay state of the System interface to enable:

```
DGS-3000-28XMP:admin#config dhcpv6_relay ipif System state enable
Command: config dhcpv6_relay ipif System state enable

Success.

DGS-3000-28XMP:admin#
```

27-8 config dhcpv6_local_relay vlan

Description

This command is used to enable or disable the DHCPv6 local relay function for a specified VLAN.

Format

config dhcpv6_local_relay vlan [<vlan_name 32> | vlanid <vlan_id>] state [enable | disable]

Parameters

<vlan_name 32> - Enter the VLAN name that will be used for this configuration.
vlanid - Specifies the VLAN ID that will be used for this configuration. It supports up to 48 VLANs. **<vlan_id>** - Enter the VLAN ID that will be used for this configuration. It supports up to 48 VLANs.
state - Specifies the DHCPv6 local relay function's state for the specified VLAN. **enable** - Specifies to enable the DHCPv6 local relay function's state for the specified VLAN. **disable** - Specifies to disable the DHCPv6 local relay function's state for the specified VLAN.

Restrictions

Only Administrators, Operators, and Power-Users can issue this command.

Example

To enable the DHCPv6 local relay function for the default VLAN:

```
DGS-3000-28XMP:admin#config dhcpv6_local_relay vlan default state enable
Command: config dhcpv6_local_relay vlan default state enable

Success.

DGS-3000-28XMP:admin#
```

27-9 config dhcpv6_relay option_18

Description

This command is used to configure the DHCPv6 relay agent information for processing option 18 within the switch.

Format

config dhcpv6_relay option_18 {state [enable | disable] | check [enable | disable] | interface_id [default | cid | vendor1 | vendor2]}(1)

Parameters

state - Specifies the DHCPv6 relay Option 18's state.

- **enable** - Specifies that the DHCPv6 relay Option 18's state is enabled. When the state is enabled, the DHCP packet will be inserted with the Option 18 field before being relayed to server.
- **disable** - Specifies that the DHCPv6 relay Option 18's state is disabled. When the state is disabled, the DHCP packet will be relayed directly to server without further checks and inserted with the Option 18.

check - Specifies whether or not to check for the Option 18 field in incoming packets. If the incoming packets contains an Option 18 field, then it will be dropped.

- **enable** - Specifies to enable the check function.
- **disable** - Specifies to disable the check function.

interface_id - Specifies the format of the Interface ID.

- **default** - Specifies to use the default formation for the Interface ID.

F01	F02
Sub Type	VLAN ID
1 byte	2 bytes

F01: Sub-type is 1 by default.

F02: VLAN ID. The incoming VLAN ID of the DHCP client packet.

- **cid** - Specifies to use the CID format for the Interface ID.

F01	F02	F03	F04
Sub Type	VLAN ID	Module ID	Port ID
1 byte	2 byte	1 byte	1 byte

F01: Sub-option type 2.

F02: VLAN ID. The VLAN ID of the incoming DHCP client packet.

F03: Module ID. For a stand-alone switch, it is 0. For a stacked switch, it is the box ID of that switch.

F04: Port ID. The port number of the incoming DHCP client packet. The port number starts from 1.

vendor1 - Specifies to use the Vendor 1 format for the Interface ID.

F01	F02	F03	F04	F05	F06	F07	F08
E (0x45)	t (0x74)	h (0x68)	e (0x65)	r (0x72)	n (0x65)	e (0x65)	t (0x74)
1 byte	1 byte	1 byte	1 byte	1 byte	1 byte	1 byte	1 byte

F09	F10	F11	F12	F13	F14	F15	F16
Chassis ID	/ (0x2F)	0 (0x30)	/ (0x2F)	Port Number	: (0x3A)	cvlan	. (0x2E)
1~2 bytes	1 byte	1 byte	1 byte	1~2 bytes	1 byte	1~4 bytes	1 byte

F17	F18	F19	F20	F21	F22	F23	F24
0 (0x30)	Space (0x20)	System Name	/ (0x2F)	0 (0x30)	/ (0x2F)	0 (0x30)	/ (0x2F)
1 byte	1 byte	1~128 bytes	1 byte	1 byte	1 byte	1 byte	1 byte

F25	F26	F27	F28	F29
Chassis ID	/ (0x2F)	0 (0x30)	/ (0x2F)	Port Number
1~2 bytes	1 byte	1 byte	1 byte	1~2 bytes

F01: Character ‘E’.

F02: Character ‘t’.

F03: Character ‘h’.

F04: Character ‘e’.

F05: Character ‘r’.

F06: Character ‘n’.

F07: Character ‘e’.

F08: Character ‘t’.

F09: Chassis ID. The number of the chassis. The format is ASCII string.

1. For a stand-alone switch, it is 0.
2. For a stacked switch, it is the box ID of that switch.

F10: Slash (/).

F11: ASCII format string ‘0’.

F12: Slash (/).

F13: Port number. The incoming port number DHCP client packets. ASCII format string.

F14: Colon (:)

F15: ‘cvlan’ is the client’s VLAN ID. The value ranges from 1 to 4094. ASCII format string.

F16: Dot (.).

F17: ASCII format string ‘0’.

F18: Space.

F19: System name of the Switch. **NOTE:** If the System name exceeds 128 bytes, it will only use the first 128 bytes.

F20: Slash (/).

F21: ASCII format string '0'.

F22: Slash (/).

F23: ASCII format string '0'.

F24: Slash (/).

F25: Chassis ID. This value is the same as F09.

F26: Slash (/).

F27: ASCII format string '0'.

F28: Slash (/).

F29: Port number. The incoming port number of DHCP client packets. ASCII format string.

Vendor2 - Specifies to use the Vendor 2 format for the Interface ID.

F01	F02	F03	F04	F05	F06	F07	F08
E (0x45)	t (0x74)	h (0x68)	e (0x65)	r (0x72)	n (0x65)	e (0x65)	t (0x74)
1 byte	1 byte	1 byte	1 byte	1 byte	1 byte	1 byte	1 byte

F09	F10	F11	F12	F13	F14	F15	F16
Chassis ID	/ (0x2F)	0 (0x30)	/ (0x2F)	Port Number	: (0x3A)	cvlan	. (0x2E)
1~2 bytes	1 byte	1 byte	1 byte	1~2 bytes	1 byte	1~4 bytes	1 byte

F17	F18	F19	F20	F21	F22	F23	F24
0 (0x30)	Space (0x20)	System Name	/ (0x2F)	0 (0x30)	/ (0x2F)	0 (0x30)	/ (0x2F)
1 byte	1 byte	1~128 bytes	1 byte	1 byte	1 byte	1 byte	1 byte

F25	F26	F27	F28	F29
Chassis ID	/ (0x2F)	0 (0x30)	/ (0x2F)	Port Number
1~2 bytes	1 byte	1 byte	1 byte	1~2 bytes

F01: Character 'E'.

F02: Character 't'.

F03: Character 'h'.

F04: Character 'e'.

F05: Character 'r'.

F06: Character 'n'.

F07: Character 'e'.

F08: Character 't'.

F09: Chassis ID. The number of the chassis. The format is ASCII string.

1. For a stand-alone switch, it is 1.
2. For a stacked switch, it is the box ID of that switch.

F10: Slash (/).

F11: ASCII format string '0'.

F12: Slash (/).

F13: Port number. The incoming port number DHCP client packets. ASCII format string.

F14: Colon (:)

F15: 'cvlan' is the client's VLAN ID. The value ranges from 1 to 4094. ASCII format string.

F16: Dot (.).

F17: ASCII format string '0'.

F18: Space.

F19: System name of the Switch. **NOTE:** If the System name exceeds 128 bytes, it will only use the first 128 bytes.

F20: Slash (/).

F21: ASCII format string '0'.

F22: Slash (/).

F23: ASCII format string '0'.

F24: Slash (/).

F25: Chassis ID. This value is the same as F09.

F26: Slash (/).

F27: ASCII format string '0'.

F28: Slash (/).

F29: Port number. The incoming port number of DHCP client packets. ASCII format string.

Restrictions

Only Administrators, Operators, and Power-Users can issue this command.

Example

To configure the DHCPv6 relay option 18:

```
DGS-3000-28XMP:admin#config dhcpv6_relay option_18 state enable
Command: config dhcpv6_relay option_18 state enable

Success.

DGS-3000-28XMP:admin#config dhcpv6_relay option_18 check enable
Command: config dhcpv6_relay option_18 check enable

Success.

DGS-3000-28XMP:admin#config dhcpv6_relay option_18 interface_id default
Command: config dhcpv6_relay option_18 interface_id default

Success.

DGS-3000-28XMP:admin#config dhcpv6_relay option_18 interface_id cid
Command: config dhcpv6_relay option_18 interface_id cid

Success.

DGS-3000-28XMP:admin#config dhcpv6_relay option_18 interface_id vendor1
Command: config dhcpv6_relay option_18 interface_id vendor1

Success.

DGS-3000-28XMP:admin#
```

27-10 config dhcpv6_relay option_37

Description

This command is used to configure the processing of option 37 for the DHCPv6 relay function

Format

config dhcpv6_relay option_37 {state [enable | disable] | check [enable | disable] | remote_id [default | cid_with_user_define <desc 128> | user_define <desc 128> | vendor1]}(1)

Parameters

state - Specifies to enable or disable the state of the DHCPv6 relay Option 37.

enable - Specifies to enable the state of the DHCPv6 relay Option 37. The DHCP packet will be inserted with the Option 37 field before being relayed to server.

disable - Specifies to disable the state of the DHCPv6 relay Option 37. The DHCP packet will be relayed directly to server without further checks and inserted with the Option 37.

check - Specifies to enable or disable the check function. When enabled, packets coming from client side should not have the option 37 field. If client originating packets have the option 37 field set, they will be dropped.

enable - Specifies to enable the check function.

disable - Specifies to disable the check function.

remote_id Specifies the content in the Remote ID.

default - The remote ID will be VLAN ID + Module + Port +System MAC address of the device.

cid_with_user_define - The remote ID will be VLAN ID + Module + Port + user defined string.

<desc 128> - Enter the user defined cid. The page title description can be up to 128 characters long.

user_define - The remote ID will be user defined string.

<desc 128> - Enter the user defined spec up to 128 characters long.

vendor1 - The remote ID will be System MAC address of the device

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the DHCPv6 relay option 37:

```
DGS-3000-28XMP:admin#config dhcpv6_relay option_37 state enable
Command: config dhcpv6_relay option_37 state enable

Success.

DGS-3000-28XMP:admin#config dhcpv6_relay option_37 check enable
Command: config dhcpv6_relay option_37 check enable

Success.

DGS-3000-28XMP:admin#config dhcpv6_relay option_37 remote_id default
Command: config dhcpv6_relay option_37 remote_id default

Success.

DGS-3000-28XMP:admin#config dhcpv6_relay option_37 remote_id cid_with_user_defin
e D-link DGS3000 Series
Command: config dhcpv6_relay option_37 remote_id cid_with_user_define D-link DGS3000 Serie
s

Success.

DGS-3000-28XMP:admin#config dhcpv6_relay option_37 remote_id user_define D-link
DGS3000 Series
Command: config dhcpv6_relay option_37 remote_id user_define D-link DGS3000 Series

Success.

DGS-3000-28XMP:admin#
```

27-11 config dhcpv6_relay port

Description

This command is used to configure the state of the DHCPv6 relay on the specified port(s).

Format

config dhcpv6_relay port [<portlist> | all] state [enable | disable]

Parameters

<portlist> - Enter a range of ports to be configured.
all - Specifies to configure all ports.
state - Specifies to enable or diable the DHCPv6 relay state on the specified port(s). **enable** - Specifies to enable the DHCPv6 relay state. This is the default value. **disable** - Specifies to disable the DHCPv6 relay state.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable the DHCPv6 relay state on port 1-3:

```
DGS-3000-28XMP:admin#config dhcpv6_relay port 1-3 state enable
Command: config dhcpv6_relay port 1-3 state enable

Success.

DGS-3000-28XMP:admin#
```

27-12 show dhcpv6_relay

Description

This command is used to display the current DHCPv6 relay configuration of all interfaces, or if an IP interface name is specified, the DHCPv6 relay configuration for that IP interface.

Format

show dhcpv6_relay {ipif <ipif_name 12>}

Parameters

ipif - (Optional) The name of the IP interface for which to display the current DHCPv6 relay configuration.
<ipif_name 12> - Enter the IP interface name used here. This name can be up to 12 characters long.

If no IP interface is specified, all configured DHCPv6 relay interfaces are displayed.

Restrictions

None.

Example

To display local DHCPv6 relay configuration:

```
DGS-3000-28XMP:admin#show dhcpv6_relay
Command: show dhcpv6_relay

DHCPv6 Relay Global State : Enabled
DHCPv6 Hops Count Limit   : 4
DHCPv6 Relay Information Option 18 State : Enabled
DHCPv6 Relay Information Option 18 Check : Enabled
DHCPv6 Relay Information Option 18 Interface ID Type : Vendor1
DHCPv6 Relay Information Option 37 State : Enabled
DHCPv6 Relay Information Option 37 Check : Enabled
DHCPv6 Relay Information Option 37 Remote ID Type : User Define
DHCPv6 Relay Information Option 37 Remote ID : D-link DGS3000 Series
----------------------------------------------------------------
IP Interface              : System
DHCPv6 Relay Status       : Enabled
Server Address            : 2001:DB8:1234::218:FEFF:FEFB:CC0E

 Total Entries   : 1


DGS-3000-28XMP:admin#
```

27-13 show dhcpv6_local_relay

Description

This command is used to display the current DHCPv6 local relay configuration.

Format

show dhcpv6_local_relay

Parameters

None.

Restrictions

None.

Example

To display local DHCPv6 relay configuration:

```
DGS-3000-28XMP:admin#show dhcpv6_local_relay
Command: show dhcpv6_local_relay

DHCPv6 Local Relay Status         : Disabled
DHCPv6 Local Relay VID List       : 1


DGS-3000-28XMP:admin#
```

27-14 show dhcpv6_relay port

Description

This command is used to display the state of the DHCPv6 relay on the specified port(s).

Format

show dhcpv6_relay port {<portlist>}

Parameters

<portlist> - (Optional) Enter the list of ports.

Restrictions

None.

Example

To display the DHCPv6 relay state on port 1-5:

```
DGS-3000-28XMP:admin#show dhcpv6_relay port 1-5
Command: show dhcpv6_relay port 1-5

Port  DHCPv6 Relay State
----  ------------------
1     Enabled
2     Enabled
3     Enabled
4     Enabled
5     Enabled

 Total Entries : 5

DGS-3000-28XMP:admin#
```

27-15 debug dhcpv6_relay state enable

Description

This command is used to enable the DHCPv6 relay debug function.

Format

debug dhcpv6_relay state enable

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To enable the DHCPv6 relay debug function:

```
DGS-3000-28XMP:admin#debug dhcpv6_relay state enable
Command: debug dhcpv6_relay state enable

Success.

DGS-3000-28XMP:admin#
```

27-16 debug dhcpv6_relay state disable

Description

This command is used to disable the DHCPv6 relay debug function.

Format

debug dhcpv6_relay state disable

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To disable the DHCPv6 relay debug function:

```
DGS-3000-28XMP:admin#debug dhcpv6_relay state disable
Command: debug dhcpv6_relay state disable

Success.

DGS-3000-28XMP:admin#
```

27-17 debug dhcpv6_relay output

Description

This command is used to send debug messages to the buffer or console.

Format

debug dhcpv6_relay output [buffer | console]

Parameters

buffer - Specifies to send debug messages to the buffer.
console - Specifies to send debug messages to the console.

Restrictions

Only Administrators can issue this command.

Example

To send debug messages to the console:

```
DGS-3000-28XMP:admin#debug dhcpv6_relay output console
Command: debug dhcpv6_relay output console

Success.

DGS-3000-28XMP:admin#
```

27-18 debug dhcpv6_relay packet

Description

This command is used to enable or disable the debug information flag for DHCPv6 relay packets including packets sending and receiving.

Format

debug dhcpv6_relay packet [all | receiving | sending] state [enable | disable]

Parameters

all - Specifies the debug flag for sending and receiving packets.
receiving - Specifies the debug flag for receiving packets.
sending - Specifies the debug flag for sending packets.
state - Specifies to enable or disable the debug flag. **enable** - Specifies to enable the debug flag. **disable** - Specifies to disable the debug flag.

Restrictions

Only Administrators can issue this command.

Example

To enable the debug flag for DHCPv6 relay packets sending:

```
DGS-3000-28XMP:admin#debug dhcpv6_relay packet sending state enable
Command: debug dhcpv6_relay packet sending state enable

Success.

DGS-3000-28XMP:admin#
```

27-19 debug dhcpv6_relay hop_count state

Description

This command is used to enable or disable the debug information flag for DHCPv6 relay hop count.

Format

debug dhcpv6_relay hop_count state [enable | disable]

Parameters

enable - Specifies to enable the debug information flag for DHCPv6 relay hop count.
disable - Specifies to disable the debug information flag for DHCPv6 relay hop count.

Restrictions

Only Administrators can issue this command.

Example

To enable the debug information flag for DHCPv6 relay hop count:

```
DGS-3000-28XMP:admin#debug dhcpv6_relay hop_count state enable
Command: debug dhcpv6_relay hop_count state enable

Success.

DGS-3000-28XMP:admin#
```

Chapter 28 Digital Diagnostic Monitoring (DDM) Commands

config ddm [trap | log] [enable | disable]
config ddm ports [<portlist> | all] [[temperature_threshold | voltage_threshold | bias_current_threshold | tx_power_threshold | rx_power_threshold] {high_alarm <float> | low_alarm <float> | high_warning <float> | low_warning <float>} | {state [enable | disable] | shutdown [alarm | warning | none]}]
show ddm
show ddm ports {<portlist>} [status | configuration]

28-1 config ddm

Description

The command configures the DDM log and trap actions when encountering an exceeding alarm or warning thresholds event.

Format

config ddm [trap | log] [enable | disable]

Parameters

trap - Specifies whether to send traps, when the operating parameter exceeds the corresponding threshold. The DDM trap is disabled by default.
log - Specifies whether to send a log, when the operating parameter exceeds the corresponding threshold. The DDM log is enabled by default.
enable - Specifies to enable the log or trap sending option.
disable - Specifies to disable the log or trap sending option.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure DDM log state to enable:

```
DGS-3000-28XMP:admin# config ddm log enable
Command: config ddm log enable

Success.

DGS-3000-28XMP:admin#
```

To configure DDM trap state to enable:

```
DGS-3000-28XMP:admin# config ddm trap enable
Command: config ddm trap enable

Success.

DGS-3000-28XMP:admin#
```

28-2 config ddm ports

Description

This command is used to configure the DDM settings of the specified ports.

Format

config ddm ports [<portlist> | all] [[temperature_threshold | voltage_threshold | bias_current_threshold | tx_power_threshold | rx_power_threshold] {high_alarm <float> | low_alarm <float> | high_warning <float> | low_warning <float>} | {state [enable | disable] | shutdown [alarm | warning | none]}]

Parameters

<portlist> - Enter the range of ports to be configured here.

all - Specifies that all the optic ports' operating parameters will be configured.

temperature_threshold - Specifies the threshold of the optic module's temperature in centigrade.

voltage_threshold - Specifies the threshold of optic module's voltage.

bias_current_threshold - Specifies the threshold of the optic module's bias current.

tx_power_threshold - Specifies the threshold of the optic module's output power.

rx_power_threshold - Specifies the threshold of the optic module's received power.

high_alarm - (Optional) Specifies the high threshold for the alarm. When the operating parameter rises above this value, the action associated with the alarm is taken.

<float> - Enter the high threshold alarm value used here.

low_alarm - (Optional) Specifies the low threshold for the alarm. When the operating parameter falls below this value, the action associated with the alarm is taken.

<float> - Enter the low threshold alarm value used here.

high_warning - (Optional) Specifies the high threshold for the warning. When the operating parameter rises above this value, the action associated with the warning is taken.

<float> - Enter the high threshold warning value here.

low_warning - (Optional) Specifies the low threshold for the warning. When the operating parameter falls below this value, the action associated with the warning is taken.

<float> - Enter the low threshold warning value here.

state - (Optional) Specifies the DDM state to enable or disable. If the state is disabled, no DDM action will take effect.

enable - Specifies to enable the DDM state.

disable - Specifies to disable the DDM state.

shutdown - (Optional) Specifies whether or not to shut down the port when the operating parameter exceeds the corresponding alarm threshold or warning threshold. The default value is none.

alarm - Shut down the port when the configured alarm threshold range is exceeded.

warning - Shut down the port when the configured warning threshold range is exceeded.

none - The port will never shut down regardless if the threshold ranges are exceeded or not.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure port 25's temperature threshold:

```
DGS-3000-28XMP:admin# config ddm ports 25 temperature_threshold high_alarm 84.9532
low_alarm -10 high_warning 70 low_warning 2.25
Command: config ddm ports 25 temperature_threshold high_alarm 84.9532 low_alarm
-10 high_warning 70 low_warning 2.25

 According to the DDM precision definition, closest value 84.9531 is chosen.

Success.

DGS-3000-28XMP:admin#
```

To configure port 25's voltage threshold:

```
DGS-3000-28XMP:admin# config ddm ports 25 voltage_threshold high_alarm 4.25 low_alarm 2.5
high_warning 3.5 low_warning 3
Command: config ddm ports 25 voltage_threshold high_alarm 4.25 low_alarm 2.5 high_warning 3.5
low_warning 3

Success.

DGS-3000-28XMP:admin#
```

To configure port 25's bias current threshold:

```
DGS-3000-28XMP:admin# config ddm ports 25 bias_current_threshold high_alarm 7.25 low_alarm
0.004 high_warning 0.5 low_warning 0.008
Command: config ddm ports 25 bias_current_threshold high_alarm 7.25 low_alarm 0.004
high_warning 0.5 low_warning 0.008

Success.

DGS-3000-28XMP:admin#
```

To configure port 25's transmit power threshold:

```
DGS-3000-28XMP:admin# config ddm ports 25 bias_current_threshold high_alarm 7.25 low_alarm
0.004 high_warning 0.5 low_warning 0.008
Command: config ddm ports 25 bias_current_threshold high_alarm 7.25 low_alarm 0.004
high_warning 0.5 low_warning 0.008

Success.

DGS-3000-28XMP:admin#
```

To configure port 25's receive power threshold:

```
DGS-3000-28XMP:admin# config ddm ports 25 rx_power_threshold high_alarm 4.55 low_alarm 0.01
high_warning 3.5 low_warning 0.03
Command: config ddm ports 25 rx_power_threshold high_alarm 4.55 low_alarm 0.01 high_warning
3.5 low_warning 0.03

Success.

DGS-3000-28XMP:admin#
```

To configure port 25's actions associate with the alarm:

```
DGS-3000-28XMP:admin# config ddm ports 25 state enable shutdown alarm
Command: config ddm ports 25 state enable shutdown alarm

Success.

DGS-3000-28XMP:admin#
```

28-3 show ddm

Description

This command is used to display the DDM global settings.

Format

show ddm

Parameters

None.

Restrictions

None.

Example

To display the DDM global settings:

```
DGS-3000-28XMP:admin# show ddm
Command: show ddm

DDM Log           :Enabled
DDM Trap          :Disabled



DGS-3000-28XMP:admin#
```

28-4 show ddm ports

Description

This command is used to show the current operating DDM parameters and configuration values of the optic module of the specified ports. There are two types of thresholds: the administrative configuration and the operation configuration threshold.

For the optic port, when a particular threshold was configured by user, it will be shown in this command with a tag indicating that it is a threshold that user configured, else it would be the threshold read from the optic module that is being inserted.

Format

show ddm ports {<portlist>} [status | configuration]

Parameters

<portlist> - (Optional) Enter the range of ports to be displayed here.
status - Specifies that the operating parameter will be displayed.
configuration - Specifies that the configuration values will be displayed.

Restrictions

None.

Example

To display ports 25-26's operating parameters:

```
DGS-3000-28XMP:admin# show ddm ports 25-26 status
Command: show ddm ports 25-26 status

 Port    Temperature   Voltage    Bias Current   TX Power     RX Power
        (in Celsius)     (V)         (mA)         (mW)         (mW)
------- ------------- ---------- -------------- ---------- ------------
  25         -            -            -            -            -
  26         -            -            -            -            -









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

Chapter 29 D-Link Discovery Protocol (DDP) Client Command List

enable ddp
disable ddp
config ddp report-timer [30 | 60 | 90 | 120 | Never]
config ddp ports [<portlist> | all] state [enable | disable]
show ddp {ports <portlist>}

29-1 enable ddp

Description

This command is used to enable DDP client function globally. This is the default value.

Format

enable ddp

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable DDP client function globally:

```
DGS-3000-28XMP:admin#enable ddp
Command: enable ddp

Success.

DGS-3000-28XMP:admin#
```

29-2 disable ddp

Description

This command is used to disable DDP client function globally.

Format

disable ddp

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To disable DDP client function globally:

```
DGS-3000-28XMP:admin#disable ddp
Command: disable ddp

Success.

DGS-3000-28XMP:admin#
```

29-3 config ddp report-timer

Description

This command is used to configure the interval between two consecutive DDP report messages.

Format

config ddp report-timer [30 | 60 | 90 | 120 | Never]

Parameters

30 - Specifies the report interval to 30 seconds. This is the default value.
60 - Specifies the report interval to 60 seconds.
90 - Specifies the report interval to 90 seconds.
120 - Specifies the report interval to 120 seconds.
Never - Specifies to stop sending report message.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the interval to 60 seconds:

```
DGS-3000-28XMP:admin#config ddp report-timer 60
Command: config ddp report-timer 60

Success.

DGS-3000-28XMP:admin#
```

29-4 config ddp ports

Description

This command is used to configure the state of DDP client function on the specified ports. When DDP is disabled on a port, the port will neither process nor generate DDP message. DDP messages received by the port are flooded in VLAN.

Format

config ddp ports [<portlist> | all] state [enable | disable]

Parameters

<portlist> - Enter a range of ports to be configured.
all - Specifies to configure all ports.
state - Specifies to enable or diable the DDP client function on the specified port(s). **enable** - Specifies to enable the DDP client function. This is the default value. **disable** - Specifies to disable the DDP client function.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable DDP client function on port 1:

```
DGS-3000-28XMP:admin#config ddp ports 1 state enable
Command: config ddp ports 1 state enable

Success.

DGS-3000-28XMP:admin#
```

29-5 show ddp

Description

This command is used to display DDP configurations of the Switch.

Format

show ddp {ports <portlist>}

Parameters

ports - (Optional) Specifies the port used for this configuration. **<portlist>** - Enter the port number used here.

Restrictions

None.

Example

To display DDP configurations of the Switch:

```
DGS-3000-28XMP:admin#show ddp
Command: show ddp

D-Link Discovery Protocol state: Enabled
Report timer: 60 seconds

DGS-3000-28XMP:admin#
```

To display DDP configurations on port 1:

```
DGS-3000-28XMP:admin#show ddp ports 1
Command: show ddp ports 1

Port   State
----   ----------
1      Enabled

DGS-3000-28XMP:admin#
```

Chapter 30 D-Link Unidirectional Link Detection (DULD) Command List

config duld ports [<portlist> | all] {state [enable | disable] | mode [shutdown | normal] | discovery_time <sec 5-65535>}(1)
config duld {recover_timer [0 | <sec 60-1000000>] | oper_timing [local_ready | local_remote_ready]}
show duld {ports {<portlist>}}

30-1 config duld ports

Description

This command is used to configure unidirectional link detection on ports. Unidirectional link detection provides discovery mechanism based on 802.3ah to discovery its neighbor. If the OAM discovery can complete in configured discovery time, it concludes the link is bidirectional. Otherwise, it starts detecting task to detect the link status.

Format

config duld ports [<portlist> | all] {state [enable | disable] | mode [shutdown | normal] | discovery_time <sec 5-65535>}(1)

Parameters

<portlist> - Enter a range of ports.
all - Specifies to select all ports.
state - Specifies these ports unidirectional link detection status. **enable** - Specifies to enable unidirectional link detection status. **disable** - Specifies to disable unidirectional link detection status.
mode - Specifies the mode when detecting unidirectional link. **shutdown** - Specifies to disable the port and log an event when any unidirectional link is detected. **normal** - Specifies to only log an event when a unidirectional link is detected.
discovery_time - Specifies these ports neighbor discovery time. If OAM discovery cannot complete in the discovery time, the unidirectional link detection will start. **<sec 5-65535>** - Enter a time in second. The default discovery time is 5 seconds.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable unidirectional link detection on port 1:

```
DGS-3000-28XMP:admin# config duld ports 1 state enable
Command: config duld ports 1 state enable

Success.

DGS-3000-28XMP:admin#
```

30-2 config duld

Description

This command is used to configure unidirectional link detection settings.

Format

config duld {recover_timer [0 | <sec 60-1000000>] | oper_timing [local_ready | local_remote_ready]}

Parameters

recover_timer - (Optional) Specifies the automatic recovery time.
- **0** - Specifies to disable this function.
- **<sec 60-1000000>** - Enter the automatic recovery time in seconds.

oper_timing - (Optional) Specifies to operate DULD.
- **local_ready** - Specifies to operate DULD when the local peer owns DULD ability.
- **local_remote_ready** - Specifies that the DULD will not be operated when the local peer owns DULD ability.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the automatic recovery time:

```
DGS-3000-28XMP:admin#config duld recover_timer 60
Command: config duld recover_timer 60

Success.

DGS-3000-28XMP:admin#
```

30-3 show duld

Description

This command is used to display DULD information.

Format

show duld {ports {<portlist>}}

Parameters

ports - (Optional) Specifies the ports for which the information is displayed.
<portlist> - (Optional) Enter the list of ports used here.

Restrictions

None.

Example

To display DULD information:

```
DGS-3000-28XMP:admin#show duld
Command: show duld

DULD Global Settings
-----------------------------------------
Recover Time          : 60 sec
DULD Operation Timing : Local Ready

DGS-3000-28XMP:admin#
```

To show ports 1-4 unidirectional link detection information:

```
DGS-3000-28XMP:admin#show duld ports 1-4
Command: show duld ports 1-4

Port   Admin State  Oper Status  Mode      Link Status     Discovery Time(Sec)
-----  -----------  -----------  --------  --------------  -------------------
1      Enabled      Disabled     Normal    Unknown         5
2      Disabled     Disabled     Normal    Unknown         5
3      Disabled     Disabled     Normal    Unknown         5
4      Disabled     Disabled     Normal    Unknown         5

DGS-3000-28XMP:admin#
```

Chapter 31 Domain Name System (DNS) Resolver Command List

config name_server add [<ipaddr> | <ipv6addr>] {primary}
config name_server delete [<ipaddr> | <ipv6addr>] {primary}
config name_server timeout <sec 1-60>
show name_server
create host_name <name 255> [<ipaddr> | <ipv6addr>]
delete host_name [<name 255> | all]
show host_name {static | dynamic}
enable dns_resolver
disable dns_resolver

31-1 config name_server add

Description

This command is used to add a DNS resolver name server to the Switch.

Format

config name_server add [<ipaddr> | <ipv6addr>] {primary}

Parameters

<ipaddr> - Enter the IPv4 address of the DNS Resolver name server.
<ipv6addr> - Enter the IPv6 address of the DNS Resolver name server.
primary - (Optional) Specifies that the name server is a primary name server.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To add DNS Resolver primary name server 10.10.10.10:

```
DGS-3000-28XMP:admin#config name_server add 10.10.10.10 primary
Command: config name_server add 10.10.10.10 primary

Success.

DGS-3000-28XMP:admin#
```

31-2 config name_server delete

Description

This command is used to delete a DNS resolver name server from the Switch.

Format

config name_server delete [<ipaddr> | <ipv6addr>] {primary}

Parameters

<ipaddr> - Enter the IPv4 address of the DNS Resolver name server.
<ipv6addr> - Enter the IPv6 address of the DNS Resolver name server.
primary - (Optional) Specifies that the name server is a primary name server.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete DNS Resolver name server 10.10.10.1:

```
DGS-3000-28XMP:admin#config name_server delete 10.10.10.1
Command: config name_server delete 10.10.10.1

Success.

DGS-3000-28XMP:admin#
```

31-3 config name_server timeout

Description

This command is used to configure the timeout value of a DNS Resolver name server.

Format

config name_server timeout <sec 1-60>

Parameters

<sec 1-60> - Enter the maximum time waiting for a response from a specified name server.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure DNS Resolver name server time out to 10 seconds:

```
DGS-3000-28XMP:admin#config name_server timeout 10
Command: config name_server timeout 10

Success.

DGS-3000-28XMP:admin#
```

31-4 show name_server

Description

This command is used to display the current DNS Resolver name servers and name server time out on the Switch.

Format

show name_server

Parameters

None.

Restrictions

None.

Example

To display the current DNS Resolver name servers and name server time out:

```
DGS-3000-28XMP:admin#show name_server
Command: show name_server

 Name Server Timeout: 10 seconds

 Static Name Server Table:
 Server IP Address                                  Priority
 -------------------------------------------------- -----------
 10.10.10.10                                        Primary

 Dynamic Name Server Table:
 Server IP Address                                  Priority
 -------------------------------------------------- -----------
 10.48.74.122                                       Primary

DGS-3000-28XMP:admin#
```

31-5 create host_name

Description

This command is used to create the static host name entry of the Switch.

Format

create host_name <name 255> [<ipaddr> | <ipv6addr>]

Parameters

<name 255> - Enter the hostname used. This name can be up to 255 characters long.
<ipaddr> - Enter the host IP address.
<ipv6addr> - Enter the host IPv6 address.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To create static host name “www.example.com”:

```
DGS-3000-28XMP:admin#create host_name www.example.com 10.10.10.10
Command: create host_name www.example.com 10.10.10.10

Success.

DGS-3000-28XMP:admin#
```

31-6 delete host_name

Description

This command is used to delete the static or dynamic host name entries of the Switch.

Format

delete host_name [<name 255> | all]

Parameters

<name 255> - Enter the hostname. This name can be up to 255 characters long.
all - Specifies that all the hostnames will be deleted.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete the static host name entry “www.example.com”:

```
DGS-3000-28XMP:admin#delete host_name www.example.com
Command: delete host_name www.example.com

Success.

DGS-3000-28XMP:admin#
```

31-7 show host_name

Description

This command is used to display the current host name.

Format

show host_name {static | dynamic}

Parameters

static - (Optional) Specifies to display the static host name entries.
dynamic - (Optional) Specifies to display the dynamic host name entries.

Restrictions

None.

Example

To display the static and dynamic host name entries:

```
DGS-3000-28XMP:admin#show host_name
Command: show host_name

 Static Host Name Table

 Host Name   : www.example.com
 IP Address   : 10.10.10.10


 Total Static Entries:  1

 Dynamic Host Name Table


 Total Dynamic Entries: 0


DGS-3000-28XMP:admin#
```

31-8 enable dns_resolver

Description

This command is used to enable the DNS Resolver state of the Switch.

Format

enable dns_resolver

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the DNS Resolver state to enabled:

```
DGS-3000-28XMP:admin#enable dns_resolver
Command: enable dns_resolver

Success.

DGS-3000-28XMP:admin#
```

31-9 disable dns_resolver

Description

This command is used to disable the DNS Resolver state of the Switch.

Format

disable dns_resolver

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the DNS Resolver state to disabled:

```
DGS-3000-28XMP:admin#disable dns_resolver
Command: disable dns_resolver

Success.

DGS-3000-28XMP:admin#
```

Chapter 32 DoS Attack Prevention Command List

config dos_prevention dos_type [{land_attack | blat_attack | tcp_null_scan | tcp_xmasscan | tcp_synfin | tcp_syn_srcport_less_1024 | ping_death_attack | tcp_tiny_frag_attack} | all] {action [drop] | state [enable | disable]}
show dos_prevention {land_attack | blat_attack | tcp_null_scan | tcp_xmasscan | tcp_synfin | tcp_syn_srcport_less_1024 | ping_death_attack | tcp_tiny_frag_attack}
config dos_prevention trap [enable | disable]
config dos_prevention log [enable | disable]

32-1 config dos_prevention dos_type

Description

This command is used to configure the prevention of Denial-of-Service (DoS) attacks, including state and action. The packet matching will be done by hardware. For a specific type of attack, the content of the packet will be matched against a specific pattern.

Format

config dos_prevention dos_type [{land_attack | blat_attack | tcp_null_scan | tcp_xmasscan | tcp_synfin | tcp_syn_srcport_less_1024 | ping_death_attack | tcp_tiny_frag_attack} | all] {action [drop] | state [enable | disable]}

Parameters

land_attack - (Optional) Specifies to check whether the source address is equal to the destination address of a received IP packet.
blat_attack - (Optional) Specifies to check whether the source port is equal to the destination port of a received TCP packet.
tcp_null_scan - (Optional) Specifies to check whether a received TCP packet contains a sequence number of 0 and no flags.
tcp_xmasscan - (Optional) Specifies to check whether a received TCP packet contains URG, Push and FIN flags.
tcp_synfin - (Optional) Specifies to check whether a received TCP packet contains FIN and SYN flags.
tcp_syn_srcport_less_1024 - (Optional) Specifies to check whether TCP packets on the source port are less than 1024 packets.
ping_death_attack - (Optional) Specifies to detect whether received packets are fragmented ICMP packets.
tcp_tiny_frag_attack - (Optional) Specifies to check whether the packets are TCP tiny fragment packets.
all - Specifies all DoS attack type.
action - (Optional) Specifies to take the following action when enabling DoS prevention. **drop** - Specifies to drop DoS attack packets.
state - (Optional) Specifies the DoS attack prevention state. **enable** - Specifies to enable DoS attack prevention. **disable** - Specifies to disable DoS attack prevention.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure land attack and blat attack prevention, the action is drop:

```
DGS-3000-28XMP:admin# config dos_prevention dos_type land_attack blat_attack action  drop
state enable
Command: config dos_prevention dos_type land_attack blat_attack action drop state enable

Success.

DGS-3000-28XMP:admin#
```

32-2 show dos_prevention

Description

This command is used to display DoS prevention information, including the trap state, the log state, the type of DoS attack, the prevention state, the corresponding action if the prevention is enabled and the counter information of the DoS packet.

Format

show dos_prevention {land_attack | blat_attack | tcp_null_scan | tcp_xmasscan | tcp_synfin | tcp_syn_srcport_less_1024 | ping_death_attack | tcp_tiny_frag_attack}

Parameters

land_attack - (Optional) Specifies to display land attack information.
blat_attack - (Optional) Specifies to display blat attack information.
tcp_null_scan - (Optional) Specifies to display TCP null scan information.
tcp_xmasscan - (Optional) Specifies to display TCP Xmas scan information.
tcp_synfin - (Optional) Specifies to display TCP SYN/FIN information.
tcp_syn_srcport_less_1024 - (Optional) Specifies to display TCP SYN SrcPort less 1024 information.
ping_death_attack - (Optional) Specifies to display ping of death attack information.
tcp_tiny_frag_attack - (Optional) Specifies to display TCP tiny fragment attack information.

Restrictions

None.

Example

To display DoS prevention information:

```
DGS-3000-28XMP:admin# show dos_prevention
Command: show dos_prevention

Trap:Disabled   Log:Disabled    Function Version  : 1.01

DoS Type                    State     Action            Frame Counts
--------------------------  --------  ----------------  ------------
Land Attack                 Enabled   Drop              -
Blat Attack                 Enabled   Drop              -
TCP Null Scan               Disabled  Drop              -
TCP Xmas Scan               Disabled  Drop              -
TCP SYNFIN                  Disabled  Drop              -
TCP SYN SrcPort Less 1024   Disabled  Drop              -
Ping of Death Attack        Disabled  Drop              -
TCP Tiny Fragment Attack    Disabled  Drop              -



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

32-3 config dos_prevention trap

Description

This command is used to enable or disable DoS prevention trap state.

Format

config dos_prevention trap [enable | disable]

Parameters

enable - Specifies to enable DoS prevention trap state.
disable - Specifies to disable DoS prevention trap state.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To disable DoS prevention trap:

```
DGS-3000-28XMP:admin# config dos_prevention trap disable
Command: config dos_prevention trap disable

Success.

DGS-3000-28XMP:admin#
```

32-4 config dos_prevention log

Description

This command is used to enable or disable dos prevention log state.

Format

config dos_prevention log [enable | disable]

Parameters

enable - Specifies to enable DoS prevention log state.
disable - Specifies to disable DoS prevention log state.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable DoS prevention log:

```
DGS-3000-28XMP:admin# config dos_prevention log enable
Command: config dos_prevention log enable

Success.

DGS-3000-28XMP:admin#
```

Chapter 33 Energy Efficient Ethernet (EEE) Command List

config eee ports [<portlist> | all] state [enable | disable]
show eee ports {<portlist>}

33-1 config eee ports

Description

This command is used to enable or disable the EEE function on the specified port(s) on the Switch.

NOTE: EEE and ERPS are mutually exclusive functions.

Format

config eee ports [<portlist> | all] state [enable | disable]

Parameters

<portlist> - Enter a range of ports to be configured.
all - Specifies to configure all ports.
state - Specifies the EEE state. The default is disabled. **enable** - Specifies to enable the EEE function for the specified port(s). **disable** - Specifies to disable the EEE function for the specified port(s).

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable the EEE state on ports 2-5:

```
DGS-3000-28XMP:admin#config eee ports 2-5 state enable
Command: config eee ports 2-5 state enable

Success.

DGS-3000-28XMP:admin#
```

33-2 show eee ports

Description

This command is used to display the EEE function state on the specified port(s).

Format

show eee ports {<portlist>}

Parameters

<portlist> - (Optional) Specifies a list of ports to be displayed.

Restrictions

None.

Example

To display the EEE state:

```
DGS-3000-28XMP:admin#show eee ports  1-6,9
Command: show eee ports 1-6,9

Port             State
---------     -----------
1             Disabled
2             Enabled
3             Enabled
4             Enabled
5             Enabled
6             Disabled
9             Disabled



DGS-3000-28XMP:admin#
```

Chapter 34 Ethernet Ring Protection Switching (ERPS) Command List

enable erps
disable erps
create erps raps_vlan <vlanid 1-4094>
create erps ring <string 1-32>
delete erps raps_vlan <vlanid 1-4094>
delete erps ring <string 1-32>
config erps version [g.8032v1 | g.8032v2]
config erps raps_vlan <vlanid 1-4094> [state [enable | disable] | ring_mel <value 0-7> | ring_port [west [<port> | virtual_channel] | east [<port> | virtual_channel]] | rpl_port [west | east | none] | rpl_owner [enable | disable] | protected_vlan [add |delete] vlanid <vidlist> | sub_ring raps_vlan <vlanid 1-4094> tc_propagation state [enable | disable] | [add | delete] sub_ring raps_vlan <vlanid 1-4094> | revertive [enable | disable] | timer { holdoff_time <millisecond 0 - 10000> | guard_time <millisecond 10 - 2000> | wtr_time <min 1-12>}(1)]
config erps ring <string 1-32> [ring_port [west [<port> | virtual_channel] | east [<port> | virtual_channel]] | [add | delete] instance <value 1-16> | ring_type [major_ring | sub_ring] | ring_id <value 1-239>]
config erps instance <value 1-16> [state [enable | disable] | raps_vlan <vlanid 1-4094> | mel <value 0-7> | rpl_port [west | east | none] | rpl_role [owner | neighbour | none] | [add | delete] sub_ring_instance <value 1-16> | tc_propagation to instance <value 1-16> state [enable | disable] | timer [holdoff_time <millisecond 0 - 10000> | guard_time <millisecond 10 - 2000> | wtr_time <min 1-12>] | revertive [enable | disable] | protected_vlan [add | delete] vlanid <vidlist>]
config erps log [enable | disable]
config erps trap [enable | disable]
erps clear instance <value 1-16>
erps force switch instance <value 1-16> ring_port [west | east]
erps manual switch instance <value 1-16> ring_port [west | east]
show erps {[ring <string 1-32> | instance <value 1-16> {sub_ring_instance} | raps_vlan <vlanid 1-4094> {sub_ring}]}

34-1 enable erps

Description

This command is used to enable the global ERPS function on a switch. When both the global state and the specified ring ERPS state are enabled, the specified ring will be activated. The default state is disabled.

The global ERPS function cannot be enabled, when any ERPS ring on the device is enabled and the integrity of any ring parameter is not available. For each ring with the ring state enabled when ERPS is enabled, the following integrity will be checked:

1. R-APS VLAN is created.
2. The Ring port is a tagged member port of the R-APS VLAN.
3. The RPL port is specified if the RPL owner is enabled.
4. The RPL port is not specified as virtual channel.

NOTE: EEE and ERPS are mutually exclusive functions.

Format

enable erps

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable ERPS:

```
DGS-3000-28XMP:admin# enable erps
Command: enable erps

Success.

DGS-3000-28XMP:admin#
```

34-2 disable erps

Description

This command is used to disable the global ERPS function on a switch.

Format

disable erps

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To disable ERPS:

```
DGS-3000-28XMP:admin# disable erps
Command: disable erps

Success.

DGS-3000-28XMP:admin#
```

34-3 create erps raps_vlan

Description

This command is used to create an R-APS VLAN on a switch. Only one R-APS VLAN should be used to transfer R-APS messages.

NOTE: The R-APS VLAN must already have been created by the **create vlan** command.

Format

create erps raps_vlan <vlanid 1-4094>

Parameters

<vlanid 1-4094> - Enter the VLAN ID to be the R-APS VLAN.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To create an R-APS VLAN:

```
DGS-3000-28XMP:admin# create erps raps_vlan 4094
Command: create erps raps_vlan 4094

Success.

DGS-3000-28XMP:admin#
```

34-4 create erps ring

Description

This command is used to create a physical ring on the Switch.

Format

create erps ring <string 1-32>

Parameters

<string 1-32> - Enter the name of the physical ring. This can be up to 32 characters long.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To create a physical ring:

```
DGS-3000-28XMP:admin#create erps ring major_ring
Command: create erps ring major_ring

Success.

DGS-3000-28XMP:admin#
```

34-5 delete erps raps_vlan

Description

This command is used to delete an R-APS VLAN on a switch. When an R-APS VLAN is deleted, all parameters related to this R-APS VLAN will also be deleted. This command can only be issued when the ring is not active.

Format

delete erps raps_vlan <vlanid 1-4094>

Parameters

<vlanid 1-4094> - Enter the VLAN ID to be the R-APS VLAN.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete an R-APS VLAN:

```
DGS-3000-28XMP:admin# delete erps raps_vlan 4094
Command: delete erps raps_vlan 4094

Success.

DGS-3000-28XMP:admin#
```

34-6 delete erps ring

Description

This command is used to delete a physical ring on the Switch.

Format

delete erps ring <string 1-32>

Parameters

<string 1-32> - Enter the name of the physical ring. This can be up to 32 characters long.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete a physical ring:

```
DGS-3000-28XMP:admin#delete erps ring major_ring
Command: delete erps ring major_ring

Success.

DGS-3000-28XMP:admin#
```

34-7 config erps version

Description

This command is used to configure the ERPS version.

G.8032v1 was released by the ITU-T in June 2008 and G.8032v2 was released in February 2012.

G.8032v2 provides the following enhancements:

- Multiple instances are supported in a physical ring.
- The manual, force, and clear operation commands are supported.
- The Ring Automatic Protection Switching (R-APS) PDU destination address is sent with the ring ID of the physical ring.

Changing the ERPS version will restart the protocol and only the default instance will be active.

If two or more Ethernet ring nodes, running G.8032v1 and G.8032v2, co-exist on an Ethernet ring, the following configurations must be implemented on the G.8032v2 device(s):

- All physical ring IDs must be 1. This is the default value.
- The major ring instance and sub-ring instance of inter-connected nodes must have a different R-APS VID.
- The manual switch or force switch commands must not be enabled.
- The physical ring must have only one instance.

The RPL owner node should be upgraded to ERPSv2 ahead of other Ethernet ring nodes deployed on the same Ethernet ring.

Format

config erps version [g.8032v1 | g.8032v2]

Parameters

g.8032v1 - Specifies to use ERPSv1.
g.8032v2 - Specifies to use ERPSv2.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To use ERPSv1:

```
DGS-3000-28XMP:admin#config erps version g.8032v1
Command: config erps version g.8032v1

Success.

DGS-3000-28XMP:admin#
```

34-8 config erps raps_vlan

Description

This command is used to configure the ERPS R-APS VLAN settings.

The ring MEL is one field in the R-APS PDU. If CFM and ERPS are used at the same time, the R-APS PDU is one of a suite of Ethernet OAM PDU. The behavior for forwarding of R-APS PDU should follow the Ethernet OAM. If the MEL of R-APS PDU is not higher than the level of the MEP with the same VLAN on the ring ports, the R-APS PDU cannot be forwarded on the ring.

Restrictions apply for ports that are included in a link aggregation group. A link aggregation group can be configured as a ring port by specifying the master port of the link aggregation port. Only the master port can be specified as a ring port. If the specified link aggregation group is eliminated, the master port retains its ring port status. If the ring port configured on virtual channel, the ring which the port connects to will be considered as a sub-ring.

RPL port - Specifies one of the R-APS VLAN ring ports as the RPL port. To remove an RPL port from an R-APS VLAN, use the none designation for rpl_port.

RPL owner - Specifies the node as the RPL owner.

The virtual channel cannot be configured as RPL. For example, if a ring port is configured on the virtual channel and the ring port is configured as an RPL port, an error message will be display and the configuration will fail.

The R-APS VLAN cannot be the protected VLAN. The protected VLAN can be one that has already been created, or it can be used for a VLAN that has not yet been created.

Hold-off timer - The Hold-off timer is used to filter out intermittent link faults when link failures occur during the protection switching process. When a ring node detects a link failure, it will start the hold-off timer and report the link failure event (R-APS BPDU with SF flag) after the link failure is confirmed within period of time specified.

Guard timer - Guard timer is used to prevent ring nodes from receiving outdated R-APS messages. This timer is used during the protection switching process after the link failure recovers. When the link node detects the recovery of the link, it will report the link failure recovery event (R-APS PDU with NR flag) and start the guard timer. Before the guard timer expires, all received R-APS messages are ignored by this ring node, except in the case where a burst of three R-APS event messages that indicates the topology of a sub-ring has changed and the node needs to flush FDB are received on the node. In this case the recovered link does not go into a blocking state. The Guard Timer should be greater than the maximum expected forwarding delay for which one R-APS message circles around the ring.

WTR timer - WTR timer is used to prevent frequent operation of the protection switch due to an intermittent defect. This timer is used during the protection switching process when a link failure recovers. It is only used by the RPL owner. When the RPL owner in protection state receives R-APS PDU with an NR flag, it will start the WTR timer. The RPL owner will block the original unblocked RPL port and start to send R-APS PDU with an RB flag after the link recovery is confirmed within this period of time.

Revertive mode- When revertive is enabled, the traffic link is restored to the working transport link. When revertive is disabled, the traffic link is allowed to use the RPL, after recovering from a failure.

When both the global state and the specified ring ERPS state are enabled, the specified ring will be activated. STP and LBD should be disabled on the ring ports before the specified ring is activated.

The ring cannot be enabled before the R-APS VLAN is created, and ring ports, RPL port and RPL owner are configured. These parameters cannot be changed when the ring is activated.

In order to guarantee correct operation, the following integrity will be checked when the ring is enabled and the global ERPS state is enabled.

1. R-APS VLAN is created.
2. The Ring port is the tagged member port of the R-APS VLAN.
3. The RPL port is specified if RPL owner is enabled.
4. The RPL port is not a virtual channel.
5. The RPL port is the mater port when it belongs to a link aggregation group.

Format

config erps raps_vlan <vlanid 1-4094> [state [enable | disable] | ring_mel <value 0-7> | ring_port [west [<port> | virtual_channel] | east [<port> | virtual_channel]] | rpl_port [west | east | none] | rpl_owner [enable | disable] | protected_vlan [add |delete] vlanid <vidlist> | sub_ring raps_vlan <vlanid 1-4094> tc_propagation state [enable | disable] | [add | delete] sub_ring raps_vlan <vlanid 1-4094> | revertive [enable | disable] | timer { holdoff_time <millisecond 0 - 10000> | guard_time <millisecond 10 - 2000> | wtr_time <min 1-12>}(1)]

Parameters

<vlanid 1-4094> - Enter the VLAN ID used here.
state - Specifies to enable or disable the specified ring. **enable** - Specifies to enable the state of the specified ring. **disable** - Specifies to disable the state of the specified ring. This is the default value.
ring_mel - Specifies the ring MEL of the R-APS function. The default ring MEL is 1. **<value 0-7>** - Enter the ring MEL value here. This value should be between 0 and 7.
ring_port - Specifies the ring port used. **west** - Specifies that the port or the virtual channel will be associated with the west ring port.

<port> - Enter the port number here.
virtual_channel - Specifies that the virtual channel will be associated with the west ring port.
east - Specifies that the port or the virtual channel will be associated with the east ring port.
<port> - Enter the port number here.
virtual_channel - Specifies that the virtual channel will be associated with the east ring port.

rpl_port - Specifies the RPL port used.
west - Specifies the west ring port as the RPL port.
east - Specifies the east ring port as the RPL port.
none - No RPL port on this node. By default, the node has no RPL port.

rpl_owner - Specifies to enable or disable the RPL owner node.
enable - Specifies the device as an RPL owner node.
disable - Specifies that this node is not an RPL owner. This is the default value.

protected_vlan - Specifies to add or delete the protected VLAN group.
add - Specifies to add VLANs to the protected VLAN group.
delete - Specifies to delete VLANs from the protected VLAN group.
vlanid - Specifies the VLAN ID to be removed or added.
<vidlist> - Enter the VLAN ID list here.

sub_ring - Specifies that the sub-ring is being configured.
raps_vlan - Specifies the R-APS VLAN.
<vlanid 1-4094> - Enter the VLAN ID used here.
tc_propogation - Specifies to configure the state of the topology change propagation for the sub-ring.
state - Specifies the propagation state of the topology change for the sub-ring.
enable - Specifies to enable the propagation state of the topology change for the sub-ring.
disable - Specifies to disable the propagation state of the topology change for the sub-ring.

add - Specifies to add a topology change propagation rule.
delete - Specifies to delete a topology change propagation rule.
sub_ring - Specifies the sub-ring configuration information.
raps_vlan - Specifies the R-APS VLAN.
<vlanid 1-4094> - Enter the R-APS VLAN ID used here.

revertive - Specifies the state of the R-APS revertive option.
enable - Specifies that the R-APS revertive option will be enabled.
disable - Specifies that the R-APS revertive option will be disabled.

timer - Specifies the R-APS timer used.
holdoff_time - Specifies the holdoff time of the R-APS function. The default holdoff time is 0 millisecond.
<millisecond 0 - 10000> - Enter the hold off time value here. This value must be in the range of 0 to 10000 milliseconds.
guard_time - Specifies the guard time of the R-APS function. The default guard time is 500 milliseconds.
<millisecond 10 - 2000> - Enter the guard time value here. This value must be in the range of 10 to 2000 milliseconds.
wtr_time - Specifies the WTR time of the R-APS function.
<min 1-12> - Enter the WTR time range value here. The range is from 1 to 12 minutes. The default WTR time is 5 minutes.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the MEL of the ERPS ring for a specific R-APS VLAN:

```
DGS-3000-28XMP:admin# config erps raps_vlan 4094 ring_mel 2
Command: config erps raps_vlan 4094 ring_mel 2

Success.

DGS-3000-28XMP:admin#
```

To configure the ports of the ERPS ring for a specific R-APS VLAN:

```
DGS-3000-28XMP:admin# config erps raps_vlan 4094 ring_port west 5
Command: config erps raps_vlan 4094 ring_port west 5

Success.

DGS-3000-28XMP:admin#
```

To configure the RPL owner for a specific R-APS VLAN:

```
DGS-3000-28XMP:admin# config erps raps_vlan 4094 rpl_owner enable
Command: config erps raps_vlan 4094 rpl_owner enable

Success.

DGS-3000-28XMP:admin#
```

To configure the protected VLAN for a specific R-APS VLAN:

```
DGS-3000-28XMP:admin# config erps raps_vlan 4094 protected_vlan add vlanid 10-20
Command: config erps raps_vlan 4094 protected_vlan add vlanid 10-20

Success.

DGS-3000-28XMP:admin#
```

To configure the ERPS timers for a specific R-APS VLAN:

```
DGS-3000-28XMP:admin# config erps raps_vlan 4094 timer holdoff_time 100 guard_time 1000
wtr_time 10
Command: config erps raps_vlan 4094 timer holdoff_time 100 guard_time 1000 wtr_time 10

Success.

DGS-3000-28XMP:admin#
```

To configure the ring state of the ERPS:

```
DGS-3000-28XMP:admin# config erps raps_vlan 4094 state enable
Command: config erps raps_vlan 4094 state enable

Success.

DGS-3000-28XMP:admin#
```

34-9 config erps ring

Description

This command is used to the ERPS ring.

Format

config erps ring <string 1-32> [ring_port [west [<port> | virtual_channel] | east [<port> | virtual_channel]] | [add | delete] instance <value 1-16> | ring_type [major_ring | sub_ring] | ring_id <value 1-239>]

Parameters

<string 1-32> - Enter the name of the physical ring. This can be up to 32 characters long.
ring_port - Specifies the ring port used. **west** - Specifies that the port or the virtual channel will be associated with the west ring port. **<port>** - Enter the port number here. **virtual_channel** - Specifies that the virtual channel will be associated with the west ring port. **east** - Specifies that the port or the virtual channel will be associated with the east ring port. **<port>** - Enter the port number here. **virtual_channel** - Specifies that the virtual channel will be associated with the east ring port.
add - Specifies to add a ring instance. **delete** - Specifies to delete a ring instance. **instance** - Specifies the ID of the ring instance. **<value 1-16>>** - Enter the instance here. This value should be between 1 and 16.
ring_type - Specifies the ring type. This parameter is for ERPSv2 only. **major_ring** - Specifies the ring as the major ring. **sub_ring** - Specifies the ring as the sub ring.
ring_id - Specifies the ID of the physical ring. This parameter is for ERPSv2 only. **<value 1-239>** - Enter the ring ID here. This value should be between 1 and 239.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the physical ring to be associated with the west ring port 1:

```
DGS-3000-28XMP:admin#config erps ring erps_ring ring_port west 1
Command: config erps ring erps_ring ring_port west 1

Success.

DGS-3000-28XMP:admin#
```

To add ring instance:

```
DGS-3000-28XMP:admin#config erps ring erps_ring add instance 2
Command: config erps ring erps_ring add instance 2

Success.

DGS-3000-28XMP:admin#
```

To configure the type of the physical ring:

```
DGS-3000-28XMP:admin#config erps ring erps_ring ring_type major_ring
Command: config erps ring erps_ring ring_type major_ring

Success.

DGS-3000-28XMP:admin#
```

To configure the ID of the physical ring:

```
DGS-3000-28XMP:admin#config erps ring erps_ring ring_id 25
Command: config erps ring erps_ring ring_id 25

Success.

DGS-3000-28XMP:admin#
```

34-10 config erps instance

Description

This command is used to configure ERPS instance.

When the specified ring instance is enabled, the specified ring instance will be activated. STP and LBD should be disabled on the physical ring ports before the specified ring instance is activated.

The instance cannot be enabled before the R-APS VLAN is designated, and physical ring ports, RPL port and RPL owner are configured. These parameters cannot be changed when the instance is activated.

In order to guarantee correct operation, the following integrity will be checked when the instance is enabled.

1. R-APS VLAN is designated.
2. The physical ring port is the tagged member port of the R-APS VLAN.
3. The RPL port is specified if RPL owner or neighbor is designated.
4. STP or LBD is enabled on the physical ring port.
5. The instance is sub-ring instance but the virtual channel does not exist.

6. The ring port is the mater port when it belongs to a link aggregation group.

The instance R-APS VLAN is used to transfer R-APS messages.

The ring MEL is one field in the R-APS PDU. If CFM and ERPS are used at the same time, the R-APS PDU is one of a suite of Ethernet OAM PDU. The behavior for forwarding of R-APS PDU should follow the Ethernet OAM. If the MEL of R-APS PDU is not higher than the level of the MEP with the same VLAN on the ring ports, the R-APS PDU cannot be forwarded on the ring.

RPL port - Specifies one of the instance ring ports as the RPL port. To remove an RPL port from an instance, use the none designation for rpl_port.

RPL role - Specifies the node's role.

The virtual channel cannot be configured as RPL. For example, if a ring port is configured on the virtual channel and the ring port is configured as an RPL port, an error message will be display and the configuration will fail.

Hold-off timer - The Hold-off timer is used to filter out intermittent link faults when link failures occur during the protection switching process. When a ring node detects a link failure, it will start the hold-off timer and report the link failure event (R-APS BPDU with SF flag) after the link failure is confirmed within period of time specified.

Guard timer - Guard timer is used to prevent ring nodes from receiving outdated R-APS messages. This timer is used during the protection switching process after the link failure recovers. When the link node detects the recovery of the link, it will report the link failure recovery event (R-APS PDU with NR flag) and start the guard timer. Before the guard timer expires, all received R-APS messages are ignored by this ring node, except in the case where a burst of three R-APS event messages that indicates the topology of a sub-ring has changed and the node needs to flush FDB are received on the node. In this case the recovered link does not go into a blocking state. The Guard Timer should be greater than the maximum expected forwarding delay for which one R-APS message circles around the ring.

WTR timer - WTR timer is used to prevent frequent operation of the protection switch due to an intermittent defect. This timer is used during the protection switching process when a link failure recovers. It is only used by the RPL owner. When the RPL owner in protection state receives R-APS PDU with an NR flag, it will start the WTR timer. The RPL owner will block the original unblocked RPL port and start to send R-APS PDU with an RB flag after the link recovery is confirmed within this period of time.

Revertive mode- When revertive is enabled, the traffic link is restored to the working transport link. In order to clear intermittent faults, the traffic channel reverts when the WTR timer expires. When revertive is disabled, the traffic link is allowed to use the RPL, after recovering from a failure. Since in ERPS, the working transport entity resources may be more optimized. In some cases it is desirable to revert to this working transport entity once all ring links are available.

This is performed at the expense of an additional traffic interruption. In some cases, there may be no advantage to revert to the working transport entities immediately. In this case, a second traffic interruption is avoided by not reverting protection switching.

The instance R-APS VLAN cannot be the protected VLAN.

Format

config erps instance <value 1-16> [state [enable | disable] | raps_vlan <vlanid 1-4094> | mel <value 0-7> | rpl_port [west | east | none] | rpl_role [owner | neighbour | none] | [add | delete] sub_ring_instance <value 1-16> | tc_propagation to instance <value 1-16> state [enable | disable] | timer [holdoff_time <millisecond 0 - 10000> | guard_time <millisecond 10 - 2000> | wtr_time <min 1-12>] | revertive [enable | disable] | protected_vlan [add | delete] vlanid <vidlist>]

Parameters

<value 1-16> - Enter the instance here. This value should be between 1 and 16.

state - Specifies to enable or disable the specified ring instance.
enable - Specifies to enable the state of the specified ring instance.
disable - Specifies to disable the state of the specified ring instance. This is the default value.

raps_vlan - Specifies the instance R-APS VLAN.
<vlanid 1-4094> - Enter the VLAN ID designated for the instance.

mel - Specifies the MEL of the ERPS instance. The default ring MEL is 1.
<value 0-7> - Enter the ring MEL value here. This value should be between 0 and 7.

rpl_port - Specifies the RPL port used.
west - Specifies the west ring port as the RPL port.
east - Specifies the east ring port as the RPL port.
none - No RPL port on this node. By default, the node has no RPL port.

rpl_role - Specifies the RPL role.
owner - Specifies the device as an RPL owner node.
neighbour - Specifies the device as an RPL neighbor node. This parameter is for ERPSv2 only.
none - Specifies that there is no role on this node. This is the default value.

add - Specifies to connect a sub-ring to another ring instance.
delete - Specifies to disconnect a sub-ring to another ring instance.
sub_ring_instance - Specifies the sub-ring instance.
<value 1-16> - Enter the instance here.

tc_propogation - Specifies to configure the state of the topology change propagation for the sub-ring instance.
to instance - Specifies ERPS instance.
<value 1-16> - Enter the instance here.
state - Specifies the propagation state of the topology change for the sub-ring instance.
enable - Specifies to enable the propagation state of the topology change for the sub-ring instance.
disable - Specifies to disable the propagation state of the topology change for the sub-ring instance.

timer - Specifies the R-APS timer used.
holdoff_time - Specifies the holdoff time of the R-APS function. The default holdoff time is 0 millisecond.
<millisecond 0 - 10000> - Enter the hold off time value here. This value must be in the range of 0 to 10000 milliseconds.
guard_time - Specifies the guard time of the R-APS function. The default guard time is 500 milliseconds.
<millisecond 10 - 2000> - Enter the guard time value here. This value must be in the range of 10 to 2000 milliseconds.
wtr_time - Specifies the WTR time of the R-APS function.
<min 1-12> - Enter the WTR time range value here. The range is from 1 to 12 minutes. The default WTR time is 5 minutes.

revertive - Specifies the state of the R-APS revertive option.
enable - Specifies that the R-APS revertive option will be enabled.
disable - Specifies that the R-APS revertive option will be disabled.

protected_vlan - Specifies to add or delete the protected VLAN group.
add - Specifies to add VLANs to the protected VLAN group.
delete - Specifies to delete VLANs from the protected VLAN group.
vlanid - Specifies the VLAN ID to be removed or added.
<vidlist> - Enter the VLAN ID list here.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the ring state of the ERPS instance:

```
DGS-3000-28XMP:admin#config erps instance 1 state enable
Command: config erps instance 1 state enable

Success.

DGS-3000-28XMP:admin#
```

To create an instance R-APS VLAN:

```
DGS-3000-28XMP:admin#config erps instance 1 raps_vlan 10
Command: config erps instance 1 raps_vlan 10

Success.

DGS-3000-28XMP:admin#
```

To configure the MEL of the ERPS ring instance for a specific R-APS VLAN:

```
DGS-3000-28XMP:admin#config erps instance 1 mel 2
Command: config erps instance 1 mel 2

Success.

DGS-3000-28XMP:admin#
```

To configure the RPL port of the ERPS ring instance:

```
DGS-3000-28XMP:admin#config erps instance 1 rpl_port west
Command: config erps instance 1 rpl_port west

Success.

DGS-3000-28XMP:admin#
```

To configure the RPL role of the ERPS ring instance:

```
DGS-3000-28XMP:admin#config erps instance 1 rpl_role owner
Command: config erps instance 1 rpl_role owner

Success.

DGS-3000-28XMP:admin#
```

To configure the sub-ring instance:

```
DGS-3000-28XMP:admin#config erps instance 1 add sub_ring_instance 2
Command: config erps instance 1 add sub_ring_instance 2

Success.

DGS-3000-28XMP:admin#
```

To enable the topology change for the sub-ring instance:

```
DGS-3000-28XMP:admin#config erps instance 1 tc_propagation to instance 2 state enable
Command: config erps instance 1 tc_propagation to instance 2 state enable

Success.

DGS-3000-28XMP:admin#
```

To configure the ERPS timers for instance 1:

```
DGS-3000-28XMP:admin#config erps instance 1 timer holdoff_time 500
Command: config erps instance 1 timer holdoff_time 500

Success.

DGS-3000-28XMP:admin#
```

To configure the protected VLAN for instance 1:

```
DGS-3000-28XMP:admin#config erps instance 1 protected_vlan add vlanid 11-20
Command: config erps instance 1 protected_vlan add vlanid 11-20

Success.

DGS-3000-28XMP:admin#
```

34-11 config erps log

Description

This command is used to configure the log state of ERPS events.

Format

config erps log [enable | disable]

Parameters

enable - Specifies to enable the log state.
disable - Specifies to disable the log state. This is the default option.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the ERPS log state:

```
DGS-3000-28XMP:admin# config erps log enable
Command: config erps log enable

Success.

DGS-3000-28XMP:admin#
```

34-12 config erps trap

Description

This command is used to configure the trap state of ERPS events.

Format

config erps trap [enable | disable]

Parameters

enable - Specifies to enable the trap state.
disable - Specifies to disable the trap state. This is the default option.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the trap state of the ERPS:

```
DGS-3000-28XMP:admin# config erps trap enable
Command: config erps trap enable

Success.

DGS-3000-28XMP:admin#
```

34-13 erps clear instance

Description

This command is used to clear the local active administrative command.

NOTE: This command is for ERPSv2 only.

Format

erps clear instance <value 1-16>

Parameters

<value 1-16> - Enter the instance here. This value should be between 1 and 16.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To clear ERPS instance 1:

```
DGS-3000-28XMP:admin#erps clear instance 1
Command: erps clear instance 1

Success.

DGS-3000-28XMP:admin#
```

34-14 erps force switch instance

Description

This command is used to block the specified instance ring port immediately.

NOTE: This command is for ERPSv2 only.

Format

erps force switch instance <value 1-16> ring_port [west | east]

Parameters

<value 1-16> - Enter the instance here. This value should be between 1 and 16.

ring_port - Specifies the ring port used.
- **west** - Specifies to block the west ring port.
- **east** - Specifies to block the east ring port.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To block ERPS instance 1 east port immediately:

```
DGS-3000-28XMP:admin#erps force switch instance 1 ring_port east
Command: erps force switch instance 1 ring_port east

Success.

DGS-3000-28XMP:admin#
```

34-15 erps manual switch instance

Description

This command is used to manually block the specified instance ring port on which an MS is configured when the link fails and FS conditions are absent.

NOTE: This command is for ERPSv2 only.

Format

erps manual switch instance <value 1-16> ring_port [west | east]

Parameters

<value 1-16> - Enter the instance here. This value should be between 1 and 16.
ring_port - Specifies the ring port used. **west** - Specifies to block the west ring port. **east** - Specifies to block the east ring port.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To manually block ERPS instance 1 west port:

```
DGS-3000-28XMP:admin#erps manual switch instance 1 ring_port west
Command: erps manual switch instance 1 ring_port west

Success.

DGS-3000-28XMP:admin#
```

34-16 show erps

Description

This command is used to display ERPS configuration and operation information.

The port state of the ring port may be as "Forwarding", "Blocking", or "Signal Fail". "Forwarding" indicates that traffic is able to be forwarded. "Blocking" indicates that traffic is blocked by ERPS and a signal failure is not detected on the port. "Signal Fail" indicates that a signal failure is detected on the port and traffic is blocked by ERPS.

The RPL role could be configured to "Owner", “Neighbor” or "None".

Format

show erps {[ring <string 1-32> | instance <value 1-16> {sub_ring_instance} | raps_vlan <vlanid 1-4094> {sub_ring}]}

Parameters

None.

Restrictions

None.

Example

To display ERPS information:

```
DGS-3000-28XMP:admin#show erps
Command: show erps

 Global Status  : Enabled
 Log Status     : Disabled
 Trap Status    : Disabled
 Global Version : G.8032v1
 ----------------------------------
 Ethernet Ring   : major_ring
 West            : 0
 East            : 0
 ----------------------------------
 Ethernet Ring   : erps_ring
 West            : 1
 East            : 0
 ----------------------------------
 Instance                          : 2
 Instance Status                   : Disabled
 Instance R-APS VLAN               : 0
 West                              : 1 (Forwarding)
 East                              : 0 (Forwarding)
 RPL Port                          : -
 RPL Role                          : None
 Protected VLANs                   :
 Instance MEL                      : 1
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

To display the ERPS R-APS VLAN settings:

```
DGS-3000-28XMP:admin#show erps raps_vlan 4094
Command: show erps raps_vlan 4094

 Ethernet Ring   : ring_4094
 West            : 5
 East            : 0
 ----------------------------------
 Instance                          : 1
 Instance Status                   : Disabled
 Instance R-APS VLAN               : 4094
 West                              : 5 (Forwarding)
 East                              : 0 (Forwarding)
 RPL Port                          : -
 RPL Role                          : Owner
 Protected VLANs                   : 10-20
 Instance MEL                      : 2
 Holdoff Time                      : 100 milliseconds
 Guard Time                        : 500 milliseconds
 WTR Time                          : 5 minutes
 Revertive Mode                    : Enabled
 Current Instance State            : Deactivated

DGS-3000-28XMP:admin#
```

To display the sub-ring of ERPS R-APS VLAN settings:

```
DGS-3000-28XMP:admin#show erps raps_vlan 4094 sub_ring
Command: show erps raps_vlan 4094 sub_ring

 Instance  1
 Sub-Ring instance              TC Propagation State
 -----------------              ----------------
 5                              Enable
 6                              Enable

DGS-3000-28XMP:admin#
```

To display the information of the physical ring:

```
DGS-3000-28XMP:admin#show erps ring erps_ring
Command: show erps ring erps_ring

 Global Status  : Enabled
 Log Status     : Disabled
 Trap Status    : Disabled
 Global Version : G.8032v1
 Ethernet Ring   : erps_ring
 West            : 1
 East            : 0
 ------------------------------------
 Instance                          : 2
 Instance Status                   : Disabled
 Instance R-APS VLAN               : 0
 West                              : 1 (Forwarding)
 East                              : 0 (Forwarding)
 RPL Port                          : -
 RPL Role                          : None
 Protected VLANs                   :
 Instance MEL                      : 1
 Holdoff Time                      : 0 milliseconds
 Guard Time                        : 500 milliseconds
 WTR Time                          : 5 minutes
 Revertive Mode                    : Enabled
 Current Instance State            : Deactivated

DGS-3000-28XMP:admin#
```

To display the information of the ring instance 1:

```
DGS-3000-28XMP:admin#show erps instance 1
Command: show erps instance 1

 Instance                          : 1
 Instance Status                   : Disabled
 Instance R-APS VLAN               : 4094
 West                              : 5 (Forwarding)
 East                              : 0 (Forwarding)
 RPL Port                          : -
 RPL Role                          : Owner
 Protected VLANs                   : 10-20
 Instance MEL                      : 2
 Holdoff Time                      : 100 milliseconds
 Guard Time                        : 500 milliseconds
 WTR Time                          : 5 minutes
 Revertive Mode                    : Enabled
 Current Instance State            : Deactivated

DGS-3000-28XMP:admin#
```

Chapter 35 Filter Command List

config filter netbios [<portlist> | all] state [enable | disable]
show filter netbios
config filter extensive_netbios [<portlist> | all] state [enable | disable]
show filter extensive_netbios

35-1 config filter netbios

Description

This command is used to configure the Switch to deny NetBIOS packets on specific ports.

Format

config filter netbios [<portlist> | all] state [enable | disable]

Parameters

<portlist> - Specifies the list of ports used.
all - Specifies that all the ports will be used for the configuration.
state- Specifies the state of the NetBIOS packet filter. **enable** - Specifies to deny NetBIOS packets through the specified ports. **disable** - Specifies to allow NetBIOS packets through the specified ports.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure filter NetBIOS state:

```
DGS-3000-28XMP:admin# config filter netbios 1-10 state enable
Command: config filter netbios 1-10 state enable

Success.

DGS-3000-28XMP:admin#
```

35-2 show filter netbios

Description

This command is used to display the NetBIOS filter state on the Switch.

Format

show filter netbios

Parameters

None.

Restrictions

None.

Example

To display the filter NetBIOS list created on the Switch:

```
DGS-3000-28XMP:admin# show filter netbios
Command: show filter netbios

Enabled ports: 1-3

DGS-3000-28XMP:admin#
```

35-3 config filter extensive_netbios

Description

This command is used to configure the Switch to filter NetBIOS packets over 802.3 frames on the specific ports.

Format

config filter extensive_netbios [<portlist> | all] state [enable | disable]

Parameters

<portlist> - Enter the list of ports used for this configuration here.
all - Specifies that all the ports will be used this configuration.
state - Specifies to enable or disable the NetBIOS packet filter over 802.3 frames. **enable** - Specifies that the filter state will be enabled. **disable** - Specifies that the filter state will be disabled.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure filter extensive NetBIOS state:

```
DGS-3000-28XMP:admin# config filter extensive_netbios 1-10 state enable
Command: config filter extensive_netbios 1-10 state enable

Success.

DGS-3000-28XMP:admin#
```

35-4 show filter extensive_netbios

Description

This command is used to display the extensive NetBIOS state on the Switch.

Format

show filter extensive_netbios

Parameters

None.

Restrictions

None.

Example

To display the extensive state created on the Switch:

```
DGS-3000-28XMP:admin# show filter extensive_netbios
Command: show filter extensive_netbios

Enabled ports: 1-3

DGS-3000-28XMP:admin#
```

Chapter 36 Filter Database (FDB) Command List

create fdb <vlan_name 32> <macaddr> [port <port> | drop]
create fdb vlanid <vidlist> <macaddr> [port <port> | drop]
create multicast_fdb <vlan_name 32> <macaddr>
config multicast_fdb <vlan_name 32> <macaddr> [add | delete] <portlist>
config fdb aging_time <sec 10-1000000>
config multicast vlan_filtering_mode [vlanid <vidlist> | vlan <vlan_name 32> | all] [forward_all_groups | forward_unregistered_groups | filter_unregistered_groups]
delete fdb <vlan_name 32> <macaddr>
clear fdb [vlan <vlan_name 32> | port <port> | all]
show multicast_fdb {[vlan <vlan_name 32> | vlanid <vidlist>] | mac_address <macaddr>}
show fdb {port <port> | [vlan <vlan_name 32> | vlanid <vidlist>] | mac_address <macaddr> | static | aging_time | security}
show multicast vlan_filtering_mode {[vlanid < vidlist> | vlan <vlan_name 32>]}

36-1 create fdb

Description

This command is used to create a static entry in the unicast MAC address forwarding table (database) based on the VLAN name.

Format

create fdb <vlan_name 32> <macaddr> [port <port> | drop]

Parameters

<vlan_name 32> - Specifies a VLAN name associated with a MAC address. The maximum length of the VLAN name is 32 bytes.
<macaddr> - Specifies the MAC address to be added to the static forwarding table.
port - Specifies the port number corresponding to the MAC destination address. The Switch will always forward traffic to the specified device through this port. **<port>** - Enter the port number corresponding to the MAC destination address here.
drop - Specifies the drop action to be taken.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To create a unicast MAC forwarding entry:

```
DGS-3000-28XMP:admin# create fdb default 00-00-00-00-01-02 port 5
Command: create fdb default 00-00-00-00-01-02 port 5

Success.

DGS-3000-28XMP:admin#
```

To filter a unicast MAC:

```
DGS-3000-28XMP:admin# create fdb default 00-00-00-00-01-02 drop
Command: create fdb default 00-00-00-00-01-02 drop

Success.

DGS-3000-28XMP:admin#
```

36-2 create fdb vlanid

Description

This command is used to create a static entry in the unicast MAC address forwarding table (database) based on the VLAN ID.

Format

create fdb vlanid <vidlist> <macaddr> [port <port> | drop]

Parameters

<vidlist> - Specifies a VLAN ID associated with a MAC address.
<macaddr> - Specifies the MAC address to be added to the static forwarding table.
port - Specifies the port number corresponding to the MAC destination address. The Switch will always forward traffic to the specified device through this port. **<port>** - Enter the port number corresponding to the MAC destination address here.
drop - Specifies the drop action to be taken.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To create a unicast MAC forwarding entry:

```
DGS-3000-28XMP:admin# create fdb vlanid 1 00-00-00-00-02-02 port 5
Command: create fdb vlanid 1 00-00-00-00-02-02 port 5

Success.

DGS-3000-28XMP:admin#
```

To filter a unicast MAC:

```
DGS-3000-28XMP:admin# create fdb vlanid 1 00-00-00-00-02-02 drop
Command: create fdb vlanid 1 00-00-00-00-02-02 drop

Success.

DGS-3000-28XMP:admin#
```

36-3 create multicast_fdb

Description

This command is used to create a static entry in the multicast MAC address forwarding table (database).

Format

create multicast_fdb <vlan_name 32> <macaddr>

Parameters

<vlan_name 32> - Enter the name of the VLAN on which the MAC address resides. The maximum name length is 32.
<macaddr> - Enter the multicasts MAC address to be added to the static forwarding table.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To create a multicast MAC forwarding entry to the default VLAN:

```
DGS-3000-28XMP:admin# create multicast_fdb default 01-00-5E-00-00-00
Command: create multicast_fdb default 01-00-5E-00-00-00

Success.

DGS-3000-28XMP:admin#
```

36-4 config multicast_fdb

Description

This command is used to configure the Switch's multicast MAC address forwarding database.

Format

config multicast_fdb <vlan_name 32> <macaddr> [add | delete] <portlist>

Parameters

<vlan_name 32> - Enter the name of the VLAN on which the MAC address resides. The maximum name length is 32.
<macaddr> - Enter the MAC address that will be added or deleted to the forwarding table.
add - Specifies to add ports to the multicast forwarding table.
delete - Specifies to remove ports from the multicast forwarding table.
<portlist> - Enter a range of ports to be configured.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To add a multicast MAC forwarding entry to the default VLAN on port 1 to 5:

```
DGS-3000-28XMP:admin# config multicast_fdb default 01-00-5E-00-00-00 add 1-5
Command: config multicast_fdb default 01-00-5E-00-00-00 add 1-5

Success.

DGS-3000-28XMP:admin#
```

36-5 config fdb aging_time

Description

This command is used to configure the MAC address table aging time. 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. 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.

Format

config fdb aging_time <sec 10-1000000>

Parameters

<sec 10-1000000> - Enter the FDB age out time between 10 to 1000000 seconds. The default value is 300 seconds.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the MAC address table aging time to 600 seconds:

```
DGS-3000-28XMP:admin# config fdb aging_time 600
Command: config fdb aging_time 600

Success.

DGS-3000-28XMP:admin#
```

36-6 config multicast vlan_filtering_mode

Description

This command is used to configure the multicast packet filtering mode for VLANs.

The registered group will be forwarded to the range of ports in the multicast forwarding database.

Format

config multicast vlan_filtering_mode [vlanid <vidlist> | vlan <vlan_name 32> | all] [forward_all_groups | forward_unregistered_groups | filter_unregistered_groups]

Parameters

vlanid - Specifies a list of VLANs to be configured. **<vidlist>** - Enter the VLAN ID list here.
vlan - Specifies the name of the VLAN. The maximum name length is 32. **<vlan_name 32>** - Enter the VLAN name can be up to 32 characters long.
all - Specifies all configured VLANs.
forward_all_groups - Specifies that both the registered group and the unregistered group will be forwarded to all member ports of the specified VLAN where the multicast traffic comes in.
forward_unregistered_groups - Specifies that the unregistered group will be forwarded to all member ports of the VLAN where the multicast traffic comes in.
filter_unregistered_groups - Specifies that the unregistered group will be filtered.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the multicast packet filtering mode to filter all unregistered multicast groups for the VLAN 200 to 300:

```
DGS-3000-28XMP:admin# config multicast vlan_filtering_mode vlanid 200-300
filter_unregistered_groups
Command: config multicast vlan_filtering_mode vlanid 200-300 filter_unregistered_groups

Success.

DGS-3000-28XMP:admin#
```

36-7 delete fdb

Description

This command is used to delete a static entry from the forwarding database.

Format

delete fdb <vlan_name 32> <macaddr>

Parameters

<vlan_name 32> - Enter the name of the VLAN on which the MAC address resides. The maximum name length is 32.
<macaddr> - Enter the multicast MAC address to be deleted from the static forwarding table.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete a static FDB entry:

```
DGS-3000-28XMP:admin# delete fdb default 00-00-00-00-01-02
Command: delete fdb default 00-00-00-00-01-02

Success.

DGS-3000-28XMP:admin#
```

36-8 clear fdb

Description

This command is used to clear the Switch's forwarding database for dynamically learned MAC addresses.

Format

clear fdb [vlan <vlan_name 32> | port <port> | all]

Parameters

vlan - Specifies to clear the FDB entry by specifying the VLAN name. **<vlan_name 32>** - Enter the name of the VLAN on which the MAC address resides. The maximum name length is 32.
port - Specifies to clear the FDB entry by specifying the port number. **<port>** - Enter the port number corresponding to the MAC destination address.
all - Specifies to clear all dynamic entries in the Switch's forwarding database.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To clear all FDB dynamic entries:

```
DGS-3000-28XMP:admin# clear fdb all
Command: clear fdb all

Success.

DGS-3000-28XMP:admin#
```

36-9 show multicast_fdb

Description

This command is used to display the multicast forwarding database of the Switch.

Format

show multicast_fdb {[vlan <vlan_name 32> | vlanid <vidlist>] | mac_address <macaddr>}

Parameters

vlan - (Optional) Specifies the name of the VLAN on which the MAC address resides. **<vlan_name 32>** - Enter the VLAN name here. The VLAN name can be up to 32 characters long.
vlanid - (Optional) Specifies to display the entries for the VLANs indicated by VID list. **<vidlist>** - Enter the VLAN ID list here.
mac_address - (Optional) Specifies a MAC address, for which FDB entries will be displayed. **<macaddr>** - Enter the MAC address here.
If no parameter is specified, all multicast FDB entries will be displayed.

Restrictions

None.

Example

To display the multicast MAC address table:

```
DGS-3000-28XMP:admin# show multicast_fdb
Command: show multicast_fdb


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


Total Entries: 1


DGS-3000-28XMP:admin#
```

36-10 show fdb

Description

This command is used to display the current unicast MAC address forwarding database.

Format

show fdb {port <port> | [vlan <vlan_name 32> | vlanid <vidlist>] | mac_address <macaddr> | static | aging_time | security}

Parameters

port - (Optional) Specifies to display the entries for a specified port. **<port>** - Enter the port number here.
vlan - (Optional) Specifies to display the entries for a specific VLAN. The maximum name length is 32. **<vlan_name 32>** - Enter the VLAN name here. The VLAN name can be up to 32 characters long.
vlanid - (Optional) Specifies to display the entries for the VLANs indicated by VID list. **<vidlist>** - Enter the VLAN ID list here.
mac_address - (Optional) Specifies to display a specific MAC address. **<macaddr>** - Enter the MAC address here.
static - (Optional) Specifies to display all permanent entries.
aging_time - (Optional) Specifies to display the unicast MAC address aging time.
security - (Optional) Specifies to display the FDB entries that are created by the security module.
If no parameter is specified, system will display the unicast address table.

Restrictions

None.

Example

To display the FDB table:

```
DGS-3000-28XMP:admin# show fdb
Command: show fdb

 Unicast MAC Address Aging Time  = 300

 VID  VLAN Name                         MAC Address       Port  Type    Status
 ---- --------------------------------- ----------------- ----- ------- -------
 1    default                           00-01-02-03-04-00 CPU   Self    Forward
 1    default                           00-23-7D-BC-08-44 1     Dynamic Forward
 1    default                           00-23-7D-BC-2E-18 1     Dynamic Forward
 1    default                           00-26-5A-AE-CA-1C 1     Dynamic Forward
 1    default                           60-33-4B-C4-52-1A 1     Dynamic Forward

Total Entries: 5

DGS-3000-28XMP:admin#
```

To display the security FDB table:

```
DGS-3000-28XMP:admin# show fdb security
Command: show fdb security


VID  MAC Address         Port   Type    Status   Security Module
---- ---------------   ----- ------- -------- ---------------
1    00-00-00-10-00-01  1    Dynamic  Drop      802.1X
1    00-00-00-10-00-02  2    Static   Forward   WAC
1    00-00-00-10-00-04  4    Static   Forward   Port Security
1    00-00-00-10-00-0A  5    Static   Forward   MAC-based Access Control
1    00-00-00-10-00-06  6    Dynamic  Drop       Compound Authentication
Total Entries: 5

DGS-3000-28XMP:admin#
```

36-11 show multicast vlan_filtering_mode

Description

This command is used to show the multicast packet filtering mode for VLANs.

NOTE: A product that supports the multicast VLAN filtering mode cannot support the port filtering mode at the same time.

Format

show multicast vlan_filtering_mode {[vlanid < vidlist> | vlan <vlan_name 32>]}

Parameters

vlanid - (Optional) Specifies a list of VLANs to be configured.

<vidlist> - Enter the VLAN ID list here.
vlan - (Optional) Specifies the name of the VLAN. The maximum name length is 32. **<vlan_name 32>** - Enter the VLAN name here. The VLAN name can be up to 32 characters long.
If no parameter is specified, the device will show all multicast filtering settings in the device.

Restrictions

None.

Example

To show the multicast vlan_filtering_mode for VLANs:

```
DGS-3000-28XMP:admin# show multicast vlan_filtering_mode
Command: show multicast vlan_filtering_mode

VLAN ID/VLAN Name                          Multicast Filter Mode
-----------------------------------------  ----------------------------
1   /default                               forward_unregistered_groups

DGS-3000-28XMP:admin#
```

Chapter 37 Flash File System (FFS) Command List

show storage_media_info
md {<drive_id>} <pathname>
rd {<drive_id>} <pathname>
cd {<pathname>}
dir {<drive_id>} {<pathname>}
rename {<drive_id>} <pathname> <filename>
del {<drive_id>} <pathname> {recursive}
erase {<drive_id>} <pathname>
move {<drive_id>} <pathname> {<drive_id>} <pathname>
copy {<drive_id>} <pathname> {<drive_id>} <pathname>

37-1 show storage_media_info

Description

This command is used to display the information of the storage media available on the system. The information for a media includes the drive number and the media identification.

Format

show storage_media_info

Parameters

None.

Restrictions

None.

Example

To display the storage media's information:

```
DGS-3000-28XMP:admin# show storage_media_info
Command: show storage_media_info

Drive  Media Type      Size  Label        FS Type
-----  ----------  --------  -----------  -------
c:/    Flash          28 MB               FFS

DGS-3000-28XMP:admin#
```

37-2 md

Description

This command is used to create a directory.

Format

md {<drive_id>} <pathname>

Parameters

<drive_id> - (Optional) Enter the drive ID.
<pathname> - Enter the path and name of the new directory. The directory will be created in the current directory if the path is not specified.

Restrictions

Only Administrators and Operators can issue this command.

Example

To make a directory:

```
DGS-3000-28XMP:admin# md c:/abc
Command: md c:/abc

Success.

DGS-3000-28XMP:admin#
```

37-3 rd

Description

This command is used to remove a directory. If there are files still existing in the directory, this command will fail and return an error message.

Format

rd {<drive_id>} <pathname>

Parameters

<drive_id> - (Optional) Enter the drive ID.
<pathname> - Enter the path and name of the directory that will be removed.

Restrictions

Only Administrators and Operators can issue this command.

Example

To remove a directory:

```
DGS-3000-28XMP:admin# rd c:/abc
Command: rd c:/abc

Success.

DGS-3000-28XMP:admin#
```

37-4 cd

Description

This command is used to change the current directory. The current directory is changed under the current drive. If you want to change the working directory to the directory in another drive, then you need to change the current drive to the desired drive, and then change the current directory.

Format

cd {<pathname>}

Parameters

<pathname> - (Optional) Enter the path and name of the directory that will be accessed.
If no parameter is specified, the current drive and current directory will be displayed.

Restrictions

None.

Example

To change to other directory or display current directory path:

```
DGS-3000-28XMP:admin# cd
Command: cd

Current work directory: "/c:".

DGS-3000-28XMP:admin#
```

37-5 dir

Description

This command is used to list all the files located in a directory of a drive.

If pathname is not specified, then all of the files in the specified drive will be displayed. If none of the parameters are specified, the files in the current drive will be displayed.

Format

dir {<drive_id>} {<pathname>}

Parameters

<drive_id> - (Optional) Enter the drive ID.
<pathname> - (Optional) Enter the path and name of the directory and/or file that will be used in the display. The contents of the current directory will be displayed if the path is not specified.

Restrictions

None.

Example

List the files:

```
DGS-3000-28XMP:admin# dir
Command: dir

Directory of /c:

Idx Info    Attr Size     Update Time         Name
--- ------- ---- -------- ------------------- ----------------
  1 RUN(*)  -rw- 5491536  2000/01/01 00:41:03 DES3200_RUNTIME_V4.00.014.had
  2 CFG(*)  -rw- 31142    2000/01/01 02:19:40 config.cfg
  3         d---          2000/01/01 00:00:16 system

29618 KB total (24127 KB free)
(*) -with boot up info          (b) -with backup info

DGS-3000-28XMP:admin#
```

37-6 rename

Description

This command is used to rename a file in the file system. The pathname specifies the file (in path form) to be renamed and the filename specifies the new filename. If the pathname is not a full path, then it refers to a path under the current directory for the drive. The renamed file will stay in the same directory.

Format

rename {<drive_id>} <pathname> <filename>

Parameters

<drive_id> - (Optional) Enter the drive ID.
<pathname> - Enter the path and name of the file that will be renamed. The file will be renamed in the current directory if the path is not specified.
<filename> - Enter the new name of the file.

Restrictions

Only Administrators and Operators can issue this command.

Example

To rename a file:

```
DGS-3000-28XMP:admin# rename run.had run1.had
Command: rename run.had run1.had

Success.

DGS-3000-28XMP:admin#
```

37-7 del

Description

This command is used to delete a file, either physically or softly. It is also used to delete a directory and its contents. If two files with the same name under the same directory are softly deleted sequentially, only the last one will exist. Deleting, copying, renaming, or moving the already softly deleted file is not possible.

System will prompt if the target file is a firmware or boot up configuration file.

Format

del {<drive_id>} <pathname> {recursive}

Parameters

<drive_id> - (Optional) Enter the drive ID.
<pathname>- Enter the path and name of the file that will be removed. The file will be removed from the current directory if the path is not specified.
recursive - (Optional) Specifies to delete a directory and its contents even if the directory is not empty.

Restrictions

Only Administrators and Operators can issue this command.

Example

Delete a directory with parameter “recursive”:

```
DGS-3000-28XMP:admin# dir
Command: dir

Directory of / c:

Idx Info    Attr Size     Update Time         Name
--- ------- ---- -------- ------------------- ----------------
  1         drw- 0        2000/04/02 06:02:04 12
  2 CFG(*)  -rw- 29661    2000/04/01 05:54:38 config.cfg
  3 RUN(*)  -rw- 4879040  2000/03/26 03:15:11 B019.had
  4         d--- 0        2000/04/01 05:17:36 system

29618 KB total (24727 KB free)
(*) -with boot up info          (b) -with backup info

DGS-3000-28XMP:admin# del 12 recursive
Command: del 12 recursive

Success.

DGS-3000-28XMP:admin# dir
Command: dir

Directory of / c:

Idx Info    Attr Size     Update Time         Name
--- ------- ---- -------- ------------------- ----------------
  1 CFG(*)  -rw- 29661    2000/04/01 05:54:38 config.cfg
  2 RUN(*)  -rw- 4879040  2000/03/26 03:15:11 B019.had
  3         d--- 0        2000/04/01 05:17:36 system

29618 KB total (24727 KB free)
(*) -with boot up info          (b) -with backup info

DGS-3000-28XMP:admin#
```

37-8 erase

Description

This command is used to delete a file stored in the file system.

System will prompt if the target file is a firmware or boot up configuration file.

Format

erase {<drive_id>} <pathname>

Parameters

<drive_id> - (Optional) Enter the drive ID.
<pathname> - Enter the path and name of the file that will be removed. The file will be removed from the current directory if the path is not specified.

Restrictions

Only Administrators and Operators can issue this command.

Example

To erase a file:

```
DGS-3000-28XMP:admin# dir
Command: dir

Directory of /c:

Idx Info    Attr Size     Update Time         Name
--- ------- ---- -------- ------------------- ----------------
  1 CFG(b)  -rw- 29661    2000/04/02 06:03:19 config2.cfg
  2 CFG(*)  -rw- 29661    2000/04/01 05:54:38 config.cfg
  3 RUN(*)  -rw- 4879040  2000/03/26 03:15:11 B019.had
  4         d--- 0        2000/04/01 05:17:36 system

29618 KB total (24697 KB free)
(*) -with boot up info          (b) -with backup info

DGS-3000-28XMP:admin# erase config2.cfg
Command: erase config2.cfg

Success.

DGS-3000-28XMP:admin# dir
Command: dir

Directory of /c:

Idx Info    Attr Size     Update Time         Name
--- ------- ---- -------- ------------------- ----------------
  1 CFG(*)  -rw- 29661    2000/04/01 05:54:38 config.cfg
  2 RUN(*)  -rw- 4879040  2000/03/26 03:15:11 B019.had
  3         d--- 0        2000/04/01 05:17:36 system

29618 KB total (24727 KB free)
(*) -with boot up info          (b) -with backup info

DGS-3000-28XMP:admin#
```

37-9 move

Description

This command is used to move a file around the file system. When a file is moved, it can be renamed at the same time.

Format

move {<drive_id>} <pathname> {<drive_id>} <pathname>

Parameters

<drive_id> - (Optional) Enter the drive ID of the source file.
<pathname> - Enter the path and name of the file that will be moved. The file will be moved from the current directory if the path is not specified.
<drive_id> - (Optional) Enter the drive ID of the destination file.
<pathname> - Enter the path and name of the destination file. The file will be moved to the current directory if the path is not specified.

Restrictions

Only Administrators and Operators can issue this command.

Example

To move a file from one location to another location:

```
DGS-3000-28XMP:admin# move c:/log.txt c:/log1.txt
Command: move c:/log.txt c:/log1.txt

Success.

DGS-3000-28XMP:admin#
```

37-10 copy

Description

This command is used to copy a file to another location in the file system.

Format

copy {<drive_id>} <pathname> {<drive_id>} <pathname>

Parameters

<drive_id> - (Optional) Enter the drive ID of the source file.
<pathname> - Enter the path and name of the file that will be copied. The file will be copied from the current directory if the path is not specified.
<drive_id> - (Optional) Enter the drive ID of the destination file.
<pathname> - Enter the path and name of the destination file. The file will be copied to the current directory if the path is not specified.

Restrictions

Only Administrators and Operators can issue this command.

Example

To copy a file:

```
DGS-3000-28XMP:admin# copy c:/log.txt c:/log1.txt
Command: copy c:/log.txt c:/log1.txt

Success.

DGS-3000-28XMP:admin#
```

Chapter 38 Flex Link Command List

create flex_link group_id <value> primary_port <port> backup_port <port>
delete flex_link group_id <value>
show flex_link {group_id <value>}

38-1 create flex_link group_id

Description

This command is used to create a Flex Link group, and define a port or the master port in a link aggregation group as the primary or backup port in the Flex Link group.

NOTE: Flex Links does not interact with STP or LBD.

Format

create flex_link group_id <value> primary_port <port> backup_port <port>

Parameters

<value> - Enter the group ID of the Flex Link. The value is from 1 to 4.
primary_port - Specifies a port or the master port in a link aggregation group to act as the primary port in the Flex Link group. **<port> -** Enter a port to be the primary port in the Flex Link group.
backup_port - Specifies a port or the master port in a link aggregation group to act as the primary port in the Flex Link group. **<port> -** Enter a port to be the backup port in the Flex Link group.

Restrictions

Only Administrators, Operators and Power users can issue this command.

Examples

To create a Flex Link group:

```
DGS-3000-28XMP:admin#create flex_link group_id 1 primary_port 1 backup_port 2
Command: create flex_link group_id 1 primary_port 1 backup_port 2

Success.

DGS-3000-28XMP:admin#
```

38-2 delete flex_link group_id

Description

This command is used to delete a Flex Link group. When the link aggregation group is removed, the master port of that link aggregation group will still remain the primary or backup port of the Flex Link group.

Format

delete flex_link group_id <value>

Parameters

<value> - Enter the group ID of the Flex Link. The value is from 1 to 4.

Restrictions

Only Administrators, Operators and Power users can issue this command.

Examples

To remove a flext link group:

```
DGS-3000-28XMP:admin#delete flex_link group_id 1
Command: delete flex_link group_id 1

Success.

DGS-3000-28XMP:admin#
```

38-3 show flex_link

Description

This command is used to display Flex Link configuration.

Format

show flex_link {group_id <value>}

Parameters

group_id - (Optional) Specifies the group ID of the Flex Link.
<value> - Enter the group ID of the Flex Link. The value is from 1 to 4.

Restrictions

None.

Examples

To display the Flex Link configuration:

```
DGS-3000-28XMP:admin#show flex_link
Command: show flex_link

Group Primary Port            Backup Port             Status(Primary/Backup)
----- ----------------------- ----------------------- --------------------------
1     1                       2                       Inactive/Inactive

Total Entries:1


DGS-3000-28XMP:admin#
```

Chapter 39 Gratuitous ARP Command List

config gratuitous_arp send ipif_status_up [enable | disable]
config gratuitous_arp send dup_ip_detected [enable | disable]
config gratuitous_arp learning [enable | disable]
config gratuitous_arp send periodically ipif <ipif_name 12> interval <value 0-65535>
enable gratuitous_arp {ipif <ipif_name 12>} {trap | log}(1)
disable gratuitous_arp {ipif <ipif_name 12>} {trap | log}(1)
show gratuitous_arp {ipif <ipif_name 12>}

39-1 config gratuitous_arp send ipif_status_up

Description

This command is used to enable/disable the sending of gratuitous ARP request packets when the IP interface status changes to up. This is used to automatically announce the interface's IP address to other nodes. By default, this is enabled, and only one gratuitous ARP packet will be broadcasted.

Format

config gratuitous_arp send ipif_status_up [enable | disable]

Parameters

enable - Specifies to enable the sending of gratuitous ARP packets when the IP interface status changes to up.
disable - Specifies to disable the sending of gratuitous ARP packets when the IP interface status changes to up.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable send gratuitous ARP request in normal situation:

```
DGS-3000-28XMP:admin# config gratuitous_arp send ipif_status_up enable
Command: config gratuitous_arp send ipif_status_up enable

Success.

DGS-3000-28XMP:admin#
```

39-2 config gratuitous_arp send dup_ip_detected

Description

This command is used to enable/disable the sending of gratuitous ARP request packets when a duplicate IP is detected. For this command, the duplicate IP detected means that the system received an ARP request packet that is sent by an IP address that matches the system's own IP address. In this case, the system knows that there is an

entity that uses an IP address that is in conflict with the system. In order to reclaim the correct host of this IP address, the system can send out the gratuitous ARP request packet for this duplicate IP address.

Format

config gratuitous_arp send dup_ip_detected [enable | disable]

Parameters

enable - Specifies to enable sending of gratuitous ARP when a duplicate IP is detected. This is the default option.
disable - Specifies to disable sending of gratuitous ARP when a duplicate IP is detected.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable send gratuitous ARP request when a duplicate IP is detected:

```
DGS-3000-28XMP:admin# config gratuitous_arp send dup_ip_detected enable
Command: config gratuitous_arp send dup_ip_detected enable

Success.

DGS-3000-28XMP:admin#
```

39-3 config gratuitous_arp learning

Description

This command is used to configure gratuitous ARP learning. Normally, the system will only learn the ARP reply packet or a normal ARP request packet that asks for the MAC address that corresponds to the system's IP address. This command is used to enable/disable the learning of an ARP entry in the ARP cache based on the received gratuitous ARP packets. The gratuitous ARP packet is sent by a source IP address that is identical to the IP that the packet is queried for. With gratuitous ARP learning, the system will not learn new entries but instead updates the ARP table based on received gratuitous ARP packets.

Format

config gratuitous_arp learning [enable | disable]

Parameters

enable - Specifies to enable the learning of ARP entries based on received gratuitous ARP packets. This is the default value.
disable - Specifies to disable the learning of ARP entries based on received gratuitous ARP packets.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To show the global gratuitous ARP state:

```
DGS-3000-28XMP:admin# config gratuitous_arp learning enable
Command: config gratuitous_arp learning enable

Success.

DGS-3000-28XMP:admin#
```

39-4 config gratuitous_arp send periodically

Description

This command is used to configure the interval for sending gratuitous ARP request packets.

Format

config gratuitous_arp send periodically ipif <ipif_name 12> interval <value 0-65535>

Parameters

ipif - Specifies the name of the Layer 3 IP interface.
<ipif_name 12> - Enter the IP interface name here. This name can be up to 12 characters long.

interval - Specifies the gratuitous ARP interval time in seconds. 0 means not to send gratuitous ARP packets periodically. The default value is 0.
<value 0-65535> - Enter the gratuitous ARP interval time here. This value must be between 0 and 65535 seconds.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure gratuitous ARP interval to 5 for IPIF System:

```
DGS-3000-28XMP:admin# config gratuitous_arp send periodically ipif System interval 5
Command: config gratuitous_arp send periodically ipif System interval 5

Success.

DGS-3000-28XMP:admin#
```

39-5 enable gratuitous_arp

Description

This command is used to enable the gratuitous ARP trap and log state. The switch can trap and log the IP conflict event to inform the administrator. By default, trap is disabled and event log is enabled.

Format

enable gratuitous_arp {ipif <ipif_name 12>} {trap | log}(1)

Parameters

ipif - (Optional) Specifies the name of the Layer 3 IP interface. **<ipif_name 12>** - Enter the IP interface name here. This name can be up to 12 characters long.
trap - Specifies to enable the trap function.
log - Specifies to enable the log function.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable system interface's gratuitous ARP log and trap:

```
DGS-3000-28XMP:admin# enable gratuitous_arp ipif System trap log
Command: enable gratuitous_arp ipif System trap log

Success.

DGS-3000-28XMP:admin#
```

39-6 disable gratuitous_arp

Description

This command is used to disable the gratuitous ARP trap and log state. The switch can trap and log the IP conflict event to inform the administrator. By default, trap is disabled and event log is enabled.

Format

disable gratuitous_arp {ipif <ipif_name 12>} {trap | log}(1)

Parameters

ipif - (Optional) Specifies the name of the Layer 3 IP interface. **<ipif_name 12>** - Enter the IP interface name here. This name can be up to 12 characters long.
trap - Specifies to disable the trap function.
log - Specifies to disable the log function.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To disable system interface's gratuitous ARP log and trap:

```
DGS-3000-28XMP:admin# disable gratuitous_arp ipif System trap log
Command: disable gratuitous_arp ipif System trap log

Success.

DGS-3000-28XMP:admin#
```

39-7 show gratuitous_arp

Description

This command is used to display the gratuitous ARP configuration.

Format

show gratuitous_arp {ipif <ipif_name 12>}

Parameters

ipif - (Optional) Specifies the name of the Layer 3 IP interface.
<ipif_name> - Enter the IP interface name here.

Restrictions

None.

Example

To display gratuitous ARP log and trap state:

```
DGS-3000-28XMP:admin# show gratuitous_arp
Command: show gratuitous_arp

Send on IPIF Status Up        : Enabled
Send on Duplicate IP Detected : Enabled
Gratuitous ARP Learning       : Enabled

IP Interface Name : System
        Gratuitous ARP Trap                    : Enabled
        Gratuitous ARP Log                     : Enabled
        Gratuitous ARP Periodical Send Interval : 5

Total Entries: 1


DGS-3000-28XMP:admin#
```

Chapter 40 IGMP Snooping Command List

The Internet Group Management Protocol (IGMP) is a L3 protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. IGMP snooping is the process of listening to IGMP network traffic. IGMP snooping, as implied by the name, is a feature that allows a layer 2 switch to "listen in" on the IGMP conversation between hosts and routers by processing the layer 3 IGMP packets sent in a multicast network.

When IGMP snooping is enabled in a switch it analyzes all IGMP packets between hosts connected to the Switch and multicast routers in the network. When a switch hears an IGMP report from a host for a given multicast group, the Switch adds the host's port number to the multicast list for that group. And, when the Switch hears an IGMP Leave, it removes the host's port from the table entry.

config igmp_snooping [vlan_name <vlan_name 32> | vlanid <vlanid_list> | all] {state [enable | disable] | fast_leave [enable | disable] | report_suppression [enable | disable] | proxy_reporting {state [enable | disable] | source_ip <ipaddr>}(1)}(1)
config igmp_snooping rate_limit [ports <portlist> | vlanid <vlanid_list>] [<value 1-1000> | no_limit]
config igmp_snooping querier [vlan_name <vlan_name 32> | vlanid <vlanid_list> | all] {query_interval <sec 1-65535> | max_response_time <sec 1-25> | robustness_variable <value 1-7> | last_member_query_interval <sec 1-25> | state [enable | disable] | version <value 1-3>}(1)
config igmp access_authentication ports [all | <portlist>] state [enable | disable]
config router_ports [<vlan_name 32> | vlanid <vlanid_list>] [add | delete] <portlist>
config router_ports_forbidden [<vlan_name 32> | vlanid <vlanid_list>] [add | delete] <portlist>
enable igmp_snooping
disable igmp_snooping
create igmp_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipaddr>
delete igmp_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipaddr>
config igmp_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipaddr> [add | delete] <portlist>
show igmp_snooping static_group {[vlan <vlan_name 32> | vlanid <vlanid_list>] <ipaddr>}
config igmp_snooping data_driven_learning [all | vlan_name <vlan_name> | vlanid <vlanid_list>] {state [enable | disable] | aged_out [enable | disable] | expiry_time <sec 1-65535>}
config igmp_snooping data_driven_learning max_learned_entry <value 1-1024>
clear igmp_snooping data_driven_group [all | [vlan_name <vlan_name> | vlanid <vlanid_list>] [<ipaddr> | all]]
show igmp_snooping {[vlan <vlan_name 32> | vlanid <vlanid_list>]}
show igmp_snooping rate_limit [ports <portlist> | vlanid <vlanid_list>]
show igmp_snooping group {[vlan <vlan_name 32> | vlanid <vlanid_list> | ports <portlist>] {<ipaddr>}} {data_driven}
show igmp_snooping forwarding {[vlan <vlan_name 32> | vlanid <vlanid_list>]}
show router_ports [vlan <vlan_name 32> | vlanid <vlanid_list> | all] {[static | dynamic | forbidden]}
show igmp_snooping statistic counter [vlan <vlan_name> | vlanid <vlanid_list> | ports <portlist>]
show igmp access_authentication ports [all | <portlist>]
show igmp_snooping host {[vlan <vlan_name 32>| vlanid <vlanid_list> | ports <portlist> | group <ipaddr>]}
clear igmp_snooping statistics counter

40-1 config igmp_snooping

Description

This command is used to configure IGMP snooping on the Switch.

Format

config igmp_snooping [vlan_name <vlan_name 32> | vlanid <vlanid_list> | all] {state [enable | disable] | fast_leave [enable | disable] | report_suppression [enable | disable] | proxy_reporting {state [enable | disable] | source_ip <ipaddr>}(1)}(1)

Parameters

vlan_name - Specifies the name of the VLAN for which IGMP snooping is to be configured.
- **<vlan_name 32>** - Enter the VLAN name here. The VLAN name can be up to 32 characters long.

vlanid - Specifies the VLAN ID for which IGMP snooping is to be configured.
- **<vlanid_list>** - Enter the VLAN ID here.

all - Specifies to use all configured VLANs.

state - Specifies to enable or disable IGMP snooping for the chosen VLAN.
- **enable** - Specifies to enable IGMP snooping for the chosen VLAN.
- **disable** - Specifies to disable IGMP snooping for the chosen VLAN.

fast_leave - Specifies to enable or disable the IGMP snooping fast leave function.
- **enable** - Specifies to enable the IGMP snooping fast leave function. If enabled, the membership is immediately removed when the system receives the IGMP leave message.
- **disable** - Specifies to disable the IGMP snooping fast leave function.

report_suppression - Specifies IGMP report suppression. When enabled, multiple IGMP reports or leave for a specific (S, G) will be integrated into one report only before sending to the router port.
- **enable** - Specifies to enable the IGMP report suppression.
- **disable** - Specifies to disable the IGMP report suppression.

proxy_reporting - Specifies IGMP proxy reporting. If enabled, multiple IGMP reports or leave for a specific (S, G) will be integrated into one report only before sending to the router port.
- **state** - Specifies to enable or disable the proxy reporting.
  - **enable** - Specifies to enable the proxy reporting.
  - **disable** - Specifies to disable the proxy reporting.
- **source_ip** - Specifies the source IP of proxy reporting integrated report. Default value is zero IP.
  - **<ipaddr>** - Enter the IP address.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure IGMP snooping:

```
DGS-3000-28XMP:admin# config igmp_snooping vlan_name default state enable
Command: config igmp_snooping vlan_name default state enable

Success.

DGS-3000-28XMP:admin#
```

40-2 config igmp_snooping rate_limit

Description

This command is used to configure the rate of IGMP control packets that are allowed per port or per VLAN.

Format

config igmp_snooping rate_limit [ports <portlist> | vlanid <vlanid_list>] [<value 1-1000> | no_limit]

Parameters

ports - Specifies a range of ports to be configured. **<portlist>** - Enter the range of ports to be configured here.
vlanid - Specifies a range of VLANs to be configured. **<vlanid_list>** - Enter the VLAN ID list here.
<value 1-1000> - Enter the rate of the IGMP control packets that the Switch can process on a specific port/VLAN. The rate is specified in packets per second. The packets that exceed the limit will be dropped.
no_limit - Specifies the rate of the IGMP control packets to be unlimited that the Switch can process on a specific port/VLAN. The rate is specified in packets per second. The packets that exceed the limit will be dropped. The default setting is no_limit.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the IGMP snooping per port rate_limit:

```
DGS-3000-28XMP:admin# config igmp_snooping rate_limit ports 1 100
Command: config igmp_snooping rate_limit ports 1 100

Success.

DGS-3000-28XMP:admin#
```

40-3 config igmp_snooping querier

Description

This command is used to configure the time in seconds between general query transmissions, the maximum time in seconds to wait for reports from members, and the permitted packet loss that guarantees IGMP snooping.

Format

config igmp_snooping querier [vlan_name <vlan_name 32> | vlanid <vlanid_list> | all] {query_interval <sec 1-65535> | max_response_time <sec 1-25> | robustness_variable <value 1-7> | last_member_query_interval <sec 1-25> | state [enable | disable] | version <value 1-3>}(1)

Parameters

vlan_name - Specifies the name of the VLAN for which IGMP snooping querier is to be configured.

<vlan_name 32> - Enter the VLAN name here. The VLAN name can be up to 32 characters long.

vlanid - Specifies the VLAN ID for which IGMP snooping querier is to be configured.

<vlanid_list> - Enter the VLAN ID list here.

all - Specifies all VLANs for which IGMP snooping querier is to be configured.

query_interval - Specifies the amount of time in seconds between general query transmissions. The default setting is 125 seconds.

<sec 1-65535> - Enter the query interval value here. This value must be between 1 and 65535 seconds.

max_reponse_time - Specifies the maximum time in seconds to wait for reports from members. The default setting is 10 seconds.

<sec 1-25> - Enter the maximum response time value here. This value must be between 1 and 25 seconds.

robustness_variable - Specifies to provide fine-tuning to allow for expected packet loss on a subnet. The value of the robustness variable is used in calculating the following IGMP message intervals:

<value 1-7> - Enter the robustness variable value here. This value must be between 1 and 7. By default, the robustness variable is set to 2. You might want to increase this value if you expect a subnet to be more loose.

- Group member interval—Amount of time that must pass before a multicast router decides there are no more members of a group on a network. This interval is calculated as follows: (robustness variable x query interval) + (1 x query response interval).
- Other querier present interval—Amount of time that must pass before a multicast router decides that there is no longer another multicast router that is the querier. This interval is calculated as follows: (robustness variable x query interval) + (0.5 x query response interval).
- Last member query count—Number of group-specific queries sent before the router assumes there are no local members of a group. The default number is the value of the robustness variable.

last_member_query_interval - Specifies the maximum amount of time between group-specific query messages, including those sent in response to leave-group messages. You might lower this interval to reduce the amount of time it takes a router to detect the loss of the last member of a group. On receiving a leave message, the router will assume there are no local members on the interface if there are no reports received after the response time (which is last member query interval * robustness variable)

<sec 1-25> - Enter the last member query interval value here. This value must be between 1 and 25 seconds.

state - If the state is enabled, it allows the Switch to be selected as an IGMP querier (sends IGMP query packets). It the state is disabled, then the Switch cannot play the role as a querier. Note that if the Layer 3 router connected to the Switch provides only the IGMP proxy function but does not provide the multicast routing function, then this state must be configured as disabled. Otherwise, if the Layer 3 router is not selected as the querier, it will not send the IGMP query packet. Since it will not send the multicast-routing protocol packets, the port will be timed out as a router port.

enable - Specifies to enable this state.

disable - Specifies to disable this state.

version - Specifies the version of IGMP packets that will be sent by this device. If an IGMP packet received by the interface has a version higher than the specified version, this packet will be dropped.

<value 1-3> - Enter the version number here. This value must be between 1 and 3.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the IGMP snooping querier:

```
DGS-3000-28XMP:admin# config igmp_snooping querier vlan_name default query_interval 125 state
enable
Command: config igmp_snooping querier vlan_name default query_interval 125 state enable

Success.

DGS-3000-28XMP:admin#
```

40-4 config igmp access_authentication ports

Description

This command is used to enable or disable the IGMP Access Control function for the specified ports. If the IGMP Access Control function is enabled and the Switch receives an IGMP JOIN message, the Switch will send the access request to the RADIUS server for authentication.

Format

config igmp access_authentication ports [all | <portlist>] state [enable | disable]

Parameters

all - Specifies all ports to be configured.
<portlist> - Specifies a range of ports to be configured.
state - Specifies the state of the RADIUS authentication function on the specified ports. **enable** - Specifies to enable the RADIUS authentication function on the specified ports. **disable** - Specifies to disable the RADIUS authentication function on the specified ports.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable IGMP Access Control for all ports:

```
DGS-3000-28XMP:admin#config igmp access_authentication ports all state enable

Command: config igmp access_authentication ports all state enable

Success.

DGS-3000-28XMP:admin#
```

40-5 config router_ports

Description

This command is used to designate a range of ports as being connected to multicast-enabled routers. This will ensure that all packets with such a router as its destination will reach the multicast-enabled router, regardless of protocol, etc.

Format

config router_ports [<vlan_name 32> | vlanid <vlanid_list>] [add | delete] <portlist>

Parameters

<vlan_name 32> - Specifies the name of the VLAN on which the router port resides.
vlanid - Specifies the ID of the VLAN on which the router port resides. **<vlanid_list>** - Enter the VLAN ID here.
add - Specifies to add the router ports.
delete - Specifies to delete the router ports.
<portlist> - Specifies a range of ports to be configured.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To set up static router ports:

```
DGS-3000-28XMP:admin#config router_ports default add 1-10
Command: config router_ports default add 1-10

Success.

DGS-3000-28XMP:admin#
```

40-6 config router_ports_forbidden

Description

This command is used to designate a range of ports as being not connected to multicast-enabled routers. This ensures that the forbidden router port will not propagate routing packets out.

Format

config router_ports_forbidden [<vlan_name 32> | vlanid <vlanid_list>] [add | delete] <portlist>

Parameters

<vlan_name 32> - Specifies the name of the VLAN on which the router port resides.
vlanid - Specifies the ID of the VLAN on which the router port resides. **<vlanid_list>** - Enter the VLAN ID list here.

add - Specifies to add the router ports.
delete - Specifies to delete the router ports.
<portlist> - Specifies a range of ports to be configured.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To set up port range 1-10 as forbidden router ports of default VLAN:

```
DGS-3000-28XMP:admin#config router_ports_forbidden default add 11-12
Command: config router_ports_forbidden default add 11-12

Success.

DGS-3000-28XMP:admin#
```

40-7 enable igmp_snooping

Description

This command is used to enable IGMP snooping on the Switch.

Format

enable igmp_snooping

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable IGMP snooping on the Switch:

```
DGS-3000-28XMP:admin# enable igmp_snooping
Command: enable igmp_snooping

Success.

DGS-3000-28XMP:admin#
```

40-8 disable igmp_snooping

Description

This command is used to disable IGMP snooping on the Switch. Disabling IGMP snooping allows all IGMP and IP multicast traffic to flood within a given IP interface.

Format

disable igmp_snooping

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To disable IGMP snooping on the Switch:

```
DGS-3000-28XMP:admin# disable igmp_snooping
Command: disable igmp_snooping

Success.

DGS-3000-28XMP:admin#
```

40-9 create igmp_snooping static_group

Description

This command is used to create an IGMP snooping static group. Member ports can be added to the static group. The static member and the dynamic member ports form the member ports of a group.

The static group will only take effect when IGMP snooping is enabled on the VLAN. For those static member ports, the device needs to emulate the IGMP protocol operation to the querier, and forward the traffic destined to the multicast group to the member ports.

For a layer 3 device, the device is also responsible for routing the packet destined for this specific group to static member ports.

The static member port will only affect V2 IGMP operation.

The Reserved IP multicast address 224.0.0.X must be excluded from the configured group.

The VLAN must be created first before a static group can be created.

Format

create igmp_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipaddr>

Parameters

vlan - Specifies the name of the VLAN on which the router port resides. **<vlan_name 32>** - Enter the VLAN name here. The VLAN name can be up to 32 characters long.
vlanid - Specifies the ID of the VLAN on which the router port resides. **<vlanid_list>** - Enter the VLAN ID here.
<ipaddr> - Enter the multicast group IP address.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To create an IGMP snooping static group for VLAN 1, group 239.1.1.1:

```
DGS-3000-28XMP:admin#create igmp_snooping static_group vlan default 239.1.1.1

Command: create igmp_snooping static_group vlan default 239.1.1.1

Success.

DGS-3000-28XMP:admin#
```

40-10 delete igmp_snooping static_group

Description

This command is used to delete an IGMP snooping multicast static group. The deletion of an IGMP snooping static group will not affect the IGMP snooping dynamic member ports of a group.

Format

delete igmp_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipaddr>

Parameters

vlan - Specifies the name of the VLAN on which the router port resides. **<vlan_name 32>** - Enter the VLAN name here. The VLAN name can be up to 32 characters long.
vlanid - Specifies the ID of the VLAN on which the router port resides. **<vlanid_list>** - Enter the VLAN ID list here.
<ipaddr> - Enter the multicast group IP address.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete an IGMP snooping static group for VLAN 1, group 239.1.1.1:

```
DGS-3000-28XMP:admin#delete igmp_snooping static_group vlan default 239.1.1.1
Command: delete igmp_snooping static_group vlan default 239.1.1.1

Success.

DGS-3000-28XMP:admin#
```

40-11 config igmp_snooping static_group

Description

This command is used to configure an IGMP snooping static group. When a port is configured as a static member port, the IGMP protocol will not operate on this port. For example, suppose that a port is a dynamic member port learned by IGMP. If this port is configured as a static member later, then the IGMP protocol will stop operating on this port. The IGMP protocol will resume once this port is removed from static member ports.

The static member port will only affect V2 IGMP operation.

Format

config igmp_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipaddr> [add | delete] <portlist>

Parameters

vlan - Specifies the name of the VLAN on which the static group resides. **<vlan_name 32>** - Enter the VLAN name here. The VLAN name can be up to 32 characters long.
vlanid - Specifies the ID of the VLAN on which the static group resides. **<vlanid_list>** - Enter the VLAN ID here.
<ipaddr> - Enter the multicast group IP address (for Layer 3 switch).
add - Specifies to add member ports.
delete - Specifies to delete member ports.
<portlist> - Enter a range of ports to be configured.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To remove port range 9-10 from IGMP snooping static member ports for group 239.1.1.1 on default VLAN:

```
DGS-3000-28XMP:admin#config igmp_snooping static_group vlan default 239.1.1.1 delete 9-10
Command: config igmp_snooping static_group vlan default 239.1.1.1 delete 9-10

Success.

DGS-3000-28XMP:admin#
```

40-12 show igmp_snooping static_group

Description

This command is used to display the IGMP snooping multicast group static members.

Format

show igmp_snooping static_group {[vlan <vlan_name 32> | vlanid <vlanid_list>] <ipaddr>}

Parameters

vlan - (Optional) Specifies the name of the VLAN on which the static group resides. **<vlan_name 32>** - Enter the VLAN name here. The VLAN name can be up to 32 characters long.
vlanid - (Optional) Specifies the ID of the VLAN on which the static group resides. **<vlanid_list>** - Enter the VLAN ID here.
<ipaddr> - (Optional) Enter the multicast group IP address.

Restrictions

None.

Example

To display all the IGMP snooping static groups:

```
DGS-3000-28XMP:admin#show igmp_snooping static_group
Command: show igmp_snooping static_group

VLAN ID/Name                           IP Address       Static Member Ports
-------------------------------------  ---------------  ----------------------
1   /default                           239.1.1.1         9-10

 Total Entries : 1


DGS-3000-28XMP:admin#
```

40-13 config igmp_snooping data_driven_learning

Description

This command is used to enable or disable the data driven learning of an IGMP snooping group.

When data-driven learning is enabled for the VLAN, and the Switch receives 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: 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.

Format

config igmp_snooping data_driven_learning [all | vlan_name <vlan_name> | vlanid <vlanid_list>] {state [enable | disable] | aged_out [enable | disable] | expiry_time <sec 1-65535>}(1)

Parameters

all - Specifies all VLANs to be configured.
vlan_name - Specifies the VLAN name to be configured. **<vlan_name>** - Enter the VLAN name here.
vlanid - Specifies the VLAN ID to be configured. **<vlanid_list>** - Enter the VLAN ID here.
state - Specifies to enable or disable the data driven learning of an IGMP snooping group. **enable** - Specifies to enable the data driven learning option. By default, the state is enabled. **disable** - Specifies to disable the data driven learning option.
aged_out - Specifies to enable or disable the aging out of the entry. **enable** - Specifies to enable the aging out of the entry. **disable** - Specifies to disable the aging out of the entry. By default, the state is disabled state.
expiry_time - Specifies the data driven group lifetime in seconds. This parameter is valid only when aged_out is enabled. **<sec 1-65535>** - Enter the expiry time here. This value must be between 1 and 65535 seconds.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

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

```
DGS-3000-28XMP:admin# config igmp_snooping data_driven_learning vlan_name default state
enable
Command: config igmp_snooping data_driven_learning vlan_name default state enable

Success.

DGS-3000-28XMP:admin#
```

40-14 config igmp_snooping data_driven_learning max_learned_entry

Description

This command is used to configure the maximum number of groups that can be learned by data driven learning.

When the table is full, the system will stop the learning of the new data-driven groups. Traffic for the new groups will be dropped.

Format

config igmp_snooping data_driven_learning max_learned_entry <value 1-1024>

Parameters

<value 1-1024> - Enter the maximum learning entry value here. This value must be between 1 and 1024. The default setting is 128.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

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

```
DGS-3000-28XMP:admin# config igmp_snooping data_driven_learning max_learned_entry 50
Command: config igmp_snooping data_driven_learning max_learned_entry 50

Success.

DGS-3000-28XMP:admin#
```

40-15 clear igmp_snooping data_driven_group

Description

This command is used to delete the IGMP snooping group(s) learned by data driven learning.

Format

clear igmp_snooping data_driven_group [all | [vlan_name <vlan_name> | vlanid <vlanid_list>] [<ipaddr> | all]]

Parameters

all - Specifies all VLANs for which IGMP snooping groups will be deleted.

vlan_name - Specifies the VLAN name.
<vlan_name> - Enter the VLAN name here.

vlanid - Specifies the VLAN ID.
<vlanid_list> - Enter the VLAN ID or the list of VLAN IDs here.

<ipaddr> - Enter the group's IP address learned by data driven learning.

all - Specifies to delete all IGMP snooping groups of the specified VLANs.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete all the groups learned by data-driven:

```
DGS-3000-28XMP:admin# clear igmp_snooping data_driven_group all
Command: clear igmp_snooping data_driven_group all

Success.

DGS-3000-28XMP:admin#
```

40-16 show igmp_snooping

Description

This command is used to display the current IGMP snooping configuration on the Switch.

Format

show igmp_snooping {[vlan <vlan_name 32> | vlanid <vlanid_list>]}

Parameters

vlan - (Optional) Specifies the name of the VLAN for which you want to view the IGMP snooping configuration. **<vlan_name 32>** - Enter the VLAN name here. The VLAN name can be up to 32 characters long.
vlanid - (Optional) Specifies the ID of the VLAN for which you want to view the IGMP snooping configuration. **<vlanid_list>** - Enter the VLAN ID list here.
If no parameter is specified, the system will display all current IGMP snooping configurations.

Restrictions

None.

Example

To show IGMP snooping:

```
DGS-3000-28XMP:admin#show igmp_snooping
Command: show igmp_snooping

 IGMP Snooping Global State              : Enabled
 Data Driven Learning Max Entries        : 128

 VLAN Name                      : default
 Query Interval                 : 125
 Max Response Time              : 10
 Robustness Value               : 2
 Last Member Query Interval     : 1
 Querier State                  : Disabled
 Querier Role                   : Non-Querier
 Querier IP                     : 0.0.0.0
 Querier Expiry Time            : 0 secs
 State                          : Disabled
 Fast Leave                     : Disabled
 Rate Limit                     : No Limitation
 Report Suppression             : Enabled
 Proxy Reporting                : Disabled
 Proxy Reporting Source IP      : 0.0.0.0
 Version                        : 3
 Data Driven Learning State     : Enabled
 Data Driven Learning Aged Out : Disabled
 Data Driven Group Expiry Time : 260

Total Entries: 1


DGS-3000-28XMP:admin#
```

40-17 show igmp_snooping rate_limit

Description

This command is used to display the IGMP snooping rate limit setting.

Format

show igmp_snooping rate_limit [ports <portlist> | vlanid <vlanid_list>]

Parameters

ports - Specifies the port range.	
	<portlist> - Enter the range of ports here.
vlanid - Specifies the VLAN range.	
	<vlanid_list> - Enter the VLAN ID list here.

Restrictions

None.

Example

To display the IGMP snooping rate limit for ports 1 to 15:

```
DGS-3000-28XMP:admin# show igmp_snooping rate_limit ports 1-15
Command: show igmp_snooping rate_limit ports 1-15

Port         Rate Limit
--------    -----------
 1            No Limit
 2            100
 3            No Limit
 4            No Limit
 5            No Limit

Total Entries: 5
```

40-18 show igmp_snooping group

Description

This command is used to display the current IGMP snooping group configuration on the Switch.

Format

show igmp_snooping group {[vlan <vlan_name 32> | vlanid <vlanid_list> | ports <portlist>] {<ipaddr>}} {data_driven}

Parameters

vlan - (Optional) Specifies the name of the VLAN for which you want to view IGMP snooping group information. If VLAN, ports and IP address are not specified, the system will display all current IGMP snooping group information. **<vlan_name 32>** - Enter the VLAN name here. The VLAN name can be up to 32 characters long.
vlanid - (Optional) Specifies the ID of the VLAN for which you want to view IGMP snooping group information. **<vlanid_list>** - Enter the VLAN ID list here.
ports - (Optional) Specifies a list of ports for which you want to view IGMP snooping group information. **<portlist>** - Enter the list of ports here.
<ipaddr> - (Optional) Specifies the group IP address for which you want to view IGMP snooping group information.
data_driven - (Optional) Specifies to only display data driven groups.

Restrictions

None.

Example

To show IGMP snooping groups when IGMP v3 is supported:

```
DGS-3000-28XMP:admin# show igmp_snooping group
Command: show igmp_snooping group

 Source/Group    : 20.64.85.0/226.1.1.1
 VLAN Name/VID    : v103/103
 Member Ports              : 6
 Router Ports               : 8
 UP Time                    : 7
 Expiry Time                   : 253
 Filter Mode                   : INCLUDE

 Source/Group                  : 20.64.85.1/226.1.1.1
 VLAN Name/VID                 : v103/103
 Member Ports                  : 6
 Router Ports                  : 8
 UP Time                       : 7
 Expiry Time                   : 252
 Filter Mode                   : INCLUDE

 Source/Group                  : 20.64.85.2/226.1.1.1
 VLAN Name/VID                 : v103/103
 Member Ports                  : 6
 Router Ports                  : 8
 UP Time                       : 7
 Expiry Time                   : 252
 Filter Mode                   : INCLUDE

 Total Entries: 3

DGS-3000-28XMP:admin#
```

To show IGMP snooping data driven groups:

```
DGS-3000-28XMP:admin# show igmp_snooping group data_driven
Command: show igmp_snooping group data_driven

 Source/Group      : NULL/226.1.1.1
 VLAN Name/VID      : v103/103
 Member Ports             :
 Router Ports                  :
 UP Time                       : 92
 Expiry Time                   : 168
 Filter Mode                   : EXCLUDE

 Total Entries: 1

DGS-3000-28XMP:admin#
```

To show IGMP snooping groups when only IGMP v2 is supported: The third item is a data-driven learned entry. If the member port list is empty, the multicast packets will be forwarded to the router ports. If the router port list is empty, the packets will be dropped.

```
DGS-3000-28XMP:admin# show igmp_snooping group
Command: show igmp_snooping group

 Source/Group        : NULL/226.1.1.1
 VLAN Name/VID            : v103/103
 Member Ports                 : 6
 Router Ports                 : 8
 UP Time                      : 10
 Expiry Time                  : 260
 Filter Mode                  : EXCLUDE

 Source/Group         : NULL/226.1.1.2
 VLAN Name/VID            : v103/103
 Member Ports                 : 6
 Router Ports                 : 8
 UP Time                      : 10
 Expiry Time                  : 260
 Filter Mode                  : EXCLUDE

 Source/Group        : NULL/226.1.1.3
 VLAN Name/VID            : v103/103
 Member Ports                 :
 Router Ports                 : 8
 UP Time                      : 80
 Expiry Time                  : 180
 Filter Mode                  : EXCLUDE

 Total Entries: 3

DGS-3000-28XMP:admin#
```

40-19 show igmp_snooping forwarding

Description

This command is used to display the Switch's current IGMP snooping forwarding table. It provides an easy way for users to check the list of ports that the multicast group that comes from a specific sources will be forwarded to. If packets come from the source VLAN, they will be forwarded to the forwarding VLAN. The IGMP snooping further restricts the forwarding ports.

Format

show igmp_snooping forwarding {[vlan <vlan_name 32> | vlanid <vlanid_list>]}

Parameters

vlan - (Optional) Specifies the name of the VLAN for which you want to view IGMP snooping forwarding table information. **<vlan_name 32>** - Enter the VLAN name here. The VLAN name can be up to 32 characters long.
vlanid - (Optional) Specifies the ID of the VLAN for which you want to view IGMP snooping forwarding table information. **<vlanid_list>** - Enter the VLAN ID list here.
If no parameter is specified, the system will display all current IGMP snooping forwarding table entries of the

Switch.

Restrictions

None.

Example

To show all IGMP snooping forwarding entries located on the Switch:

```
DGS-3000-28XMP:admin# show igmp_snooping forwarding
Command: show igmp_snooping forwarding

VLAN Name      : default
Source IP      : *
Multicast Group: 225.0.0.0
Port Member    : 2,7

VLAN Name      : default
Source IP      : *
Multicast Group: 225.0.0.1
Port Member    : 2,5

VLAN Name      : default
Source IP      : *
Multicast Group: 225.0.0.2
Port Member    : 2,8

Total Entries : 3

DGS-3000-28XMP:admin#
```

40-20 show router_ports

Description

This command is used to display the currently configured router ports on the Switch.

Format

show router_ports [vlan <vlan_name 32> | vlanid <vlanid_list> | all] {[static | dynamic | forbidden]}

Parameters

vlan - Specifies the name of the VLAN on which the router port resides. **<vlan_name 32>** - Enter the VLAN name here. The VLAN name can be up to 32 characters long.
vlanid - Specifies the ID of the VLAN on which the router port resides. **<vlanid_list>** - Enter the VLAN ID list here.
all - Specifies all VLANs on which the router port resides.
static - (Optional) Displays router ports that have been statically configured.
dynamic - (Optional) Displays router ports that have been dynamically configured.

forbidden - (Optional) Displays forbidden router ports that have been statically configured.
If no parameter is specified, the system will display all currently configured router ports on the Switch.

Restrictions

None.

Example

To display router ports:

```
DGS-3000-28XMP:admin# show router_ports all
Command: show router_ports all

VLAN Name               : default
Static Router Port      : 1-10
Dynamic Router Port     :
          Router IP     : 10.0.0.1, 10.0.0.2, 10.0.0.3
Forbidden router port   :

VLAN Name               : vlan2
Static router port      :
Dynamic router port     : 13
          Router IP     : 10.0.0.4, 10.0.0.5, 10.0.0.6
Forbidden router port   :

Total Entries : 2

DGS-3000-28XMP:admin#
```

40-21 show igmp_snooping statistics counter

Description

This command is used to display the statistics counter for IGMP protocol packets that are received by the Switch since IGMP snooping was enabled.

Format

show igmp_snooping statistic counter [vlan <vlan_name> | vlanid <vlanid_list> | ports <portlist>]

Parameters

vlan - Specifies a VLAN to be displayed. **<vlan_name>** - Enter the VLAN name here.
vlanid - Specifies a list of VLANs to be displayed. **<vlanid_list>** - Enter the VLAN ID list here.
ports - Specifies a list of ports to be displayed. **<portlist>** - Enter the list of ports to be displayed here.

Restrictions

None.

Example

To display the IGMP snooping statistics counter:

```
DGS-3000-28XMP:admin# show igmp_snooping statistic counter vlanid 67
Command: show igmp_snooping statistic counter vlanid 67

VLAN Name         : VLAN67
-------------------------------------------------
Group Number      : 0

Receive Statistics
    Query
      IGMP v1 Query                    : 0
      IGMP v2 Query                    : 0
      IGMP v3 Query                    : 0
      Total                            : 0
      Dropped By Rate Limitation       : 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 Rate Limitation       : 0
      Dropped By Max Group Limitation  : 0
      Dropped By Group Filter          : 0
      Dropped By Multicast VLAN        : 0

Transmit Statistics
    Query
      IGMP v1 Query                    : 0
      IGMP v2 Query                    : 44
      IGMP v3 Query                    : 0
      Total                            : 44

    Report & Leave
      IGMP v1 Report                   : 0
      IGMP v2 Report                   : 0
      IGMP v3 Report                   : 0
      IGMP v2 Leave                    : 0
      Total                            : 0

 Total Entries : 1

DGS-3000-28XMP:admin#
```

To display the IGMP snooping statistics counter for a port:

```
DGS-3000-28XMP:admin# show igmp_snooping statistic counter ports 1
Command: show igmp_snooping statistic counter ports 1

Port #            : 1
-------------------------------------------------
Group Number      : 0

Receive Statistics
    Query
      IGMP v1 Query                    : 0
      IGMP v2 Query                    : 0
      IGMP v3 Query                    : 0
      Total                            : 0
      Dropped By Rate Limitation       : 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 Rate Limitation       : 0
      Dropped By Max Group Limitation  : 0
      Dropped By Group Filter          : 0
      Dropped By Multicast VLAN        : 0

Transmit Statistics
    Query
      IGMP v1 Query                    : 0
      IGMP v2 Query                    : 0
      IGMP v3 Query                    : 0
      Total                            : 0

    Report & Leave
      IGMP v1 Report                   : 0
      IGMP v2 Report                   : 0
      IGMP v3 Report                   : 0
      IGMP v2 Leave                    : 0
      Total                            : 0

 Total Entries : 1

DGS-3000-28XMP:admin#
```

40-22 show igmp access_authentication ports

Description

This command is used to display the current IGMP Access Control configuration.

Format

show igmp access_authentication ports [all | <portlist>]

Parameters

all - Specifies all ports to be displayed.
<portlist> - Enter a range of ports to be displayed.

Restrictions

None.

Example

To display the IGMP Access Control status for ports 1-4:

```
DGS-3000-28XMP:admin# show igmp access_authentication ports 1-4
Command: show igmp access_authentication ports 1-4

Port     State
-----    ---------
1        Enabled
2        Disabled
3        Disabled
4        Disabled

DGS-3000-28XMP:admin#
```

To display the IGMP Access Control status for all ports:

```
DGS-3000-28XMP:admin# show igmp access_authentication ports all
Command: show igmp access_authentication ports all

Port     State
-----    ---------
1        Enabled
2        Disabled
3        Disabled
4        Disabled
5        Disabled
6        Disabled
7        Disabled
8        Disabled
9        Disabled
10       Disabled
11       Disabled
12       Disabled
13       Disabled
14       Disabled
15       Disabled
16       Disabled
17       Disabled
18       Disabled
19       Disabled
20       Disabled
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

40-23 show igmp_snooping host

Description

This command is used to display the IGMP hosts that joined groups on specific ports or VLANs.

Format

show igmp_snooping host {[vlan <vlan_name 32> | vlanid <vlanid_list> | ports <portlist> | group <ipaddr>]}

Parameters

vlan - (Optional) Specifies the name of the VLAN. **<vlan_name 32>** - Enter the VLAN name.
vlanid - (Optional) Specifies the ID of the VLAN. **<vlanid_list>** - Enter the list of VLANs.
ports - (Optional) Specifies ports to be displayed. **<portlist>** - Enter a range of ports to be displayed.
group - (Optional) Specifies the group to be displayed. **<ipaddr>** - Enter the IP address of the group.

Restrictions

None.

Example

To display the IGMP host IP information for the default VLAN:

```
DGS-3000-28XMP:admin#show igmp_snooping host vlan default
Command: show igmp_snooping host vlan default

VLANID  Group            Port Host
------- ---------------  ---  ---------------
 1      225.0.1.0        2    198.19.1.2
 1      225.0.1.0        2    198.19.1.3
 1      225.0.1.0        3    198.19.1.4
 1      225.0.1.2        2    198.19.1.3
 1      225.0.2.3        3    198.19.1.4
 1      225.0.3.4        3    198.19.1.5
 1      225.0.4.5        5    198.19.1.6
 1      225.0.5.6        5    198.19.1.7
 1      225.0.6.7        4    198.19.1.8
 1      225.0.7.8        4    198.19.1.9
 1      239.255.255.250  7    10.90.90.90

Total Entries : 11

DGS-3000-28XMP:admin#
```

To display the host IP information for the group “225.0.1.0”:

```
DGS-3000-28XMP:admin# show igmp_snooping host group 225.0.1.0
Command: show igmp_snooping host group 225.0.1.0

VLANID   Group              Port Host
------- ---------------  ---  ---------------
 1        225.0.1.0          2    198.19.1.2
 1        225.0.1.0          2    198.19.1.3
 1        225.0.1.0          3    198.19.1.4

Total Entries : 3

DGS-3000-28XMP:admin#
```

40-24 clear igmp_snooping statistics counter

Description

This command is used to clear the IGMP snooping statistics counter.

Format

clear igmp_snooping statistics counter

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To clear the IGMP snooping statistics counter:

```
DGS-3000-28XMP:admin# clear igmp_snooping statistic counter
Command: clear igmp_snooping statistic counter

Success.

DGS-3000-28XMP:admin#
```

Chapter 41 IP-MAC-Port Binding (IMPB) Command List

create address_binding ip_mac ipaddress <ipaddr> mac_address <macaddr> {ports [<portlist> | all]}
config address_binding ip_mac ports [<portlist> | all] {arp_inspection [strict | loose | disable] | ip_inspection [enable | disable] | nd_inspection [enable | disable] | protocol [ipv4 | ipv6 | all] | allow_zeroip [enable | disable] | forward_dhcppkt [enable | disable] | stop_learning_threshold <int 0-500>}
create address_binding ip_mac ipv6address <ipv6addr> mac_address <macaddr> {ports [<portlist> | all]}
config address_binding ip_mac ipv6address <ipv6addr> mac_address <macaddr> {ports [<portlist>| all]}
delete address_binding blocked [all | vlan_name <vlan_name> mac_address <macaddr>]
delete address_binding ip_mac [all | ipaddress <ipaddr> mac_address <macaddr> | ipv6address <ipv6addr> mac_address <macaddr>]
config address_binding ip_mac ipaddress <ipaddr> mac_address <macaddr> {ports [<portlist> | all]}
show address_binding {ports {<portlist>}}
show address_binding blocked [all | vlan_name <vlan_name> mac_address <macaddr>]
show address_binding ip_mac [all | [ipaddress <ipaddr> | ipv6address <ipv6addr>] mac_address <macaddr>]
show address_binding {[ip_mac [all | [[ipaddress <ipaddr>] [mac_address <macaddr>]] | blocked [all | vlan_name <vlan_name> mac_address <macaddr>] | ports {<portlist>}]}
enable address_binding dhcp_snoop {[ipv6 | all]}
disable address_binding dhcp_snoop {[ipv6 | all]}
clear address_binding dhcp_snoop binding_entry ports [<portlist> | all] {[ipv6 | all]}
show address_binding dhcp_snoop {max_entry {ports <portlist>}}
show address_binding dhcp_snoop binding_entry {port <port>}
config address_binding dhcp_snoop max_entry ports [<portlist> | all] limit [<value 1-50> | no_limit] {ipv6}
enable address_binding nd_snoop
disable address_binding nd_snoop
config address_binding nd_snoop ports [<portlist> | all] max_entry [<value 1-50> | no_limit]
show address_binding nd_snoop {ports <portlist>}
show address_binding nd_snoop binding_entry {port <port>}
clear address_binding nd_snoop binding_entry ports [<portlist> | all]
enable address_binding trap_log
disable address_binding trap_log
config address_binding recover_learning ports [<portlist> | all]
debug address_binding [event | dhcp | all] state [enable | disable]
no debug address_binding
enable address_binding roaming
disable address_binding roaming
download address_binding snoop_entry_fromTFTP [<ipaddr>| <ipv6addr> | <domain_name 255>] filename <path_filename 64>
upload address_binding snoop_entry_toTFTP [<ipaddr> | <ipv6addr> | <domain_name 255>] filename <path_filename 64>

download address_binding snoop_entry_fromFTP [<ipaddr> {tcp_port <tcp_port_number 1-65535>} filename <path_filename 64> | ftp: <string user:pasword@ipaddr:tcpport/path_filename>]
upload address_binding snoop_entry_toFTP [<ipaddr> {tcp_port <tcp_port_number 1-65535>} filename <path_filename 64> | ftp: <string user:pasword@ipaddr:tcpport/path_filename>]
enable address_binding dhcp_pd_snoop
disable address_binding dhcp_pd_snoop
show address_binding dhcp_pd_snoop {binding_entry {port <port>}}

41-1 create address_binding ip_mac ipaddress

Description

This command is used to create an IMPB entry.

Format

create address_binding ip_mac ipaddress <ipaddr> mac_address <macaddr> {ports [<portlist> | all]}

Parameters

<ipaddr> - Enter the IP address used for the IMPB entry.
mac_address - Specifies the MAC address used for the IMPB entry. **<macaddr>** - Enter the MAC address used here.
ports - (Optional) Specifies the portlist the entry will apply to. If not ports are specified, the settings will be applied to all ports. **<portlist>** - Enter a list of ports used for this configuration here. **all** - Specifies that all the ports will be included.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To create an IMPB entry:

```
DGS-3000-28XMP:admin#create address_binding ip_mac ipaddress 10.1.1.1 mac_address 00-00-00-
00-00-11
Command: create address_binding ip_mac ipaddress 10.1.1.1 mac_address 00-00-00-00-00-11


Success.


DGS-3000-28XMP:admin#
```

41-2 config address_binding ip_mac ports

Description

This command is used to configure the state of IMPB on the Switch for each port.

Format

config address_binding ip_mac ports [<portlist> | all] {arp_inspection [strict | loose | disable] | ip_inspection [enable | disable] | nd_inspection [enable | disable] | protocol [ipv4 | ipv6 | all] | allow_zeroip [enable | disable] | forward_dhcppkt [enable | disable] | stop_learning_threshold <int 0-500>}

Parameters

<portlist> - Enter the list of ports used for this configuration here.

all - Specifies that all the ports will be used.

arp_inspection - (Optional) Specifies that the ARP inspection option will be configured.

- **strict** - In this mode, all packets are dropped by default until a legal ARP or IP packet is detected.
- **loose** - In this mode, all packets are forwarded by default until an illegal ARP or broadcasted IP packet is detected.
- **disable** - Specifies to disable ARP inspection function. This is the default value.

ip_inspection - (Optional) Specifies that the IP inspection option will be configured.

- **enable** - Specifies to enable IP inspection function. The legal IP packets will be forwarded, while the illegal IP packets will be dropped.
- **disable** - Specifies to disable IP inspection function. The default value is disabled.

nd_inspection - (Optional) Specifies the ND inspection state of the port.

- **enable** - Specifies to enable the ND inspection state. Legal ND packets will be forwarded, while illegal packets will be dropped.
- **disable** - Specifies to disable the ND inspection state. The default value is disabled.

protocol - (Optional) Specifies the version used.

- **ipv4** - Only IPv4 packets will be checked.
- **ipv6** - Specifies that only IPv6 packets will be checked.
- **all** - Specifies that all packets will be checked.

allow_zeroip - (Optional) Specifies whether to allow ARP packets with a source IP address of 0.0.0.0. If the IP address 0.0.0.0 is not configured in the binding list and this setting is enabled, ARP packets with the source IP address of 0.0.0.0 will be allowed; If the IP address 0.0.0.0 is not configured in the binding list and this setting is disabled, ARP packets with the source IP address of 0.0.0.0 will not be allowed. This option does not affect the IMPB ACL Mode.

- **enable** - Specifies that the allow zero IP option will be enabled.
- **disable** - Specifies that the allow zero IP option will be disabled.

forward_dhcppkt - (Optional) By default, DHCP packets with a broadcast DA will be flooded. When set to disabled, the broadcast DHCP packet received by the specified port will not be forwarded. This setting is effective when DHCP Snooping is enabled, in this case DHCP packets trapped by the CPU must be forwarded by the software. This setting controls the forwarding behavior in this situation.

- **enable** - Specifies that the forward DHCP packets option will be enabled.
- **disable** - Specifies that the forward DHCP packets option will be disabled.

stop_learning_threshold - (Optional) When the number of blocked entries exceeds the threshold, the port will stop learning new addresses. Packets with a new address will be dropped.

- **<int 0-500>** - Enter the stop learning threshold value here. This value must be between 0 and 500.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable IMPB on port 1:

```
DGS-3000-28XMP:admin#config address_binding ip_mac ports 1 arp_inspection strict
Command: config address_binding ip_mac ports 1 arp_inspection strict

Success.

DGS-3000-28XMP:admin#
```

41-3 create address_binding ip_mac ipv6address

Description

This command is used to create an IP-MAC-Port binding entry using IPv6.

Format

create address_binding ip_mac ipv6address <ipv6addr> mac_address <macaddr> {ports [<portlist> | all]}

Parameters

<ipv6addr> - Enter the IPv6 address.
mac_address - Specifies the MAC address. **<macaddr>** - Enter the MAC address here.
ports - (Optional) Specifies a range of ports or all ports. **<portlist>** - Enter a range of ports to be configured. **all** - Specifies to apply to all the ports.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To create a static IPv6 IMPB entry that binds the IPv6 address fe80::240:5ff:fe00:28 to the MAC address 00-00-00-00-00-11:

```
DGS-3000-28XMP:admin#create address_binding ip_mac ipv6address fe80::240:5ff:fe00:28
mac_address 00-00-00-00-00-11
Command: create address_binding ip_mac ipv6address FE80::240:5FF:FE00:28 mac_address 00-00-
00-00-00-11

Success.

DGS-3000-28XMP:admin#
```

41-4 config address_binding ip_mac ipv6address

Description

This command is used to update an address binding entry using IPv6.

Format

config address_binding ip_mac ipv6address <ipv6addr> mac_address <macaddr> {ports [<portlist> | all]}

Parameters

<ipv6addr> - Enter the IPv6 address used here.

mac_address - Specifies the MAC address.
<macaddr> - Enter the MAC address here.

ports - (Optional) Specifies a range of ports to be configured. If the ports are not specified, it will apply to all ports.
<portlist> - Enter a range of ports to be applied to.
all - Specifies all ports to be applied to.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure a static IPv6 IMPB entry so that that IPv6 address fe80::240:5ff:fe00:28 is bound to the MAC address 00-00-00-00-00-11:

```
DGS-3000-28XMP:admin#config address_binding ip_mac ipv6address fe80::240:5ff:fe00:28
mac_address 00-00-00-00-00-11
Command: config address_binding ip_mac ipv6address FE80::240:5FF:FE00:28 mac_address 00-00-
00-00-00-11

Success.

DGS-3000-28XMP:admin#
```

41-5 delete address_binding blocked

Description

This command is used to delete a blocked entry.

Format

delete address_binding blocked [all | vlan_name <vlan_name> mac_address <macaddr>]

Parameters

all - Specifies all the entries in the address database that the system has automatically blocked to be deleted.

vlan_name - Specifies the name of the VLAN associated with the blocked MAC address.
<vlan_name> - Enter the VLAN name.
mac_address - Specifies the MAC address of the entry or the blocked MAC address.
<macaddr> - Enter the MAC address used.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete a blocked address:

```
DGS-3000-28XMP:admin# delete address_binding blocked vlan_name v31 mac_address 00-00-00-00-
00-11
Command: delete address_binding blocked vlan_name v31 mac_address 00-00-00-00-00-11

Success.

DGS-3000-28XMP:admin#
```

41-6 delete address_binding ip_mac

Description

This command is used to delete an IMPB entry.

Format

delete address_binding ip_mac [all | ipaddress <ipaddr> mac_address <macaddr> | ipv6address <ipv6addr> mac_address <macaddr>]

Parameters

all - Specifies all the MAC addresses to be deleted.
ipaddress - Specifies the learned IP address of the entry in the database. **<ipaddr>** - Enter the IP address used. **mac_address** - Specifies the MAC address used for this configuration. **<macaddr>** - Enter the MAC address used.
ipv6address - Specifies the learned IPv6 address of the entry in the database. **<ipv6addr>** - Enter the IPv6 address used. **mac_address** - Specifies the MAC address used for this configuration. **<macaddr>** - Enter the MAC address used.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete a blocked address:

```
DGS-3000-28XMP:admin# delete address_binding ip_mac ipaddress 10.1.1.1 mac_address 00-00-00-
00-00-11
Command: delete address_binding ip_mac ipaddress 10.1.1.1 mac_address 00-00-00-00-00-11

Success.

DGS-3000-28XMP:admin#
```

41-7 config address_binding ip_mac ipaddress

Description

This command is used to update an IMPB entry.

Format

config address_binding ip_mac ipaddress <ipaddr> mac_address <macaddr> {ports [<portlist> | all]}

Parameters

<ipaddr> - Enter the IP address used here.
mac_address - Specifies the MAC address of the entry being updated. **<macaddr>** - Enter the MAC address used here.
ports - (Optional) Specifies which ports are used for the IMPB entry being updated. If not specified, then it is applied to all ports. **<portlist>** - Enter the list of ports used here. **all** - Specifies that all the ports will be used.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure an IMPB entry:

```
DGS-3000-28XMP:admin# config address_binding ip_mac ipaddress 10.1.1.1 mac_address 00-00-00-
00-00-11
Command: config address_binding ip_mac ipaddress 10.1.1.1 mac_address 00-00-00-00-00-11

Success.

DGS-3000-28XMP:admin#
```

41-8 show address_binding

Description

This command is used to display the IMPB global settings or IMPB settings on specified ports.

Format

show address_binding {ports {<portlist>}}

Parameters

ports - (Optional) Specifies the ports for which the information is displayed. If not specified, all ports are displayed. **<portlist>** - (Optional) Enter the list of ports used here.

Restrictions

None.

Example

To show the IMPB global configuration:

```
DGS-3000-28XMP:admin#show address_binding
Command: show address_binding

Roaming state     : Enabled
Trap/Log          : Disabled
DHCP Snoop(IPv4)  : Disabled
DHCP Snoop(IPv6)  : Disabled
DHCP-PD Snoop     : Disabled
ND Snoop          : Disabled
Function Version  : 3.97


DGS-3000-28XMP:admin#
```

To show the IMPB ports:

```
DGS-3000-28XMP:admin#show address_binding ports
Command: show address_binding ports


 ARP: ARP Inspection   IP: IP Inspection   ND: ND Inspection   Prot: Protocol

 Port  ARP      IP       ND       Prot Zero IP   DHCP Packet Stop Learning
                                                             Threshold/Mode
 ----- -------- -------- -------- ---- --------- ----------- --------------
 1     Disabled Disabled Disabled All  Not Allow Forward     500/Normal
 2     Disabled Disabled Disabled All  Not Allow Forward     500/Normal
 3     Disabled Disabled Disabled All  Not Allow Forward     500/Normal
 4     Disabled Disabled Disabled All  Not Allow Forward     500/Normal
 5     Disabled Disabled Disabled All  Not Allow Forward     500/Normal
 6     Disabled Disabled Disabled All  Not Allow Forward     500/Normal
 7     Disabled Disabled Disabled All  Not Allow Forward     500/Normal
 8     Disabled Disabled Disabled All  Not Allow Forward     500/Normal
 9     Disabled Disabled Disabled All  Not Allow Forward     500/Normal
 10    Disabled Disabled Disabled All  Not Allow Forward     500/Normal
 11    Disabled Disabled Disabled All  Not Allow Forward     500/Normal
 12    Disabled Disabled Disabled All  Not Allow Forward     500/Normal
 13    Disabled Disabled Disabled All  Not Allow Forward     500/Normal
 14    Disabled Disabled Disabled All  Not Allow Forward     500/Normal
 15    Disabled Disabled Disabled All  Not Allow Forward     500/Normal
 16    Disabled Disabled Disabled All  Not Allow Forward     500/Normal
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

41-9 show address_binding blocked

Description

This command is used to display the blocked MAC entries.

Format

show address_binding blocked [all | vlan_name <vlan_name> mac_address <macaddr>]

Parameters

all - Specifies all the addresses in the database that the system has auto-learned and blocked to be displayed.
vlan_name - Specifies the name of the VLAN to which the blocked MAC address belongs. **<vlan_name>** - Enter the VLAN name used. **mac_address** - Specifies the MAC address of the entry or the blocked MAC address. **<macaddr>** - Enter the MAC address of the entry or the blocked MAC address.

Restrictions

None.

Example

To show the IMPB entries that are blocked:

```
DGS-3000-28XMP:admin# show address_binding blocked all
Command: show address_binding blocked all

 VID  VLAN Name                        MAC Address       Port
 ---- -------------------------------- ----------------- ----
 1    default                          00-0C-6E-AA-B9-C0 1

Total Entries : 1


DGS-3000-28XMP:admin#
```

41-10 show address_binding ip_mac

Description

This command is used to display the IMPB entries.

Format

show address_binding ip_mac [all | [ipaddress <ipaddr> | ipv6address <ipv6addr>] mac_address <macaddr>]

Parameters

all - Specifies all the IP addresses to be displayed.

ipaddress - Specifies the learned IP address of the entry in the database.
<ipaddr> - Enter the learned IP address.
ipv6address - Specifies the learned IPv6 address of the entry in the database.
<ipv6addr> - Enter the learned IPv6 address.
mac_address - Specifies the MAC address of the entry in the database.
<macaddr> - Enter the MAC address here.

Restrictions

None.

Example

To show IMPB entries:

```
DGS-3000-28XMP:admin# show address_binding ip_mac all
Command: show address_binding ip_mac all

 M(Mode) - D:DHCP, S:Static ACL - A:Active I:Inactive

 IP Address                              MAC Address       M  ACL Ports
 --------------------------------------- ----------------- -- -- ---------------
 10.1.1.1                                00-00-00-00-00-11 S  I  1-28

Total Entries : 1

DGS-3000-28XMP:admin#
```

41-11 enable address_binding dhcp_snoop

Description

This command is used to enable DHCP snooping mode.

By default, DHCP snooping is disabled.

If a user enables DHCP Snooping mode, all ports which have IMPB disabled will become server ports. The switch will learn the IP addresses through server ports (by using DHCP Offer and DHCP ACK packets).

The DHCP discover packet cannot be passed through the user ports if the allow_zeroip function is disabled on the port.

The auto-learned IMPB entry will be mapped to a specific source port based on the MAC address learning function. This entry will be created as an IP-Inspection mode binding entry for this specific port. Each entry is associated with a lease time. When the lease time has expired, the expired entry will be removed from the port. The auto-learned binding entry can be moved from one port to another port if the DHCP snooping function has learned that the MAC address has moved to a different port.

Situations can occur where a binding entry learned by DHCP snooping conflicts with a statically configured entry. For example, if IP A is bound to MAC X with a static configuration and suppose that the binding entry learned by DHCP snooping is that IP A is bound to MAC Y, then it will conflict. When the DHCP snooping learned entry binds with the static configured entry, the DHCP snooping learned entry will not be created.

In a situation where the same IMPB pair has been statically configured, the auto-learned entry will not be created. In a situation where the learned information is consistent with the statically configured entry the auto-learned entry will not be created. In a situation where the entry is statically configured in ARP mode the auto-learned entry will not be created. In a situation where the entry is statically configured on one port and the entry is auto-learned on another port, the auto-learned entry will not be created.

Format

enable address_binding dhcp_snoop {[ipv6 | all]}

Parameters

ipv6 - (Optional) Specifies to disable the IPv6 entries.
all - (Optional) Specifies to disable all DHCP snooping mode.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable DHCP IPv4 snooping mode:

```
DGS-3000-28XMP:admin# enable address_binding dhcp_snoop
Command: enable address_binding dhcp_snoop

Success.

DGS-3000-28XMP:admin#
```

41-12 disable address_binding dhcp_snoop

Description

This command is used to disable DHCP snooping mode. When the DHCP snooping function is disabled, all of auto-learned binding entries will be removed.

Format

disable address_binding dhcp_snoop {[ipv6 | all]}

Parameters

ipv6 - (Optional) Specifies to disable the IPv6 entries.
all - (Optional) Specifies to disable all DHCP snooping mode.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To disable DHCP IPv4 snooping mode:

```
DGS-3000-28XMP:admin# disable address_binding dhcp_snoop
Command: disable address_binding dhcp_snoop

Success.

DGS-3000-28XMP:admin#
```

41-13 clear address_binding dhcp_snoop binding_entry ports

Description

This command is used to clear the DHCP snooping entries learned for the specified ports.

Format

clear address_binding dhcp_snoop binding_entry ports [<portlist> | all] {[ipv6 | all]}

Parameters

<portlist> - Enter the list of ports used.
all - Specifies that all the ports will be used.
ipv6 - (Optional) Specifies to clear the IPv6 entries.
all - (Optional) Specifies to clear all entries.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To clear DHCP IPv4 snooping entries on ports 1-3:

```
DGS-3000-28XMP:admin# clear address_binding dhcp_snoop binding_entry ports 1-3
Command: clear address_binding dhcp_snoop binding_entry ports 1-3

Success.

DGS-3000-28XMP:admin#
```

41-14 show address_binding dhcp_snoop

Description

This command is used to display the DHCP snooping configuration and learning database.

Format

show address_binding dhcp_snoop {max_entry {ports <portlist>}}

Parameters

max_entry - (Optional) Specifies to show the maximum number of entries per port. **ports** - (Optional) Specifies the ports used for this configuration. **<portlist>** - Enter a list of ports used here.
If no parameter is specified, show DHCP snooping displays the enable/disable state.

Restrictions

None.

Example

To show the DHCP snooping state:

```
DGS-3000-28XMP:admin#show address_binding dhcp_snoop
Command: show address_binding dhcp_snoop

DHCP Snoop(IPv4) : Disabled
DHCP Snoop(IPv6) : Disabled

DGS-3000-28XMP:admin#
```

To display DHCP snooping maximum entry configuration:

```
DGS-3000-28XMP:admin#show address_binding dhcp_snoop max_entry
Command: show address_binding dhcp_snoop max_entry

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
6     No Limit   No Limit
7     No Limit   No Limit
8     No Limit   No Limit
9     No Limit   No Limit
10    No Limit   No Limit
11    No Limit   No Limit
12    No Limit   No Limit
13    No Limit   No Limit
14    No Limit   No Limit
15    No Limit   No Limit
16    No Limit   No Limit
17    No Limit   No Limit
18    No Limit   No Limit
19    No Limit   No Limit
20    No Limit   No Limit
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

41-15 show address_binding dhcp_snoop binding_entry

Description

This command is used to display the DHCP snooping binding entries.

Format

show address_binding dhcp_snoop binding_entry {port <port>}

Parameters

port - (Optional) Specifies the port used for this configuration.
<port> - Enter the port number used here.

Restrictions

None.

Example

To display the DHCP snooping binding entries:

```
DGS-3000-28XMP:admin#show address_binding dhcp_snoop binding_entry
Command: show address_binding dhcp_snoop binding_entry

 S (Status) - A: Active, I: Inactive
 Time - Left Time (sec)

 IP Address                              MAC Address       S  LT(sec)    Port
 --------------------------------------- ----------------- -- ---------- -----

Total Entries : 0

DGS-3000-28XMP:admin#
```

41-16 config address_binding dhcp_snoop max_entry ports

Description

This command is used to specify the maximum number of entries that can be learned by a specified port.

Format

config address_binding dhcp_snoop max_entry ports [<portlist> | all] limit [<value 1-50> | no_limit] {ipv6}

Parameters

<portlist> - Enter the list of ports used here.

all - Specifies that all the ports will be used.

limit - Specifies the maximum number. The default value is no_limit.
<value 1-50> - Enter the limit value here. This value must be between 1 and 50.

	no_limit - Specifies that the maximum number of learned entries is unlimited.
ipv6 - (Optional) Specifies the IPv6 address used for this configuration.	

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To set the maximum number of DHCP IPv4 snooping entries that ports 1–3 can learn to 10 entries:

```
DGS-3000-28XMP:admin# config address_binding dhcp_snoop max_entry ports 1-3 limit 10
Command: config address_binding dhcp_snoop max_entry ports 1-3 limit 10

Success.

DGS-3000-28XMP:admin#
```

41-17 enable address_binding nd_snoop

Description

This command is used to enable ND snooping on the Switch.

Format

enable address_binding nd_snoop

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable the ND snooping function on the switch:

```
DGS-3000-28XMP:admin#enable address_binding nd_snoop
Command: enable address_binding nd_snoop

Success.

DGS-3000-28XMP:admin#
```

41-18 disable address_binding nd_snoop

Description

This command is used to disable ND snooping on the Switch.

Format

disable address_binding nd_snoop

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To disable the ND snooping function on the switch:

```
DGS-3000-28XMP:admin#disable address_binding nd_snoop
Command: disable address_binding nd_snoop

Success.

DGS-3000-28XMP:admin#
```

41-19 config address_binding nd_snoop ports

Description

This command is used to specify the maximum number of entries that can be learned with ND snooping. By default, there is no limit on the maximum number of entries that can be learned on a port with ND snooping.

Format

config address_binding nd_snoop ports [<portlist> | all] max_entry [<value 1-50> | no_limit]

Parameters

<portlist> - Enter the list of ports used for this configuration.
all - Specifies that all the ports will be used for this configuration.
max_entry - Specifies the maximum number of entries. **<value 1-50>** - Enter the maximum number of entries used here. This value must be between 1 and 50. **no_limit** - Specifies that the maximum number of learned entries is unlimited.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To have a maximum of 10 entries can be learned by ND snooping on ports 1 to 3:

```
DGS-3000-28XMP:admin#config address_binding nd_snoop ports 1-3 max_entry 10
Command: config address_binding nd_snoop ports 1-3 max_entry 10

Success.

DGS-3000-28XMP:admin#
```

41-20 show address_binding nd_snoop

Description

This command is used to display the status of ND snooping on the Switch.

Format

show address_binding nd_snoop {ports <portlist>}

Parameters

ports - (Optional) Specifies the list of ports used for this display.
<portlist> - Enter the list of ports used for this display here.

Restrictions

None.

Example

To show the ND snooping state:

```
DGS-3000-28XMP:admin#show address_binding nd_snoop
Command: show address_binding nd_snoop

ND Snoop          : Enabled

DGS-3000-28XMP:admin#
```

To show the ND snooping maximum entry information for ports 1-5:

```
DGS-3000-28XMP:admin#show address_binding nd_snoop ports 1-5
Command: show address_binding nd_snoop ports 1-5

Port  Max Entry
----  ---------
1     10
2     10
3     10
4     No Limit
5     No Limit

DGS-3000-28XMP:admin#
```

41-21 show address_binding nd_snoop binding_entry

Description

This command is used to show the ND snooping binding entries on the Switch.

Format

show address_binding nd_snoop binding_entry {port <port>}

Parameters

port - (Optional) Specifies a port used for this display.
<port> - Enter the port number used for this display here.

Restrictions

None.

Example

To show the ND snooping binding entry:

```
DGS-3000-28XMP:admin#show address_binding nd_snoop binding_entry
Command: show address_binding nd_snoop binding_entry

 S (Status) - A: Active, I: Inactive
 Time - Left Time (sec)

 IP Address                              MAC Address       S  LT(sec)    Port
 --------------------------------------- ----------------- -- ---------- -----
 2001:2222:1111:7777:5555:6666:7777:8888 00-00-00-00-00-02  I  50         5
 2001::1                                 00-00-00-00-03-02  A  100        6

Total Entries : 2

DGS-3000-28XMP:admin#
```

41-22 clear address_binding nd_snoop binding_entry ports

Description

This command is used to clear the ND snooping entries on specified ports.

Format

clear address_binding nd_snoop binding_entry ports [<portlist> | all]

Parameters

<portlist> - Enter the list of ports that you would like to clear the ND snoop learned entry.

all - Specifies to clear all ND snooping learned entries.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To clear ND snooping entry on ports 1-3:

```
DGS-3000-28XMP:admin#clear address_binding nd_snoop binding_entry ports 1-3
Command: clear address_binding nd_snoop binding_entry ports 1-3

Success.

DGS-3000-28XMP:admin#
```

41-23 enable address_binding trap_log

Description

This command is used to send traps and logs when the IMPB module detects an illegal IP and MAC address.

Format

enable address_binding trap_log

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable the IMPB traps and logs:

```
DGS-3000-28XMP:admin# enable address_binding trap_log
Command: enable address_binding trap_log

Success.

DGS-3000-28XMP:admin#
```

41-24 disable address_binding trap_log

Description

This command is used to disable the IMPB traps and logs.

Format

disable address_binding trap_log

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To disable IMPB traps and logs:

```
DGS-3000-28XMP:admin# disable address_binding trap_log
Command: disable address_binding trap_log

Success.

DGS-3000-28XMP:admin#
```

41-25 config address_binding recover_learning ports

Description

This command is used to recover the IMPB checking functionality after it has been stopped on the specified ports.

Format

config address_binding recover_learning ports [<portlist> | all]

Parameters

<portlist> - Enter the list of ports that will be used in this configuration.
all - Specifies that all the ports will be used in this configuration.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To recover the IMPB checking functionality on ports 6 to 8:

```
DGS-3000-28XMP:admin# config address_binding recover_learning ports 6-8
Command: config address_binding recover_learning ports 6-8

Success.

DGS-3000-28XMP:admin#
```

41-26 debug address_binding

Description

This command is used to start the IMPB debug when the IMPB module receives an ARP/IP packet or a DHCP packet.

Format

debug address_binding [event | dhcp | all] state [enable | disable]

Parameters

event - Specifies to print out the debug messages when the IMPB module receives ARP/IP packets.
dhcp - Specifies to print out the debug messages when the IMPB module receives DHCP packets.
all - Specifies to print out all debug messages.
state - Specifies the IMPB debug state to be enabled or disabled. **enable** - Specifies to enable the IMPB debug state. **disable** - Specifies to disable the IMPB debug state.

Restrictions

Only Administrators can issue this command.

Example

To print out all debug IMPB messages:

```
DGS-3000-28XMP:admin# debug address_binding all state enable
Command: debug address_binding all state enable

Success.

DGS-3000-28XMP:admin#
```

41-27 no debug address_binding

Description

This command is used to stop the IMPB debug when the IMPB module receives an ARP/IP packet or a DHCP packet.

Format

no debug address_binding

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To stop IMPB debug: when the IMPB module receives an ARP/IP or DHCP packet:

```
DGS-3000-28XMP:admin# no debug address_binding
Command: no debug address_binding

Success.

DGS-3000-28XMP:admin#
```

41-28 enable address_binding roaming

Description

This command is used to enable the IMPB roaming.

Format

enable address_binding roaming

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable the IMPB roaming:

```
DGS-3000-28XMP:admin#enable address_binding roaming
Command: enable address_binding roaming

Success.

DGS-3000-28XMP:admin#
```

41-29 disable address_binding roaming

Description

This command is used to disable the IMPB roaming.

Format

disable address_binding roaming

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To disable the IMPB roaming:

```
DGS-3000-28XMP:admin#disable address_binding roaming
Command: disable address_binding roaming

Success.

DGS-3000-28XMP:admin#
```

41-30 download address_binding snoop_entry_fromTFTP

Description

This command is used to download DHCPv4 snooping binding entries from the TFTP server.

Limitations when downloading DHCP snooping bind entries:

- If IMPB is disabled, downloading binding entries cannot be performed.
- If DHCP snooping is disabled, downloading binding entries cannot be performed.
- The binding entry will be discarded if the data integrity check failed.
- The binding entry will be discarded if the entry does not match the IMPB configuration.
- The binding entry will be discarded if the entry conflicts with the current binding table.
- The binding entry will be discarded if the entry already exists.
- The binding entry will be discarded if the hardware resource is not available.
- The uploaded and restored time left of the binding entry will be recorded while the entry is downloaded.
- The lease time of the entry will not be modified and the lifetime counter will continue while the entry is provisioned.

Format

download address_binding snoop_entry_fromTFTP [<ipaddr>| <ipv6addr> | <domain_name 255>] filename <path_filename 64>

Parameters

<ipaddr> - Enter the IP address of the TFTP server.
<ipv6addr> - Enter the IPv6 address of the TFTP server.
<domain_name 255> - Enter the domain name of the TFTP server.
filename - Specifies to enter the parameter “path_filename”. **<path_filename 64>** - Enter the pathname here. This name can be up to 64 characters long.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To download the DHCP snooping binding table from the TFTP server:

```
DGS-3000-28XMP:admin#download address_binding snoop_entry_fromTFTP 10.0.0.1 filename impb.cfg
Command: download address_binding snoop_entry_fromTFTP 10.0.0.1 filename impb.cfg

Success.

DGS-3000-28XMP:admin#
```

41-31 upload address_binding snoop_entry_toTFTP

Description

This command is used to upload DHCPv4 snooping binding entries to the TFTP server.

Format

upload address_binding snoop_entry_toTFTP [<ipaddr> | <ipv6addr> | <domain_name 255>] filename <path_filename 64>

Parameters

<ipaddr> - Enter the IP address of the TFTP server.
<ipv6addr> - Enter the IPv6 address of the TFTP server.
<domain_name 255> - Enter the domain name of the TFTP server.
filename - Specifies to enter the parameter “path_filename”. **<path_filename 64>** - Enter the pathname here. This name can be up to 64 characters long.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To upload the DHCP snooping binding table to the TFTP server:

```
DGS-3000-28XMP:admin#upload address_binding snoop_entry_toTFTP 10.0.0.1 filename impb.cfg
Command: upload address_binding snoop_entry_toTFTP 10.0.0.1 filename impb.cfg

Success.

DGS-3000-28XMP:admin#
```

41-32 download address_binding snoop_entry_fromFTP

Description

This command is used to download DHCPv4 snooping binding entries from the FTP server.

Limitations when downloading DHCP snooping bind entries:

- If IMPB is disabled, downloading binding entries cannot be performed.

- If DHCP snooping is disabled, downloading binding entries cannot be performed.
- The binding entry will be discarded if the data integrity check failed.
- The binding entry will be discarded if the entry does not match the IMPB configuration.
- The binding entry will be discarded if the entry conflicts with the current binding table.
- The binding entry will be discarded if the entry already exists.
- The binding entry will be discarded if the hardware resource is not available.
- The uploaded and restored time left of the binding entry will be recorded while the entry is downloaded.
- The lease time of the entry will not be modified and the lifetime counter will continue while the entry is provisioned.

Format

download address_binding snoop_entry_fromFTP [<ipaddr> {tcp_port <tcp_port_number 1-65535>} filename <path_filename 64> | ftp: <string user:pasword@ipaddr:tcpport/path_filename>]

Parameters

<ipaddr> - Enter the IP address of the FTP server.

tcp_port - Specifies the TCP port.

<tcp_port_number1-65535> - Enter a value between 1 and 65535.

filename - Specifies the source file location.

<path_filename 64> - Enter the pathname specifies the pathname on the FTP server. It can be a relative pathname or an absolute pathname. This name can be up to 64 characters long.

ftp: - Specifies the FTP site.

<string user:password@ipaddr:tcpport/path_filename> - Enter the FTP directory.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To download the DHCP snooping binding table from the FTP server:

```
DGS-3000-28XMP:admin#download address_binding snoop_entry_fromFTP 10.0.0.1 tcp_port 21
filename impb.cfg
Command: download address_binding snoop_entry_fromFTP 10.0.0.1 tcp_port 21 filename impb.cfg

Connecting to server.................. Done.
User(Anonymous): IMPB
Pass:******
Download DHCPv4 Snooping binding table................. Done.

Success.

DGS-3000-28XMP:admin#
```

41-33 upload address_binding snoop_entry_toFTP

Description

This command is used to upload DHCPv4 snooping binding entries to the FTP server.

Format

upload address_binding snoop_entry_toFTP [<ipaddr> {tcp_port <tcp_port_number 1-65535>} filename <path_filename 64> | ftp: <string user:pasword@ipaddr:tcpport/path_filename>]

Parameters

<ipaddr> - Enter the IP address of the FTP server.

tcp_port - Specifies the TCP port.

<tcp_port_number1-65535> - Enter a value between 1 and 65535.

filename - Specifies the source file location.

<path_filename 64> - Enter the pathname specifies the pathname on the FTP server. It can be a relative pathname or an absolute pathname. This name can be up to 64 characters long.

ftp: - Specifies the FTP site.

<string user:password@ipaddr:tcpport/path_filename> - Enter the FTP directory.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To upload the DHCP snooping binding table to the FTP server:

```
DGS-3000-28XMP:admin# upload address_binding snoop_entry_toFTP 10.0.0.1 tcp_port 21 filename
impb.cfg
Command: upload address_binding snoop_entry_toFTP 10.0.0.1 tcp_port 21 filename impb.cfg

Connecting to server.................. Done.
User(Anonymous): IMPB
Pass:******
Upload DHCPv4 Snooping binding table................. Done.

Success.

DGS-3000-28XMP:admin#
```

41-34 enable address_binding dhcp_pd_snoop

Description

This command is used to enable DHCP-PD snooping. This function is used to snoop IPv6 prefixes assigned using DHCPv6 prefix delegation (PD) protocol. It sets up the IPv6-prefix white-list. IMPBv6 filters IPv6 packets based on this white-list. When the source IP matches the white-list, IPv6 packets will be forwarded. Otherwise, packets will be dropped.

Format

enable address_binding dhcp_pd_snoop

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable DHCP-PD snooping:

```
DGS-3000-28XMP:admin#enable address_binding dhcp_pd_snoop
Command: enable address_binding dhcp_pd_snoop

Success.

DGS-3000-28XMP:admin#
```

41-35 disable address_binding dhcp_pd_snoop

Description

This command is used to disable DHCP-PD snooping. This is the default option. When disabled, all of auto-learned binding entries will be removed.

Format

disable address_binding dhcp_pd_snoop

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To disable DHCP-PD snooping:

```
DGS-3000-28XMP:admin#disable address_binding dhcp_pd_snoop
Command: disable address_binding dhcp_pd_snoop

Success.

DGS-3000-28XMP:admin#
```

41-36 show address_binding dhcp_pd_snoop

Description

This command is used to display the information of DHCP-PD snooping.

Format

show address_binding dhcp_pd_snoop {binding_entry {port <port>}}

Parameters

binding_entry - (Optional) Specifies to display DHCP-PD snooping binding entries. If no parameter is specified, DHCP-PD snooping configuration will be displayed.

port - (Optional) Specifies the port. If no port is specified, all binding entries will be displayed.

<port> - Enter the port to be displayed.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To display DHCP-PD snooping configuration:

```
DGS-3000-28XMP:admin#show address_binding dhcp_pd_snoop
Command: show address_binding dhcp_pd_snoop

DHCP-PD Snoop : Enabled

DGS-3000-28XMP:admin#
```

To display DHCP-PD snooping binding entries:

```
DGS-3000-28XMP:admin#show address_binding dhcp_pd_snoop binding_entry
Command: show address_binding dhcp_pd_snoop binding_entry

 S (Status) - A: Active, I: Inactive
 Time - Left Time (sec)

 IP Address                              MAC Address       S  LT(sec)    Port
 --------------------------------------- ----------------- -- ---------- -----

Total Entries : 0

DGS-3000-28XMP:admin#
```

Chapter 42 IPv6 Neighbor Discover Command List

create ipv6 neighbor_cache ipif <ipif_name 12> <ipv6addr> <macaddr>
delete ipv6 neighbor_cache ipif [<ipif_name 12> | all] [<ipv6addr> | static | dynamic | all]
show ipv6 neighbor_cache ipif [<ipif_name 12> | all] [ipv6address <ipv6addr> | static | dynamic | all]
config ipv6 nd ns ipif <ipif_name 12> **retrans_time** <millisecond 0-4294967295>
show ipv6 nd {ipif <ipif_name 12>}

42-1 create ipv6 neighbor_cache ipif

Description

This command is used to add a static neighbor on an IPv6 interface.

Format

create ipv6 neighbor_cache ipif <ipif_name 12> <ipv6addr> <macaddr>

Parameters

<ipif_name 12> - Enter the IP interface name here. This name can be up to 12 characters long.
<ipv6addr> - Enter the address of the neighbor.
<macaddr> - Enter the MAC address of the neighbor.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

Create a static neighbor cache entry:

```
DGS-3000-28XMP:admin# 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-3000-28XMP:admin#
```

42-2 delete ipv6 neighbor_cache ipif

Description

This command is used to delete a neighbor cache entry or static neighbor cache entries from the address cache or all address cache entries on this IP interface. Both static and dynamic entries can be deleted.

Format

delete ipv6 neighbor_cache ipif [<ipif_name 12> | all] [<ipv6addr> | static | dynamic | all]

Parameters

<ipif_name 12> - Enter the IP interface name here. This name can be up to 12 characters long.
all - Specifies that all the interfaces will be used in this configuration.
<ipv6addr> - Enter the neighbor's IPv6 address.
static - Specifies to delete the static entry.
dynamic - Specifies to delete the dynamic entries.
all - Specifies that all entries including static and dynamic entries will be deleted.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete a neighbor cache entry on IP interface "System":

```
DGS-3000-28XMP:admin# delete ipv6 neighbor_cache ipif System 3ffc::1
Command: delete ipv6 neighbor_cache ipif System 3FFC::1

Success.

DGS-3000-28XMP:admin#
```

42-3 show ipv6 neighbor_cache ipif

Description

This command is used to display the neighbor cache entry for the specified interface. You can display a specific entry, all entries, or all static entries.

Format

show ipv6 neighbor_cache ipif [<ipif_name 12> | all] [ipv6address <ipv6addr> | static | dynamic | all]

Parameters

<ipif_name 12> - Enter the IP interface name here. This name can be up to 12 characters long.
all - Specifies that all the interface will be displayed.
ipv6address - Specifies the neighbor's IPv6 address. **<ipv6addr>** - Enter the IPv6 address here.
static - Specifies the static neighbor cache entry.
dynamic - Specifies the dynamic entries.
all - Specifies that all entries including static and dynamic entries will be displayed.

Restrictions

None

Example

Show all neighbor cache entries of IP interface “System”:

```
DGS-3000-28XMP:admin# show ipv6 neighbor_cache ipif System all
Command: show ipv6 neighbor_cache ipif System all


3FFC::1                                 State: Static
MAC Address : 00-01-02-03-04-05         Port : NA
Interface   : System                    VID  : 1

Total Entries: 1


DGS-3000-28XMP:admin#
```

42-4 config ipv6 nd ns retrans_time ipif

Description

This command is used to configure the IPv6 ND neighbor solicitation retransmit time, which is the interval between retransmissions of neighbor solicitation messages to a neighbor when resolving the address or when probing the reachability of a neighbor.

Format

config ipv6 nd ns ipif <ipif_name 12> retrans_time <millisecond 0-4294967295>

Parameters

<ipif_name 12> - Enter the IP interface name here. This name can be up to 12 characters long.
retrans_time - Specifies the neighbor solicitation retransmit timer in millisecond. **<millisecond 0-4294967295>** - Enter the retransmit timer value here. This value must be between 0 and 4294967295 milliseconds.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the retransmit time of IPv6 ND neighbor solicitation:

```
DGS-3000-28XMP:admin# config ipv6 nd ns ipif Zira retrans_time 1000000
Command: config ipv6 nd ns ipif Zira retrans_time 1000000

Success.

DGS-3000-28XMP:admin#
```

42-5 show ipv6 nd

Description

This command is used to display information regarding neighbor detection on the Switch.

Format

show ipv6 nd {ipif <ipif_name 12>}

Parameters

ipif - (Optional) The name of the interface. **<ipif_name 12>** - Enter the IP interface name here. This name can be up to 12 characters long.
If no parameter is specified, it will show the IPv6 ND related configuration of all interfaces.

Restrictions

None.

Example

To show IPv6 ND related configuration:

```
DGS-3000-28XMP:admin# show ipv6 nd ipif System
Command: show ipv6 nd ipif System

Interface Name            : System
NS Retransmit Time        : 0 (ms)

DGS-3000-28XMP:admin#
```

Chapter 43 Jumbo Frame Command List

enable jumbo_frame
disable jumbo_frame
show jumbo_frame

43-1 enable jumbo_frame

Description

This command is used to enable jumbo frames.

Format

enable jumbo_frame

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable the Jumbo frame:

```
DGS-3000-28XMP:admin#enable jumbo_frame
Command: enable jumbo_frame

The maximum size of jumbo frame is 9216 bytes.
Success.

DGS-3000-28XMP:admin#
```

43-2 disable jumbo_frame

Description

This command is used to disable jumbo frames.

Format

disable jumbo_frame

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To disable the Jumbo frame:

```
DGS-3000-28XMP:admin# disable jumbo_frame
Command: disable jumbo_frame

Success.

DGS-3000-28XMP:admin#
```

43-3 show jumbo_frame

Description

This command is used to display the current jumbo frame configuration.

Format

show jumbo_frame

Parameters

None.

Restrictions

None.

Example

To show the Jumbo frame:

```
DGS-3000-28XMP:admin# show jumbo_frame
Command: show jumbo_frame

Jumbo Frame State  : Disabled
Maximum Frame Size : 1536 Bytes

DGS-3000-28XMP:admin#
```

Chapter 44 Layer 2 Protocol Tunneling (L2PT) Command List

enable l2protocol_tunnel
disable l2protocol_tunnel
config l2protocol_tunnel ports [<portlist> | all] type [uni tunneled_protocol [{stp | gvrp | protocol_mac [01-00-0C-CC-CC-CC | 01-00-0C-CC-CC-CD]}(1) | all] {threshold <value 0-65535>} | nni | none]
show l2protocol_tunnel {[uni | nni]}

44-1 enable l2protocol_tunnel

Description

This command is used to enable the L2PT function.

Format

enable l2protocol_tunnel

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable the L2PT function:

```
DGS-3000-28XMP:admin# enable l2protocol_tunnel
Command: enable l2protocol_tunnel

Success.

DGS-3000-28XMP:admin#
```

44-2 disable l2protocol_tunnel

Description

This command is used to disable the L2PT function globally on the Switch.

Format

disable l2protocol_tunnel

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To disable the L2PT function:

```
DGS-3000-28XMP:admin# disable l2protocol_tunnel
Command: disable l2protocol_tunnel

Success.

DGS-3000-28XMP:admin#
```

44-3 config l2protocol_tunnel ports

Description

This command is used to configure L2PT on ports. L2PT is used to tunnel Layer 2 protocol packets. If a Layer 2 protocol is tunnel-enabled on an UNI, once the PDU is received on this port, the multicast destination address of the PDU will be replaced by the L2PT multicast address. The L2PT multicast address for STP is 01-05-5D-00-00-00, for GVRP is 01-05-5D-00-00-21, for Layer 2 protocols MAC 01-00-0C-CC-CC-CC is 01-05-5D-00-00-10 and for protocol MAC 01-00-0C-CC-CC-CD is 01-05-5D-00-00-11.

When QinQ is enabled, an S-TAG will be added to the Layer 2 PDU. The S-TAG is assigned according to the QinQ VLAN configuration.

Format

config l2protocol_tunnel ports [<portlist> | all] type [uni tunneled_protocol [{stp | gvrp | protocol_mac [01-00-0C-CC-CC-CC | 01-00-0C-CC-CC-CD]}(1) | all] {threshold <value 0-65535>} | nni | none]

Parameters

<portlist> - Specifies a list of ports on which the L2PT to be configured.

all – Specifies all ports to be configured.

type - Specifies the type of the ports.

- **uni** - Specifies the ports as UNI ports.
  - **tunneled_protocol** - Specifies the tunneling protocol on the UNI ports.
    - **stp** - Specifies to use the STP protocol.
    - **gvrp** - Specifies to use the GVRP protocol.
    - **protocol_mac** - Specifies the destination MAC address of the L2 protocol packets that will be tunneled on these UNI ports.
      - **01-00-0C-CC-CC-CC** - Specifies the MAC address as 01-00-0C-CC-CC-CC.
      - **01-00-0C-CC-CC-CD** - Specifies the MAC address as 01-00-0C-CC-CC-CD.
    - **all** - Specifies that all tunnel-abled Layer 2 protocols will be tunneled on the ports.
  - **threshold** - (Optional) Specifies the drop threshold for packets-per-second accepted on the UNI ports. The ports drop the PDU if the protocol's threshold is exceeded.
    - **<value 0-65535>** - Enter the threshold value ranging from 0 to 65535 (packet/second). The value 0

means no limit. By default, the value is 0.
nni - Specifies the ports as NNI ports.
none - Specifies to disable tunneling on the port(s).

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the STP tunneling on ports 1-4:

```
DGS-3000-28XMP:admin# config l2protocol_tunnel ports 1-4 type uni tunneled_protocol stp
Command: config l2protocol_tunnel ports 1-4 type uni tunneled_protocol stp

Success.

DGS-3000-28XMP:admin#
```

44-4 show l2protocol_tunnel

Description

This command is used to display L2PT information.

Format

show l2protocol_tunnel {[uni | nni]}

Parameters

uni - (Optional) Specifies to show UNI detail information, including tunneled and dropped PDU statistics.
nni - (Optional) Specifies to show NNI detail information, including de-capsulated Layer 2 PDU statistics.

Restrictions

None.

Example

To show L2PT information summary:

```
DGS-3000-28XMP:admin# show l2protocol_tunnel
Command: show l2protocol_tunnel

Global State : Enabled
UNI Ports    : 1-4
NNI Ports    :

DGS-3000-28XMP:admin#
```

To show UNI Layer 2 protocol tunneling information:

```
DGS-3000-28XMP:admin# show l2protocol_tunnel uni
Command: show l2protocol_tunnel uni

 UNI   Tunneled           Threshold
 Port  Protocol           (packet/sec)
 ----  -----------------  ------------
 1     STP                0
 2     STP                0
 3     STP                0
 4     STP                0

DGS-3000-28XMP:admin#
```

Chapter 45 Link Aggregation Command List

create link_aggregation group_id <value> {type [lacp | static]}
delete link_aggregation group_id <value>
config link_aggregation group_id <value> {master_port <port> | ports <portlist> | state [enable | disable]
config link_aggregation algorithm [mac_source | mac_destination|mac_source_dest | ip_source | ip_destination | ip_source_dest]
show link_aggregation {group_id <value> | algorithm}
config lacp_port <portlist> mode [active | passive]
show lacp_port {<portlist>}

45-1 create link_aggregation group_id

Description

This command is used to create a link aggregation group on the Switch.

Format

create link_aggregation group_id <value> {type [lacp | static]}

Parameters

<value > - Enter the group ID value here.
type - (Optional) Specifies the group type as static or LACP. If type is not specified, the default is static type. **lacp** - Specifies to use LACP as the group type. **static** - Specifies to use static as the group type.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To create link aggregation group:

```
DGS-3000-28XMP:admin# create link_aggregation group_id 1 type lacp
Command: create link_aggregation group_id 1 type lacp

Success.

DGS-3000-28XMP:admin#
```

45-2 delete link_aggregation group_id

Description

This command is used to delete a previously configured link aggregation group.

Format

delete link_aggregation group_id <value>

Parameters

<value> - Enter the group ID value here.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete link aggregation group:

```
DGS-3000-28XMP:admin# delete link_aggregation group_id 3
Command: delete link_aggregation group_id 3

Success.

DGS-3000-28XMP:admin#
```

45-3 config link_aggregation group_id

Description

This command is used to configure a previously created link aggregation group. Port locking, port mirroring, traffic control, and 802.1X must not be enabled on the trunk group.

Format

config link_aggregation group_id <value> {master_port <port> | ports <portlist> | state [enable | disable]

Parameters

<value> - Enter the group ID value here.

master_port - (Optional) Specifies the master port ID. Specifies which port (by port number) of the link aggregation group will be the master port. All of the ports in a link aggregation group will share the same port configuration as the master port.

<port> - Enter the master port number here.

ports - (Optional) Specifies a range of ports that will belong to the link aggregation group.

<portlist> - Enter the list of ports used for the configuration here.

state - (Optional) Specifies to enable or disable the specified link aggregation group. If not specified, the group will keep the previous state.

enable - Specifies to enable the specified link aggregation group.

disable - Specifies to disable the specified link aggregation group. This is the default option.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To define a load-sharing group of ports:

```
DGS-3000-28XMP:admin# config link_aggregation group_id 1 master_port 5 ports 5-7
Command: config link_aggregation group_id 1 master_port 5 ports 5-7

Success.

DGS-3000-28XMP:admin#
```

45-4 config link_aggregation algorithm

Description

This command is used to configure the Link Aggregation algorithm. This feature is available using the address-based load-sharing algorithm, only.

Format

config link_aggregation algorithm [mac_source | mac_destination|mac_source_dest | ip_source | ip_destination | ip_source_dest]

Parameters

mac_source - Specifies that the Switch should examine the MAC source address.
mac_destination - Specifies that the Switch should examine the MAC destination address.
mac_source_dest - Specifies that the Switch should examine the MAC source and destination address.
ip_source - Specifies that the Switch should examine the IP source address.
ip_destination - Specifies that the Switch should examine the IP destination address.
ip_source_dest - Specifies that the Switch should examine the IP source address and destination address.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

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

```
DGS-3000-28XMP:admin# config link_aggregation algorithm mac_source_dest
Command: config link_aggregation algorithm mac_source_dest

Success.

DGS-3000-28XMP:admin#
```

45-5 show link_aggregation

Description

This command is used to display the current link aggregation configuration on the Switch.

Format

show link_aggregation {group_id <value> | algorithm}

Parameters

group_id - (Optional) Specifies the group ID. The group number identifies each of the groups. **<value>** - Enter the group ID value here.
algorithm - (Optional) Specifies to allow you to specify the display of link aggregation by the algorithm in use by that group.
If no parameter is specified, system will display all link aggregation information.

Restrictions

None.

Example

Link aggregation group enable:

```
DGS-3000-28XMP:admin# show link_aggregation
Command: show link_aggregation

Link Aggregation Algorithm = MAC-Source-Dest

Group ID      : 1
Type          : LACP
Master Port   : 5
Member Port   : 5-7
Active Port   :
Status        : Enabled
Flooding Port : 7

Total Entries : 1

DGS-3000-28XMP:admin#
```

Link aggregation group enable and no member linkup:

```
DGS-3000-28XMP:admin# show link_aggregation
Command: show link_aggregation

Link Aggregation Algorithm = MAC-Source-Dest

Group ID      : 1
Type          : LACP
Master Port   : 5
Member Port   : 5-7
Active Port   :
Status        : Enabled
Flooding Port :

Total Entries : 1

DGS-3000-28XMP:admin#
```

Link aggregation group disabled:

```
DGS-3000-28XMP:admin# show link_aggregation
Command: show link_aggregation

Link Aggregation Algorithm = MAC-Source-Dest

Group ID      : 1
Type          : LACP
Master Port   : 5
Member Port   : 5-7
Active Port   :
Status        : Disabled
Flooding Port : 7

Total Entries : 1

DGS-3000-28XMP:admin#
```

45-6 config lacp_port

Description

This command is used to configure the LACP mode per port.

Format

config lacp_port <portlist> mode [active | passive]

Parameters

<portlist> - Enter the list of ports used for the configuration here.
mode - Specifies the LACP mode used. **active** - Specifies to set the LACP mode as active. **passive** - Specifies to set the LACP mode as passive.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure LACP mode on port 1-12:

```
DGS-3000-28XMP:admin# config lacp_port 1-12 mode active
command: config lacp_port 1-12 mode active

Success.

DGS-3000-28XMP:admin#
```

45-7 show lacp_port

Description

This command is used to display the current LACP mode of the ports.

Format

show lacp_port {<portlist>}

Parameters

<portlist> - (Optional) Enter the list of ports used for this configuration here.
If no parameter is specified, the system will display current LACP and all port status.

Restrictions

None.

Example

To show the LACP mode of the ports:

```
DGS-3000-28XMP:admin#show lacp_port
Command: show lacp_port


 Port     Activity

 -----    --------
 1        Active
 2        Active
 3        Active
 4        Active
 5        Active
 6        Active
 7        Active
 8        Active
 9        Active
 10       Active
 11       Active
 12       Active
 13       Passive
 14       Passive
 15       Passive
 16       Passive
 17       Passive
 18       Passive
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

Chapter 46 Link Layer Discovery Protocol (LLDP) Command List

enable lldp
disable lldp
config lldp [message_tx_interval <sec 5-32768> | message_tx_hold_multiplier <int 2-10> | tx_delay <sec 1-8192> | reinit_delay <sec 1-10>]
config lldp notification_interval <sec 5-3600>
config lldp ports [<portlist> | all] [notification [enable | disable] | admin_status [tx_only | rx_only | tx_and_rx | disable] | mgt_addr [ipv4 <ipaddr> | ipv6 <ipv6addr>] [enable | disable] | basic_tlvs [{all} | {port_description | system_name | system_description | system_capabilities}] [enable | disable] | dot1_tlv_pvid [enable | disable] | dot1_tlv_protocol_vid [vlan [all | <vlan_name 32>] | vlanid <vidlist>] [enable | disable] | dot1_tlv_vlan_name [vlan [all | <vlan_name 32>] | vlanid <vidlist>] [enable | disable] | dot1_tlv_protocol_identity [all | {eapol | lacp | gvrp | stp}] [enable | disable] | dot3_tlvs [{all} | {mac_phy_configuration_status | link_aggregation | power_via_mdi | maximum_frame_size}] [enable | disable]]
config lldp forward_message [enable | disable]
show lldp
show lldp mgt_addr {[ipv4 <ipaddr> | ipv6 <ipv6addr>]}
show lldp ports {<portlist>}
show lldp local_ports {<portlist>} {mode [brief | normal | detailed]}
show lldp remote_ports {<portlist>} {mode [brief | normal | detailed]}
show lldp statistics
show lldp statistics ports {<portlist>}

46-1 enable lldp

Description

This command is used to globally enable the LLDP function.

When this function is enabled, the Switch can start to transmit LLDP packets and receive and process the LLDP packets. The specific function of each port will depend on the per-port LLDP setting.

For the advertisement of LLDP packets, the Switch announces the information to its neighbor through ports. For the receiving of LLDP packets, the Switch will learn the information from the LLDP packets advertised from the neighbor in the neighbor table. The default state for LLDP is disabled.

Format

enable lldp

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable LLDP:

```
DGS-3000-28XMP:admin# enable lldp
Command: enable lldp

Success.

DGS-3000-28XMP:admin#
```

46-2 disable lldp

Description

This command is used to disable the sending and receiving of LLDP advertisement packets.

Format

disable lldp

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To disable LLDP:

```
DGS-3000-28XMP:admin# disable lldp
Command: disable lldp

Success.

DGS-3000-28XMP:admin#
```

46-3 config lldp

Description

This command is used to change the LLDP packet transmission interval.

Format

config lldp [message_tx_interval <sec 5-32768> | message_tx_hold_multiplier <int 2-10> | tx_delay <sec 1-8192> | reinit_delay <sec 1-10>]

Parameters

message_tx_interval - Specifies to change the interval between consecutive transmissions of LLDP

advertisements on any given port. The default value is 30 seconds.

<sec 5-32768> - Enter the message transmit interval value here. This value must be between 5 and 32768 seconds.

message_tx_hold_multiplier - Specifies to configure the message hold multiplier. The default value is 4.

<int 2-10> - Enter the message transmit hold multiplier value here. This value must be between 2 and 10.

tx_delay - Specifies the minimum interval between sending of LLDP messages due to constantly change of MIB content. The default value is 2 seconds.

<sec 1-8192> - Enter the transmit delay value here. This value must be between 1 and 8192 seconds.

reinit_delay - Specifies the minimum time of reinitialization delay interval. The default value is 2 seconds.

<sec 1-10> - Enter the re-initiate delay value here. This value must be between 1 and 10 seconds.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To change the packet transmission interval:

```
DGS-3000-28XMP:admin# config lldp message_tx_interval 30
Command: config lldp message_tx_interval 30

Success.

DGS-3000-28XMP:admin#
```

46-4 config lldp notification_interval

Description

This command is used to configure the interval timer for sending notifications to configured SNMP trap receiver(s).

Format

config lldp notification_interval <sec 5-3600>

Parameters

<sec 5-3600> - Enter the notification interval value here. This value must be between 5 and 3600 seconds. The default setting is 5 seconds.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To changes the notification interval to 10 second:

```
DGS-3000-28XMP:admin# config lldp notification_interval 10
Command: config lldp notification_interval 10

Success.

DGS-3000-28XMP:admin#
```

46-5 config lldp ports

Description

This command is used to configure each port for sending a notification to the configured the SNMP trap receiver(s).

Format

config lldp ports [<portlist> | all] [notification [enable | disable] | admin_status [tx_only | rx_only | tx_and_rx | disable] | mgt_addr [ipv4 <ipaddr> | ipv6 <ipv6addr>] [enable | disable] | basic_tlvs [{all} | {port_description | system_name | system_description | system_capabilities}] [enable | disable] | dot1_tlv_pvid [enable | disable] | dot1_tlv_protocol_vid [vlan [all | <vlan_name 32>] | vlanid <vidlist>] [enable | disable] | dot1_tlv_vlan_name [vlan [all | <vlan_name 32>] | vlanid <vidlist>] [enable | disable] | dot1_tlv_protocol_identity [all | {eapol | lacp | gvrp | stp}] [enable | disable] | dot3_tlvs [{all} | {mac_phy_configuration_status | link_aggregation | power_via_mdi | maximum_frame_size}] [enable | disable]]

Parameters

<portlist> - Enter a list of ports used for the configuration here.

all - Specifies that all the ports will be used for this configuration.

notification - Specifies to enable or disable the SNMP trap notification of LLDP data changes detected on advertisements received from neighbor devices.

- **enable** - Specifies that the SNMP trap notification of LLDP data changes detected will be enabled.
- **disable** - Specifies that the SNMP trap notification of LLDP data changes detected will be disabled. This is the default value.

admin_status - Specifies the per-port transmit and receive modes.

- **tx_only** - Specifies to transmit LLDP packets, but block inbound LLDP packets from neighbor devices.
- **rx_only** - Specifies to receive LLDP packets from neighbors, but block outbound packets to neighbors.
- **tx_and_rx** - Specifies to both transmit and receive LLDP packets.
- **disable** - Specifies to disable LLDP packet transmission and reception on the specified port(s).

mgt_addr - Specifies the management address used.

- **ipv4** - Specifies the IPv4 address used.
  - **<ipaddr>** - Enter the IP address used for this configuration here.
- **ipv6** - Specifies the IPv6 address used.
  - **<ipv6addr>** - Enter the IPv6 address used for this configuration here.
- **enable** - Specifies that the advertising indicated management address instance will be enabled.
- **disable** - Specifies that the advertising indicated management address instance will be disabled.

basic_tlvs - Specifies the basic TLV data types used from outbound LLDP advertisements.

- **all** - (Optional) Specifies that all the basic TLV data types will be used.
- **port_description** - (Optional) Specifies that the LLDP agent should transmit 'Port Description TLV on the port. The default state is disabled.
- **system_name** - (Optional) Specifies that the LLDP agent should transmit 'System Name TLV'. The default state is disabled.

system_description - (Optional) Specifies that the LLDP agent should transmit 'System Description TLV'. The default state is disabled.

system_capabilities - (Optional) Specifies that the LLDP agent should transmit 'System Capabilities TLV'. The system capability will indicate whether the device provides repeater, bridge, or router function, and whether the provided functions are currently enabled. The default state is disabled.

enable - Specifies that the basic TLV data types used from outbound LLDP advertisements will be enabled.

disable - Specifies that the basic TLV data types used from outbound LLDP advertisements will be disabled.

dot1_tlv_pvid - Specifies whether the IEEE 802.1 organizationally-defined port VLAN ID TLV transmission is allowed on a given LLDP transmission-capable port. The default state is disable.

enable - Specifies that the Dot1 TLV PVID option will be enabled.

disable - Specifies that the Dot1 TLV PVID option will be disabled.

dot1_tlv_protocol_vid - Specifies whether the IEEE 802.1 organizationally-defined port and protocol VLAN ID TLV transmission is allowed on a given LLDP transmission-capable port. The default state is disable.

vlan - Specifies the VLAN used for this configuration.

all - Specifies that all the configured VLANs will be used for this configuration.

<vlan_name 32> - Enter the name of the VLAN here. This name can be up to 32 characters long.

vlanid - Specifies the VLAN ID used for this configuration.

<vlanid_list> - Enter the ID of the VLAN here.

enable - Specifies that the Dot1 TLV protocol VID will be enabled.

disable - Specifies that the Dot1 TLV protocol VID will be disabled.

dot1_tlv_vlan_name - Specifies whether the corresponding Local System's VLAN name instance will be transmitted on the port. If a port is associated with multiple VLANs, only the enabled VLAN IDs will be advertised. The default state is disabled.

vlan - Specifies the VLAN used for this configuration.

all - Specifies that all the configured VLANs will be used for this configuration.

<vlan_name 32> - Enter the name of the VLAN here. This name can be up to 32 characters long.

vlanid - Specifies the VLAN ID used for this configuration.

<vlanid_list> - Enter the ID of the VLAN here.

enable - Specifies that the Dot1 TLV VLAN name will be enabled.

disable - Specifies that the Dot1 TLV VLAN name will be disabled.

dot1_tlv_protocol_identity - Specifies whether the corresponding Local System's Protocol Identity instance will be transmitted on the port. The Protocol Identity TLV provides a way for stations to advertise protocols that are important to the operation of the network. Such as Spanning Tree Protocol, the Link Aggregation Control Protocol, and numerous vendor proprietary variations are responsible for maintaining the topology and connectivity of the network. If EAPOL, GVRP, STP (including MSTP), and LACP protocol identity is enabled on this port and it is enabled to be advertised, then this protocol identity will be advertised. The default state is disabled.

all - Specifies that all the vendor proprietary protocols will be advertised.

eapol - (Optional) Specifies that the EAPOL protocol will be advertised.

lacp - (Optional) Specifies that the LACP protocol will be advertised.

gvrp - (Optional) Specifies that the GVRP protocol will be advertised.

stp - (Optional) Specifies that the STP protocol will be advertised.

enable - Specifies that the protocol identity TLV according to the protocol specified will be advertised.

disable - Specifies that the protocol identity TLV according to the protocol specified will not be advertised.

dot3_tlvs - Specifies that the IEEE 802.3 specific TLV data type will be configured.

all - (Optional) Specifies that all the IEEE 802.3 specific TLV data type will be used.

mac_phy_configuration_status - (Optional) Specifies that the LLDP agent should transmit 'MAC/PHY configuration/status TLV'. This type indicates it is possible for two ends of an IEEE 802.3 link to be configured with different duplex and/or speed settings and still establish some limited network connectivity. More precisely, the information includes whether the port supported the auto-negotiation function, whether the function is enabled, the auto-negotiated advertised capability, and the operational MAU type. The default state is disabled.

link_aggregation - (Optional) Specifies that the LLDP agent should transmit 'Link Aggregation TLV'. This type

indicates the current link aggregation status of IEEE 802.3 MACs. More precisely, the information should include whether the port is capable of doing link aggregation, whether the port is aggregated in an aggregated link, and the aggregated port ID. The default state is disabled.

power_via_mdi - (Optional) Specifies that the LLDP agent should transmit 'Power via MDI TLV'. Three IEEE 802.3 PMD implementations (10BASE-T, 100BASE-TX, and 1000BASE-T) allow power to be supplied over the link for connected non-powered systems. The Power Via MDI TLV allows network management to advertise and discover the MDI power support capabilities of the sending IEEE 802.3 LAN station. The default state is disabled.

maximum_frame_size - (Optional) Specifies that the LLDP agent should transmit 'Maximum-frame-size TLV. The default state is disabled.

enable - Specifies that the IEEE 802.3 specific TLV data type selected will be advertised.

disable - Specifies that the IEEE 802.3 specific TLV data type selected will be not advertised.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable SNMP notifications from port 1-5:

```
DGS-3000-28XMP:admin# config lldp ports 1-5 notification enable
Command: config lldp ports 1-5 notification enable

Success.

DGS-3000-28XMP:admin#
```

To configure port 1-5 to transmit and receive:

```
DGS-3000-28XMP:admin# config lldp ports 1-5 admin_status tx_and_rx
Command: config lldp ports 1-5 admin_status tx_and_rx

Success.

DGS-3000-28XMP:admin#
```

To enable ports 1-2 for manage address entry:

```
DGS-3000-28XMP:admin# config lldp ports 1-2 mgt_addr ipv4 10.90.90.90 enable
Command: config lldp ports 1-2 mgt_addr ipv4 10.90.90.90 enable

Success.

DGS-3000-28XMP:admin#
```

To exclude the system name TLV from the outbound LLDP advertisements for all ports:

```
DGS-3000-28XMP:admin# config lldp ports all basic_tlvs system_name enable
Command: config lldp ports all basic_tlvs system_name enable

Success.

DGS-3000-28XMP:admin#
```

To configure the IEEE 802.1 organizationally-defined port VLAN ID TLV transmission is allowed on all ports:

```
DGS-3000-28XMP:admin# config lldp ports all dot1_tlv_pvid enable
Command: config lldp ports all dot1_tlv_pvid enable

Success.

DGS-3000-28XMP:admin#
```

To exclude the port and protocol VLAN ID TLV from the outbound LLDP advertisements for all ports:

```
DGS-3000-28XMP:admin# config lldp ports all dot1_tlv_protocol_vid vlanid 1-3 enable
Command: config lldp ports all dot1_tlv_protocol_vid vlanid 1-3 enable

Success.

DGS-3000-28XMP:admin#
```

To exclude the VLAN name TLV from the outbound LLDP advertisements for all ports:

```
DGS-3000-28XMP:admin# config lldp ports all dot1_tlv_vlan_name vlanid 1-3 enable
Command: config lldp ports all dot1_tlv_vlan_name vlanid 1-3 enable

Success.

DGS-3000-28XMP:admin#
```

To exclude the protocol identity TLV from the outbound LLDP advertisements for all ports:

```
DGS-3000-28XMP:admin# config lldp ports all dot1_tlv_protocol_identity all enable
Command: config lldp ports all dot1_tlv_protocol_identity all enable

Success.

DGS-3000-28XMP:admin#
```

To exclude the MAC/PHY configuration/status TLV from the outbound LLDP advertisements for all ports:

```
DGS-3000-28XMP:admin# config lldp ports all dot3_tlvs mac_phy_configuration_status enable
Command: config lldp ports all dot3_tlvs mac_phy_configuration_status enable

Success.

DGS-3000-28XMP:admin#
```

46-6 config lldp forward_ message

Description

This command is used to configure forwarding of LLDP PDU packets when LLDP is disabled.

Format

config lldp forward_message [enable | disable]

Parameters

enable - Specifies to enable the forwarding of LLDP PDU packets when LLDP is disabled.
disable - Specifies to disable the forwarding of LLDP PDU packets when LLDP is disabled.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure LLDP to forward LLDP PDUs:

```
DGS-3000-28XMP:admin# config lldp forward_message  enable
Command: config lldp forward_message enable

Success.

DGS-3000-28XMP:admin#
```

46-7 show lldp

Description

This command is used to display the Switch’s general LLDP configuration status.

Format

show lldp

Parameters

None.

Restrictions

None.

Example

To display the LLDP system level configuration status:

```
DGS-3000-28XMP:admin#show lldp
Command: show lldp

LLDP System Information
    Chassis ID Subtype        : MAC Address
    Chassis ID                : F0-7D-68-15-10-00
    System Name               :
    System Description        : Gigabit Ethernet Switch
    System Capabilities       : Repeater, Bridge

LLDP Configurations
    LLDP Status               : Disabled
    LLDP Forward Status       : Disabled
    Message TX Interval       : 30
    Message TX Hold Multiplier: 4
    ReInit Delay              : 2
    TX Delay                  : 2
    Notification Interval     : 5

DGS-3000-28XMP:admin#
```

46-8 show lldp mgt_addr

Description

This command is used to display the LLDP management address information.

Format

show lldp mgt_addr {[ipv4 <ipaddr> | ipv6 <ipv6addr>]}

Parameters

ipv4 - (Optional) Specifies the IPv4 address to be displayed. **<ipaddr>** - Enter the IPv4 address used for this configuration here.
ipv6 - (Optional) Specifies the IPv6 address to be displayed. **<ipv6addr>** - Enter the IPv6 address used for this configuration here.

Restrictions

None.

Example

To display management address information:

```
DGS-3000-28XMP:admin# show lldp mgt_addr ipv4 10.90.90.90
Command: show lldp mgt_addr ipv4 10.90.90.90

Address 1 :
-----------------------------------------------
    Subtype                          : IPv4
    Address                          : 10.90.90.90
    IF Type                          : IfIndex
    OID                              : 1.3.6.1.4.1.171.10.113.8.1
    Advertising Ports                : 1-2,5

DGS-3000-28XMP:admin#
```

46-9 show lldp ports

Description

This command is used to display the LLDP per port configuration for advertisement options.

Format

show lldp ports {<portlist>}

Parameters

<portlist> - (Optional) Specifies a range of ports to be displayed.
If no parameter is specified, information for all the ports will be displayed.

Restrictions

None.

Example

To display the LLDP port 1 TLV option configuration:

```
DGS-3000-28XMP:admin# show lldp ports 1
Command: show lldp ports 1

Port ID                 : 1
------------------------------------------------------------------
Admin Status            : TX_and_RX
Notification Status     : Enabled
Advertised TLVs Option  :
    Port Description                                    Disabled
    System Name                                         Enabled
    System Description                                  Disabled
    System Capabilities                                 Disabled
    Enabled Management Address
        10.90.90.90
    Port VLAN ID                                        Enabled
    Enabled Port_and_Protocol_VLAN_ID
        1, 2, 3
    Enabled VLAN Name
        1-3
    Enabled Protocol_Identity
        (None)
    MAC/PHY Configuration/Status                        Disabled
    Power Via MDI                                       Disabled
    Link Aggregation                                    Disabled
    Maximum Frame Size                                  Disabled


DGS-3000-28XMP:admin#
```

46-10 show lldp local_ports

Description

This command is used to display the per-port information currently available for populating outbound LLDP advertisements.

Format

show lldp local_ports {<portlist>} {mode [brief | normal | detailed]}

Parameters

<portlist> - (Optional) Specifies a range of ports to be configured. If this is not specified, information for all ports will be displayed.

mode - (Optional) Specifies the display mode.

brief - Specifies to display the information in brief mode.

normal - Specifies to display the information in normal mode. This is the default display mode.

detailed - Specifies to display the information in detailed mode.

Restrictions

None.

Example

To display outbound LLDP advertisements for port 1 in detailed mode. Port description on the display should use the same value as ifDescr.

```
DGS-3000-28XMP:admin#show lldp local_ports 1 mode detailed
Command: show lldp local_ports 1 mode detailed


Port ID : 1
------------------------------------------------------------------------------
Port ID Subtype                           : MAC Address
Port ID                                   : F0-7D-68-15-10-01
Port Description                          : D-Link DGS-3000-28XMP R4.00.010
                                             Port 1
Port PVID                                 : 1
Management Address Count                  : 1
        Subtype                           : IPv4
        Address                           : 10.90.90.90
        IF Type                           : IfIndex
        OID                               : 1.3.6.1.4.1.171.10.133.11.2

PPVID Entries Count                       : 0
    (None)
VLAN Name Entries Count                   : 1
    Entry 1 :
        VLAN ID                           : 1
        VLAN Name                         : default

Protocol Identity Entries Count           : 0
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

To display outbound LLDP advertisements for port 1 in normal mode:

```
DGS-3000-28XMP:admin#show lldp local_ports 1 mode normal
Command: show lldp local_ports 1 mode normal


Port ID : 1
------------------------------------------------------------------------------
Port ID Subtype                          : MAC Address
Port ID                                  : F0-7D-68-15-10-01
Port Description                         : D-Link DGS-3000-28XMP R4.00.010
                                           Port 1
Port PVID                                : 1
Management Address Count                 : 1
PPVID Entries Count                      : 0
VLAN Name Entries Count                  : 1
Protocol Identity Entries Count          : 0
MAC/PHY Configuration/Status             : (See Detail)
Power Via MDI                            : (See Detail)
Link Aggregation                         : (See Detail)
Maximum Frame Size                       : 1536

DGS-3000-28XMP:admin#
```

To display outbound LLDP advertisements for port 1 in brief mode:

```
DGS-3000-28XMP:admin#show lldp local_ports 1 mode brief
Command: show lldp local_ports 1 mode brief


Port ID : 1
------------------------------------------------------------------------------
Port ID Subtype                          : MAC Address
Port ID                                  : F0-7D-68-15-10-01
Port Description                         : D-Link DGS-3000-28XMP R4.00.010
                                           Port 1

DGS-3000-28XMP:admin#
```

46-11 show lldp remote_ports

Description

This command is used to display the information learned from the neighbor parameters.

Format

show lldp remote_ports {<portlist>} {mode [brief | normal | detailed]}

Parameters

<portlist> - (Optional) Specifies a range of ports to be configured. If this is not specified, information for all ports will be displayed.
mode – (Optional) Specifies the display mode.

brief - Specifies to display the information in brief mode.
normal - Specifies to display the information in normal mode. This is the default display mode.
detailed - Specifies to display the information in detailed mode.

Restrictions

None.

Example

To display remote table in brief mode:

```
DGS-3000-28XMP:admin# show lldp remote_ports 3 mode brief
Command: show lldp remote_ports 3 mode brief

Port ID : 3
------------------------------------------------------------------------------
Remote Entities Count : 1
Entity 1
    Chassis ID Subtype                      : MAC Address
    Chassis ID                              : 00-12-13-04-05-00
    Port ID Subtype                         : MAC Address
    Port ID                                 : 00-12-13-04-05-03
    Port Description                        : D-Link DGS-3000-28XMP
                                              R4.00.010 Port 3

DGS-3000-28XMP:admin#
```

To display remote table in normal mode:

```
DGS-3000-28XMP:admin# show lldp remote_ports 3 mode normal
Command: show lldp remote_ports 3 mode normal

Port ID : 3
------------------------------------------------------------------------------
Remote Entities Count : 1
Entity 1
    Chassis ID Subtype                      : MAC Address
    Chassis ID                              : 00-12-13-04-05-00
    Port ID Subtype                         : MAC Address
    Port ID                                 : 00-12-13-04-05-03
    Port Description                        : D-Link DGS-3000-28XMP
                                              R4.00.010 Port 3
    System Name                             :
    System Description                      : Gigabit Ethernet Switch
    System Capabilities                     : Repeater, Bridge
    Management Address Count                : 1
    Port PVID                               : 1
    PPVID Entries Count                     : 0
    VLAN Name Entries Count                 : 0
    Protocol ID Entries Count               : 0
    MAC/PHY Configuration/Status            : (See Detail)
    Power Via MDI                           : (None)
    Link Aggregation                        : (See Detail)
    Maximum Frame Size                      : 1536
    Unknown TLVs Count                      : 0


DGS-3000-28XMP:admin#
```

To display remote table in detailed mode:

```
DGS-3000-28XMP:admin# show lldp remote_ports 3 mode detailed
Command: show lldp remote_ports 3 mode detailed

Port ID : 3
------------------------------------------------------------------------------
Remote Entities Count : 1
Entity 1
    Chassis ID Subtype                          : MAC Address
    Chassis ID                                  : 00-12-13-04-05-00
    Port ID Subtype                             : MAC Address
    Port ID                                     : 00-12-13-04-05-03
    Port Description                            : D-Link DGS-3000-28XMP
                                                  R4.00.010 Port 3
    System Name                                 :
    System Description                          : Gigabit Ethernet Switch
    System Capabilities                         : Repeater, Bridge
    Management Address Count                    : 1
        Entry 1 :
            Subtype                             : IPv4
            Address                             : 10.90.90.90
            IF Type                             : IfIndex
            OID                                 : 1.3.6.1.4.1.171.10.113.9.1

    Port PVID                                   : 1

    PPVID Entries Count                         : 0
        (None)

    VLAN Name Entries Count                     : 0
        (None)

    Protocol ID Entries Count                   : 0
        (None)

    MAC/PHY Configuration/Status                :
        Auto-Negotiation Support                : Supported
        Auto-Negotiation Status                 : Enabled
        Auto-Negotiation Advertised Capability  : 6c00(hex)
        Auto-Negotiation Operational MAU Type   : 0010(hex)

    Power Via MDI                               : (None)
    Link Aggregation                            :
        Aggregation Capability                  : Aggregated
        Aggregation Status                      : Not Currently in Aggregation
        Aggregation Port ID                     : 0

    Maximum Frame Size                          : 1536
    Unknown TLVs Count                          : 0
        (None)

DGS-3000-28XMP:admin#
```

46-12 show lldp statistics

Description

This command is used to display an overview of neighbor detection activity on the Switch.

Format

show lldp statistics

Parameters

None.

Restrictions

None.

Example

To display global statistics information:

```
DGS-3000-28XMP:admin# show lldp statistics
Command: show lldp statistics

Last Change Time       : 1792
Number of Table Insert : 0
Number of Table Delete : 0
Number of Table Drop   : 0
Number of Table Ageout : 0

DGS-3000-28XMP:admin#
```

46-13 show lldp statistics ports

Description

This command is used to display per-port LLDP statistics.

Format

show lldp statistics ports {<portlist>}

Parameters

<portlist> - (Optional) Specifies a range of ports to be configured.
If no parameter is specified, information for all ports will be displayed.

Restrictions

None.

Example

To display statistics information of port 1:

```
DGS-3000-28XMP:admin# show lldp statistics ports 1
Command: show lldp statistics ports 1

Port ID : 1
-----------------------------------------------
    LLDPStatsTXPortFramesTotal           : 23
    LLDPStatsRXPortFramesDiscardedTotal  : 0
    LLDPStatsRXPortFramesErrors          : 0
    LLDPStatsRXPortFramesTotal           : 0
    LLDPStatsRXPortTLVsDiscardedTotal    : 0
    LLDPStatsRXPortTLVsUnrecognizedTotal : 0
    LLDPStatsRXPortAgeoutsTotal          : 0

DGS-3000-28XMP:admin#
```

Chapter 47 LLDP-MED Command List

config lldp_med fast_start repeat_count <value 1 - 10>
config lldp_med log state [enable | disable]
config lldp_med notification topo_change ports [<portlist> | all] state [enable | disable]
config lldp_med ports [<portlist> | all] med_transmit_capabilities [all | {capabilities | network_policy | power_pse | inventory}(1)] state [enable | disable]
show lldp_med ports {<portlist>}
show lldp_med
show lldp_med local_ports {<portlist>}
show lldp_med remote_ports {<portlist>}

47-1 config lldp_med fast_start repeat_count

Description

This command is used to configure the fast start repeat count. When an LLDP-MED Capabilities TLV is detected for an MSAP identifier not associated with an existing LLDP remote system MIB, the application layer shall start the fast start mechanism and set the 'medFastStart' timer to 'medFastStartRepeatCount' times 1.

Format

config lldp_med fast_start repeat_count <value 1 - 10>

Parameters

<value 1-10> - Enter a fast start repeat count value between 1 and 10. The default value is 4.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure a LLDP-MED fast start repeat count of 5:

```
DGS-3000-28XMP:admin#config lldp_med fast_start repeat_count 5
Command: config lldp_med fast_start repeat_count 5

Success.

DGS-3000-28XMP:admin#
```

47-2 config lldp_med log state

Description

This command is used to configure the log state of LLDP-MED events.

Format

config lldp_med log state [enable | disable]

Parameters

enable - Specifies to enable the log state for LLDP-MED events.
disable - Specifies to disable the log state for LLDP-MED events. The default is disabled.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable the log state of LLDP-MED events:

```
DGS-3000-28XMP:admin#config lldp_med log state enable
Command: config lldp_med log state enable

Success.

DGS-3000-28XMP:admin#
```

47-3 config lldp_med notification topo_change ports

Description

This command is used to enable or disable each port for sending topology change notification to configured SNMP trap receiver(s) if an endpoint device is removed or moved to another port.

Format

config lldp_med notification topo_change ports [<portlist> | all] state [enable | disable]

Parameters

<portlist> - Enter a range of ports to be configured.
all - Specifies to set all ports in the system.
state - Specifies to enable or disable the SNMP trap notification of topology change detected state. **enable** - Specifies to enable the SNMP trap notification of topology change detected. **disable** - Specifies to disable the SNMP trap notification of topology change detected. The default notification state is disabled.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable topology change notification on ports 1 to 2:

```
DGS-3000-28XMP:admin#config lldp_med notification topo_change ports 1-2 state enable
Command: config lldp_med notification topo_change ports 1-2 state enable

Success.

DGS-3000-28XMP:admin#
```

47-4 config lldp_med ports

Description

This command is used to enable or disable transmitting LLDP-MED TLVs. It effectively disables LLDP-MED on a per-port basis by disabling transmission of TLV capabilities. In this case, the remote table's objects in the LLDP-MED MIB corresponding to the respective port will not be populated.

Format

config lldp_med ports [<portlist> | all] med_transmit_capabilities [all | {capabilities | network_policy | power_pse | inventory}(1)] state [enable | disable]

Parameters

<portlist> - Enter a range of ports to be configured.

all - Specifies to set all ports in the system.

med_transit_capabilities - Specifies to send the LLDP-MED TLV capabilities specified.

- **all** - Specifies to send capabilities, network policy, and inventory.
- **capabilities** - Specifies that the LLDP agent should transmit "LLDP-MED capabilities TLV." If a user wants to transmit LLDP-MED PDU, this TLV type should be enabled. Otherwise, this port cannot transmit LLDP-MED PDU.
- **network_policy** - Specifies that the LLDP agent should transmit "LLDP-MED network policy TLV."
- **power_pse** - Specifies that the LLDP agent should transmit 'LLDP-MED extended Power via MDI TLV' if the local device is a PSE device.
- **inventory** - Specifies that the LLDP agent should transmit "LLDP-MED inventory TLV."

state - Specifies to enable or disable the transmitting of LLDP-MED TLVs.

- **enable** - Specifies to enable the transmitting of LLDP-MED TLVs.
- **disable** - Specifies to disable the transmitting of LLDP-MED TLVs.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable transmitting all capabilities on all ports:

```
DGS-3000-28XMP:admin#config lldp_med ports all med_transmit_capabilities all state enable
Command: config lldp_med ports all med_transmit_capabilities all state enable

Success.

DGS-3000-28XMP:admin#
```

47-5 show lldp_med ports

Description

This command is used to display LLDP-MED per port configuration for advertisement options.

Format

show lldp_med ports {<portlist>}

Parameters

<portlist> - (Optional) Enter a range of ports to be displayed.
If a port list is not specified, information for all ports will be displayed.

Restrictions

None.

Example

To display LLDP-MED configuration information for port 1:

```
DGS-3000-28XMP:admin#show lldp_med ports 1
Command: show lldp_med ports 1

Port ID                : 1
----------------------------------------------------------------
Topology Change Notification Status              :Enabled
LLDP-MED Capabilities TLV                        :Enabled
LLDP-MED Extended Power Via MDI PSE TLV          :Enabled
LLDP-MED Inventory TLV                           :Enabled


DGS-3000-28XMP:admin#
```

47-6 show lldp_med

Description

This command is used to display the Switch’s general LLDP-MED configuration status.

Format

show lldp_med

Parameters

None.

Restrictions

None.

Example

To display the Switch's general LLDP-MED configuration status:

```
DGS-3000-28XMP:admin#show lldp_med
Command: show lldp_med

LLDP-MED System Information:
    Device Class              : Network Connectivity Device
    Hardware Revision         : B1
    Firmware Revision         : 4.00.001
    Software Revision         : 4.00.010
    Serial Number             : DGS-3000-28XMP
    Manufacturer Name         : D-Link
    Model Name                : DGS-3000-28XMP Gigabit Ethernet
    Asset ID                  :
    PoE Device Type           : PSE Device
    PoE PSE Power Source      : Primary

LLDP-MED Configuration:
    Fast Start Repeat Count   : 4

LLDP-MED Log State:Disabled

DGS-3000-28XMP:admin#
```

47-7 show lldp_med local_ports

Description

This command is used to display the per-port LLDP-MED information currently available for populating outbound LLDP-MED advertisements.

Format

show lldp_med local_ports {<portlist>}

Parameters

<portlist> - (Optional) Enter a range of ports to be displayed.

Restrictions

None.

Example

To display LLDP-MED information currently available for populating outbound LLDP-MED advertisements for port 1:

```
DGS-3000-28XMP:admin#show lldp_med local_ports 1
Command: show lldp_med local_ports 1


Port ID                 : 1
----------------------------------------------------------------
LLDP-MED Capabilities Support:
    Capabilities               :Support
    Network Policy             :Not Support
    Location Identification    :Not Support
    Extended Power Via MDI PSE :Support
    Extended Power Via MDI PD  :Not Support
    Inventory                  :Support

Extended Power Via MDI:
    Power Priority             :Low
    Power Value                :162

DGS-3000-28XMP:admin#
```

47-8 show lldp_med remote_ports

Description

This command is used to display LLDP-MED information learned from neighbors.

Format

show lldp_med remote_ports {<portlist>}

Parameters

<portlist> - (Optional) Enter a range of ports to be displayed.

Restrictions

None.

Example

To display remote entry information:

```
DGS-3000-28XMP:admin#show lldp_med remote_ports  1
Command: show lldp_med remote_ports 1

Port ID : 1
------------------------------------------------------------------------------
Remote Entities Count : 1
Entity 1
   Chassis ID Subtype                        : MAC Address
   Chassis ID                                : 00-01-02-03-04-00
   Port ID Subtype                           : Net Address
   Port ID                                   : 172.18.10.11

   LLDP-MED capabilities:
       LLDP-MED Device Class: Endpoint Device Class III
       LLDP-MED Capabilities Support:
           Capabilities                      : Support
           Network Policy                    : Support
           Location Identification           : Support
           Extended Power Via MDI            : Support
           Inventory                         : Support
       LLDP-MED Capabilities Enabled:
          Capabilities                       : Enabled
          Network Policy                     : Enabled
          Location Identification            : Enabled
          Extended Power Via MDI             : Enabled
          Inventory                          : Enabled

   Network Policy:
      Application Type : Voice
         VLAN ID                             :
         Priority                            :
         DSCP                                :
         Unknown                             : True
         Tagged                              :
    Application Type : Softphone Voice
         VLAN ID                             : 200
         Priority                            : 7
         DSCP                                : 5
         Unknown                             : False
         Tagged                              : True

      Location Identification:
         Location Subtype: CoordinateBased
            Location Information             :
         Location Subtype: CivicAddress
            Location Information             :

Extended Power Via MDI
     Power Device Type: PD Device

           Power Priority                    : High
           Power Source                      : From PSE
           Power Request                     : 8 Watts

  Inventory Management:
```

```
     Hardware Revision                 :
     Firmware Revision                 :
     Software Revision                 :
     Serial Number                     :
     Manufacturer Name                 :
     Model Name                        :
     Asset ID                          :

DGS-3000-28XMP:admin#
```

Chapter 48 Loop Back Detection (LBD) Command List

config loopdetect {recover_timer [<value 0> | <sec 60-1000000>] | interval <sec 1-32767> | mode [port-based | vlan-based]}
config loopdetect ports [<portlist> | all] state [enable | disable]
enable loopdetect
disable loopdetect
show loopdetect
show loopdetect ports {<portlist>}
config loopdetect trap [none | loop_detected | loop_cleared | both]
config loopdetect log state [enable | disable]

48-1 config loopdetect

Description

This command is used to setup the loop-back detection function (LBD) for the entire Switch.

Format

config loopdetect {recover_timer [<value 0> | <sec 60-1000000>] | interval <sec 1-32767> | mode [port-based | vlan-based]}

Parameters

recover_timer - (Optional) Specifies the time interval, in seconds, used by the Auto-Recovery mechanism to decide how long to check before determining that the loop status has gone. The valid range is from 60 to 1000000. The default value is 60 seconds.

<value 0> - Enter 0 to disable the auto-recovery mechanism. When the auto-recovery mechanism is disabled, a user would need to manually recover a disabled port.

<sec 60-1000000> - Enter the recovery timer value here. This value must be between 60 and 1000000 seconds.

interval - (Optional) Specifies the time interval, in seconds, that the device will transmit all the CTP (Configuration Test Protocol) packets to detect a loop-back event. The default value is 10 seconds.

<sec - 1-32767> - Enter the time interval value here. This value must be between 1 and 32767 seconds.

mode - (Optional) Specifies the loop-detection operation mode. In port-based mode, the port will be shut down (disabled) when loop has been detected In VLAN-based mode, the port cannot process the packets of the VLAN that has detected the loop.

port-based - Specifies that the loop-detection operation mode will be set to port-based mode.

vlan-based - Specifies that the loop-detection operation mode will be set to VLAN-based mode.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To set the auto-recover time to 0, which disables the auto-recovery mechanism, the interval to 20 seconds and specify VLAN-based mode:

```
DGS-3000-28XMP:admin# config loopdetect recover_timer 0 interval 20 mode vlan-based
Command: config loopdetect recover_timer 0 interval 20 mode vlan-based

Success.

DGS-3000-28XMP:admin#
```

48-2 config loopdetect ports

Description

This command is used to setup the loop-back detection function for the interfaces on the Switch.

Format

config loopdetect ports [<portlist> | all] state [enable | disable]

Parameters

<portlist> - Enter a list of ports
all - Specifies to configure all ports in the system, you may use the “all” parameter.
state - Specifies whether the LBD function should be enabled or disabled on the ports specified in the port list. The default state is disabled. **enable** - Specifies to enable the LBD function. **disable** - Specifies to disable the LBD function.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable the LBD function on ports 1-5:

```
DGS-3000-28XMP:admin# config loopdetect ports 1-5 state enable
Command: config loopdetect ports 1-5 state enable

Success.

DGS-3000-28XMP:admin#
```

48-3 enable loopdetect

Description

This command is used to enable the LBD function globally on the Switch. The default state is disabled.

Format

enable loopdetect

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable the LBD function globally:

```
DGS-3000-28XMP:admin# enable loopdetect
Command: enable loopdetect

Success.

DGS-3000-28XMP:admin#
```

48-4 disable loopdetect

Description

This command is used to disable the LBD function globally on the Switch.

Format

disable loopdetect

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To disable the LBD function globally:

```
DGS-3000-28XMP:admin# disable loopdetect
Command: disable loopdetect

Success.

DGS-3000-28XMP:admin#
```

48-5 show loopdetect

Description

This command is used to display the LBD global configuration.

Format

show loopdetect

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To show the LBD global settings:

```
DGS-3000-28XMP:admin# show loopdetect
Command: show loopdetect

 LBD Global Settings
 ---------------------------
 Status         : Disabled
 Mode           : Port-based
 Interval       : 10 sec
 Recover Time   : 60 sec
 Trap State     : None
 Log State      : Enabled

DGS-3000-28XMP:admin#
```

48-6 show loopdetect ports

Description

This command is used to display the LBD per-port configuration.

Format

show loopdetect ports {<portlist>}

Parameters

<portlist> - Enter the list of ports to be displayed.
If no parameter is specified, the configuration for all ports will be displayed.

Restrictions

None.

Example

To show the LBD settings on ports 1-9:

```
DGS-3000-28XMP:admin# show loopdetect  ports 1-9
Command: show loopdetect  ports 1-9

Port   Loopdetect State    Loop Status
------ ------------------ ----------
1      Enabled            Normal
2      Enabled            Normal
3      Enabled            Normal
4      Enabled            Normal
5      Enabled            Loop!
6      Enabled            Normal
7      Enabled            Loop!
8      Enabled            Normal
9      Enabled            Normal

DGS-3000-28XMP:admin#
```

48-7 config loopdetect trap

Description

This command is used to configure the trap modes for LBD.

Format

config loopdetect trap [none | loop_detected | loop_cleared | both]

Parameters

none - Specifies that there is no trap in the LBD function.
loop_detected - Specifies that the trap will only be sent when the loop condition is detected.
loop_cleared - Specifies that the trap will only be sent when the loop condition is cleared.
both - Specifies that the trap will either be sent when the loop condition is detected or cleared.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To specify that traps will be sent when the loop condition is detected or cleared:

```
DGS-3000-28XMP:admin# config loopdetect trap both
Command: config loopdetect trap both

Success.

DGS-3000-28XMP:admin#
```

48-8 config loopdetect log

Description

This command is used to configure the log state for LBD. The default value is enabled.

Format

config loopdetect log state [enable | disable]

Parameters

enable - Specifies to enable the LBD log feature.
disable - Specifies to disable the LBD log feature. All LBD-related logs will not be recorded.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable the log state for LBD:

```
DGS-3000-28XMP:admin# config loopdetect log state enable
Command: config loopdetect log state enable

Success.

DGS-3000-28XMP:admin#
```

Chapter 49 MAC Notification Command List

enable mac_notification
disable mac_notification
config mac_notification {interval <sec 1-2147483647> | historysize <int 1-500>}
config mac_notification ports [<portlist> | all] [enable | disable]
show mac_notification
show mac_notification ports {<portlist>}

49-1 enable mac_notification

Description

This command is used to enable global MAC address table notification on the Switch.

Format

enable mac_notification

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable MAC notification function:

```
DGS-3000-28XMP:admin# enable mac_notification
Command: enable mac_notification

Success.

DGS-3000-28XMP:admin#
```

49-2 disable mac_notification

Description

This command is used to disable global MAC address table notification on the Switch.

Format

disable mac_notification

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To disable MAC notification function:

```
DGS-3000-28XMP:admin# disable mac_notification
Command: disable mac_notification

Success.

DGS-3000-28XMP:admin#
```

49-3 config mac_notification

Description

This command is used to configure the Switch's MAC address table notification global settings.

Format

config mac_notification {interval <sec 1-2147483647> | historysize <int 1-500>}

Parameters

interval - (Optional) Specifies the time in seconds between notifications.	
	<sec 1-2147483647> - Enter the interval time here. This value must be between 1 and 2147483647 seconds.
historysize - (Optional) Specifies the maximum number of entries listed in the history log used for notification. Up to 500 entries can be specified.	
	<int 1-500> - Enter the history log size here. This value must be between 1 and 500.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

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

```
DGS-3000-28XMP:admin# config mac_notification interval 1 historysize 500
Command: config mac_notification interval 1 historysize 500

Success.

DGS-3000-28XMP:admin#
```

49-4 config mac_notification ports

Description

This command is used to configure the port's MAC address table notification status settings.

Format

config mac_notification ports [<portlist> | all] [enable | disable]

Parameters

<portlist> - Enter a list of ports used for the configuration here.
all - Specifies that all the ports will be used for this configuration.
enable - Specifies to enable the port's MAC address table notification.
disable - Specifies to disable the port's MAC address table notification.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable the MAC address table notification on port 7:

```
DGS-3000-28XMP:admin# config mac_notification ports 7 enable
Command: config mac_notification ports 7 enable

Success.

DGS-3000-28XMP:admin#
```

49-5 show mac_notification

Description

This command is used to display the Switch's MAC address table notification global settings.

Format

show mac_notification

Parameters

None.

Restrictions

None.

Example

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

```
DGS-3000-28XMP:admin# show mac_notification
Command: show mac_notification

Global MAC Notification Settings

State        : Disabled
Interval     : 1
History Size : 1

DGS-3000-28XMP:admin#
```

49-6 show mac_notification ports

Description

This command is used to display the port's MAC address table notification status settings.

Format

show mac_notification ports {<portlist>}

Parameters

<portlist> - (Optional) Enter a list of ports used for the configuration here.

Restrictions

None.

Example

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

```
DGS-3000-28XMP:admin# show mac_notification ports
Command: show mac_notification ports

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

Chapter 50 MAC-based Access Control Command List

enable mac_based_access_control
disable mac_based_access_control
config mac_based_access_control password <passwd 16>
config mac_based_access_control method [local | radius]
config mac_based_access_control guest_vlan ports <portlist>
config mac_based_access_control ports [<portlist> | all] {state [enable | disable] | mode [port_based | host_based] | aging_time [infinite | <min 1-1440>] | block_time <sec 0-300> | max_users [<value 1-1000> | no_limit]}(1)
create mac_based_access_control [guest_vlan <vlan_name 32> | guest_vlanid <vlanid 1-4094>]
delete mac_based_access_control [guest_vlan <vlan_name 32> | guest_vlanid <vlanid 1-4094>]
clear mac_based_access_control auth_state [ports [all | <portlist>] | mac_addr <macaddr>]
create mac_based_access_control_local mac <macaddr> {[vlan <vlan_name 32> | vlanid <vlanid 1-4094>]}
config mac_based_access_control_local mac <macaddr> [vlan <vlan_name 32> | vlanid <vlanid 1-4094> | clear_vlan]
delete mac_based_access_control_local [mac <macaddr> | vlan <vlan_name 32> | vlanid <vlanid 1-4094>]
config mac_based_access_control authorization attributes {radius [enable | disable] | local [enable | disable]}(1)
show mac_based_access_control {ports {<portlist>}}
show mac_based_access_control_local {[mac <macaddr> | vlan <vlan_name 32> | vlanid <vlanid 1-4094>]}
show mac_based_access_control auth_state ports {<portlist>}
config mac_based_access_control max_users [<value 1-1000> | no_limit]
config mac_based_access_control trap state [enable | disable]
config mac_based_access_control log state [enable | disable]

50-1 enable mac_based_access_control

Description

This command is used to enable MAC-based Access Control.

Format

enable mac_based_access_control

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable the MAC-based Access Control global state:

```
DGS-3000-28XMP:admin# enable mac_based_access_control
Command: enable mac_based_access_control

Success.

DGS-3000-28XMP:admin#
```

50-2 disable mac_based_access_control

Description

This command is used to disable MAC-based Access Control.

Format

disable mac_based_access_control

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To disable the MAC-based Access Control global state:

```
DGS-3000-28XMP:admin# disable mac_based_access_control
Command: disable mac_based_access_control

Success.

DGS-3000-28XMP:admin#
```

50-3 config mac_based_access_control password

Description

This command is used to configure the RADIUS authentication password for MAC-based Access Control.

Format

config mac_based_access_control password <passwd 16>

Parameters

<password> - Enter the password used here. The maximum length of the key is 16. The default password is "default".

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To set the MAC-based Access Control password:

```
DGS-3000-28XMP:admin# config mac_based_access_control password switch
Command: config mac_based_access_control password switch

Success.

DGS-3000-28XMP:admin#
```

50-4 config mac_based_access_control method

Description

This command is used to configure the MAC-based Access Control authentication method.

Format

config mac_based_access_control method [local | radius]

Parameters

local - Specifies to authenticate via the local database.
radius - Specifies to authenticate via a RADIUS server.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To set the MAC-based Access Control authentication method as local:

```
DGS-3000-28XMP:admin# config mac_based_access_control method local
Command: config mac_based_access_control method local

Success.

DGS-3000-28XMP:admin#
```

50-5 config mac_based_access_control guest_vlan ports

Description

This command is used to assign a specified port list to the MAC-based Access Control guest VLAN. Ports that are not contained in port list will be removed from the MAC-based Access Control guest VLAN.

For detailed information on the operation of MAC-based Access Control guest VLANs, refer to the description for the **config mac_based_access_control ports** command.

Format

config mac_based_access_control guest_vlan ports <portlist>

Parameters

<portlist> - Enter a list of ports to be configured.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To set the MAC-based Access Control guest VLAN membership:

```
DGS-3000-28XMP:admin# config mac_based_access_control guest_vlan ports 1-8
Command: config mac_based_access_control guest_vlan ports 1-8

Success.

DGS-3000-28XMP:admin#
```

50-6 config mac_based_access_control ports

Description

This command is used to configure MAC-based Access Control port's setting.

When the MAC-based Access Control function is enabled for a port and the port is not a MAC-based Access Control guest VLAN member, the user who is attached to this port will not be forwarded unless the user passes the authentication.

- A user that does not pass the authentication will not be serviced by the Switch.
- If the user passes the authentication, the user will be able to forward traffic operated under the assigned VLAN.

When the MAC-based Access Control function is enabled for a port, and the port is a MAC-based Access Control guest VLAN member, the port(s) will be removed from the original VLAN(s) member ports, and added to MAC-based Access Control guest VLAN member ports.

- Before the authentication process starts, the user is able to forward traffic under the guest VLAN.
- After the authentication process, the user will be able to access the assigned VLAN.

If the port authorize mode is port based mode, when the port has been moved to the authorized VLAN, the subsequent users will not be authenticated again. They will operate in the current authorized VLAN.

If the port authorize mode is host based mode, then each user will be authorized individually and be capable of getting its own assigned VLAN.

If port's block time is set to" infinite", it means that a failed authentication client will never be blocked. Block time will be set to "0".

Format

config mac_based_access_control ports [<portlist> | all] {state [enable | disable] | mode [port_based | host_based] | aging_time [infinite | <min 1-1440>] | block_time <sec 0-300> | max_users [<value 1-1000> | no_limit]}(1)

Parameters

<portlist> - Enter a list of ports to be configured.
all - Specifies all existed ports of switch for configuring the MAC-based Access Control function parameters.
state - Specifies whether the port's MAC-based Access Control function is enabled or disabled. **enable** - Specifies that the port's MAC-based Access Control states will be enabled. **disable** - Specifies that the port's MAC-based Access Control states will be disabled.
mode - Specifies the MAC-based access control port mode used. **port_based** - Specifies that the MAC-based access control port mode will be set to port-based. **host_based** - Specifies that the MAC-based access control port mode will be set to host-based.
aging_time - Specifies a time period during which an authenticated host will be kept in an authenticated state. When the aging time has timed-out, the host will be moved back to unauthenticated state. **infinite** - Specifies that the authorized clients will not be aged out automatically. **<min 1-1440>** - Enter the aging time value here. This value must be between 1 and 1440 minutes.
block_time - Specifies the block time. If a host fails to pass the authentication, the next authentication will not start within the block time unless the user clears the entry state manually. **<sec 0-300>** -Enter the block time value here. This value must be between 0 and 300 seconds. If the block time is set to 0, it means do not block the client that failed authentication.
max_users - Specifies maximum number of users per port. The default value is 128. **<value 1-1000>** - Enter the maximum number of users per port here. This value must be between 1 and 1000. **no_limit** - Specifies to not limit the maximum number of users on the port.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure an unlimited number of maximum users for MAC-based Access Control on ports 1 to 8:

```
DGS-3000-28XMP:admin# config mac_based_access_control ports 1-8 max_users no_limit
Command: config mac_based_access_control ports 1-8 max_users no_limit

Success.

DGS-3000-28XMP:admin#
```

To configure the MAC-based Access Control timer parameters to have an infinite aging time and a block time of 120 seconds on ports 1 to 8:

```
DGS-3000-28XMP:admin# config mac_based_access_control ports 1-8 aging_time infinite
block_time 120
Command: config mac_based_access_control ports 1-8 aging_time infinite block_time 120

Success.

DGS-3000-28XMP:admin#
```

50-7 create mac_based_access_control

Description

This command is used to assign a static 802.1Q VLAN as a MAC-based Access Control guest VLAN.

Format

create mac_based_access_control [guest_vlan <vlan_name 32> | guest_vlanid <vlanid 1-4094>]

Parameters

guest_vlan - Specifies MAC-based Access Control guest VLAN by name, it must be a static 1Q VLAN.	
	<vlan_name 32> - Enter the VLAN name here. This name can be up to 32 characters long.
guest_vlanid - Specifies MAC-based Access Control guest VLAN by VID, it must be a static 1Q VLAN.	
	<vlanid 1-4094> - Enter the VLAN ID here. This value must be between 1 and 4094.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To create a MAC-based Access Control guest VLAN:

```
DGS-3000-28XMP:admin# create mac_based_access_control guest_vlan VLAN8
Command: create mac_based_access_control guest_vlan VLAN8

Success.

DGS-3000-28XMP:admin#
```

50-8 delete mac_based_access_control

Description

This command is used to remove a MAC-based Access Control guest VLAN.

Format

delete mac_based_access_control [guest_vlan <vlan_name 32> | guest_vlanid <vlanid 1-4094>]

Parameters

guest_vlan - Specifies the name of the MAC-based Access Control's guest VLAN. **<vlan_name 32>** - Enter the VLAN name here. This name can be up to 32 characters long.
guest_vlanid - Specifies the VID of the MAC-based Access Control's guest VLAN. **<vlanid 1-4094>** - Enter the VLAN ID here. This value must be between 1 and 4094.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete the MAC-based Access Control guest VLAN called default:

```
DGS-3000-28XMP:admin# delete mac_based_access_control guest_vlan default
Command: delete mac_based_access_control guest_vlan default

Success.

DGS-3000-28XMP:admin#
```

50-9 clear mac_based_access_control auth_state

Description

This command is used to clear the authentication state of a user (or port). The port (or the user) will return to an un-authenticated state. All the timers associated with the port (or the user) will be reset.

Format

clear mac_based_access_control auth_state [ports [all | <portlist>] | mac_addr <macaddr>]

Parameters

ports - Specifies the port range to delete MAC addresses on them. **all** - Specifies all MAC-based Access Control enabled ports to delete MAC addresses. **<portlist>** - Enter the list of ports used for this configuration here.
mac_addr - Specifies to delete a specified host with this MAC address. **<macaddr>** - Enter the MAC address used here.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To clear MAC-based Access Control clients' authentication information for all ports:

```
DGS-3000-28XMP:admin# clear mac_based_access_control auth_state ports all
Command: clear mac_based_access_control auth_state ports all

Success.

DGS-3000-28XMP:admin#
```

To delete the MAC-based Access Control authentication information for the host that has a MAC address of 00-00-00-47-04-65:

```
DGS-3000-28XMP:admin# clear mac_based_access_control auth_state mac_addr 00-00-00-47-04-65
Command: clear mac_based_access_control auth_state mac_addr 00-00-00-47-04-65

Success.

DGS-3000-28XMP:admin#
```

50-10 create mac_based_access_control_local mac

Description

This command is used to create a MAC-based Access Control local database entry that will be used for authentication. This command can also specify the VLAN that an authorized host will be assigned to.

Format

create mac_based_access_control_local mac <macaddr> {[vlan <vlan_name 32> | vlanid <vlanid 1-4094>]}

Parameters

<macaddr> - Enter the MAC address that can pass local authentication.
vlan - (Optional) Specifies the target VLAN by using the VLAN name. When this host is authorized, it will be assigned to this VLAN. **<vlan_name 32>** - Enter the VLAN name here. This name can be up to 32 characters long.
vlanid - (Optional) Specifies the target VLAN by using the VID. When this host is authorized, it will be assigned to this VLAN if the target VLAN exists. **<vlanid 1-4094>** - Enter the VLAN ID here. This value must be between 1 and 4094.
If no vlanid or vlan parameter is specified, the target VLAN is not specified for this host.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To create one MAC-based Access Control local database entry for MAC address 00-00-00-00-00-01 and specify that the host will be assigned to the “default” VLAN after the host has been authorized:

```
DGS-3000-28XMP:admin# create mac_based_access_control_local mac 00-00-00-00-00-01 vlan
default
Command: create mac_based_access_control_local mac 00-00-00-00-00-01 vlan default

Success.

DGS-3000-28XMP:admin#
```

50-11 config mac_based_access_control_local mac

Description

This command is used to configure a MAC-based Access Control local database entry.

Format

config mac_based_access_control_local mac <macaddr> [vlan <vlan_name 32> | vlanid <vlanid 1-4094> | clear_vlan]

Parameters

<macaddr> - Enter the authenticated host's MAC address here.
vlan - Specifies the target VLAN by VLAN name. When this host is authorized, the host will be assigned to this VLAN. **<vlan_name 32>** - Enter the VLAN name here. This name can be up to 32 characters long.
vlanid - Specifies the target VLAN by VID. When this host is authorized, the host will be assigned to this VLAN if the target VLAN exists. **<vlanid 1-4094>** - Enter the VLAN ID here. This value must be between 1 and 4094.
clear_vlan - Specifies to clear the VLAN that is the target VLAN. When this host is authorized, it will not be assigned to the target VLAN.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the target VLAN "default" for the MAC-based Access Control local database entry 00-00-00-00-00-01:

```
DGS-3000-28XMP:admin# config mac_based_access_control_local mac 00-00-00-00-00-01 vlan
default
Command: config mac_based_access_control_local mac 00-00-00-00-00-01 vlan default

Success.

DGS-3000-28XMP:admin#
```

50-12 delete mac_based_access_control_local

Description

This command is used to delete a MAC-based Access Control local database entry.

Format

delete mac_based_access_control_local [mac <macaddr> | vlan <vlan_name 32> | vlanid <vlanid 1-4094>]

Parameters

mac - Specifies to delete local database entry by specific MAC address. **<macaddr>** - Enter the MAC address used here.
vlan - Specifies to delete local database entries by specific target VLAN name. **<vlan_name 32>** - Enter the VLAN name here. This name can be up to 32 characters long.
vlanid - Specifies to delete local database entries by specific target VLAN ID. **<vlanid 1-4094>** - Enter the VLAN ID here. This value must be between 1 and 4094.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete the MAC-based Access Control local database entry for MAC address 00-00-00-00-00-01:

```
DGS-3000-28XMP:admin# delete mac_based_access_control_local mac 00-00-00-00-00-01
Command: delete mac_based_access_control_local mac 00-00-00-00-00-01

Success.

DGS-3000-28XMP:admin#
```

To delete the MAC-based Access Control local database entry for the VLAN name VLAN3:

```
DGS-3000-28XMP:admin# delete mac_based_access_control_local vlan VLAN3
Command: delete mac_based_access_control_local vlan VLAN3

Success.

DGS-3000-28XMP:admin#
```

50-13 config mac_based_access_control authorization attributes

Description

This command is used to enable or disable the acceptation of an authorized configuration.

When authorization is enabled for MAC-based Access Controls with RADIUS authentication, the authorized attributes (for example VLAN, 802.1p default priority, and ACL) assigned by the RADUIS server will be accepted if the global authorization status is enabled.

When authorization is enabled for MAC-based Access Controls with local authentication, the authorized attributes assigned by the local database will be accepted.

Format

config mac_based_access_control authorization attributes {radius [enable | disable] | local [enable | disable]}(1)

Parameters

radius - Specifies to enable or disable the RADIUS attributes.

enable - Specifies to enable the RADIUS attributes. The authorized attributes (for example VLAN, 802.1p default priority, and ACL) assigned by the RADUIS server will be accepted if the global authorization status is enabled. The is the default option.

disable - Specifies to disable the RADIUS attributes.

local - Specifies to enable or disable the local attributes.

enable - Specifies to enable the local attributes. The authorized attributes assigned by the local database will be accepted if the global authorization status is enabled. The is the default option.

disable - Specifies to disable the local attributes.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

The following example will disable the configuration authorized from the local database:

```
DGS-3000-28XMP:admin# config mac_based_access_control authorization attributes local disable
Command: config mac_based_access_control authorization attributes local disable

Success.

DGS-3000-28XMP:admin#
```

50-14 show mac_based_access_control

Description

This command is used to display the MAC-based Access Control setting.

Format

show mac_based_access_control {ports {<portlist>}}

Parameters

ports – (Optional) Specifies to display the MAC-based Access Control settings for a specific port or range of ports.

<portlist> - (Optional) Enter a list of ports to be used for this configuration here.

If no parameter is specified, the global MAC-based Access Control settings will be displayed.

Restrictions

None.

Example

To show the MAC-based Access Control port configuration for ports 1 to 4:

```
DGS-3000-28XMP:admin# show mac_based_access_control ports 1-4
Command: show mac_based_access_control ports 1-4


Port    State     Aging Time   Block Time  Auth Mode    Max User
                    (min)        (sec)
-----  --------   ----------   ---------   ----------   --------
1      Disabled   1440         300         Host-based   128
2      Disabled   1440         300         Host-based   128
3      Disabled   1440         300         Host-based   128
4      Disabled   1440         300         Host-based   128

DGS-3000-28XMP:admin#
```

50-15 show mac_based_access_control_local

Description

This command is used to display the MAC-based Access Control local database entries.

Format

show mac_based_access_control_local {[mac <macaddr> | vlan <vlan_name 32> | vlanid <vlanid 1-4094>]}

Parameters

mac - (Optional) Specifies to display MAC-based Access Control local database entries for a specific MAC address.

<macaddr> - Enter the MAC address used here.

vlan - (Optional) Specifies to display MAC-based Access Control local database entries for a specific target VLAN name.

<vlan_name 32> - Enter the VLAN name here. This name can be up to 32 characters long.

vlanid - (Optional) Specifies to display MAC-based Access Control local database entries for a specific target VLAN ID.

<vlanid 1-4094> - Enter the VLAN ID here. This value must be between 1 and 4094.

If no parameter is specified, all of the MAC-based Access Control local database entries will be displayed.

Restrictions

None.

Example

To show MAC-based Access Control local database for the VLAN named default:

```
DGS-3000-28XMP:admin#show mac_based_access_control_local vlan default
Command: show mac_based_access_control_local vlan default

MAC Address        VID
-----------------  ----
00-11-22-33-44-55  1

Total Entries:1

DGS-3000-28XMP:admin#
```

50-16 show mac_based_access_control auth_state ports

Description

This command is used to display the MAC-based Access Control authentication status on the specified ports.

Format

show mac_based_access_control auth_state ports {<portlist>}

Parameters

<portlist> - (Optional) Enter the list of ports used for this configuration here.
If no parameter is specified, the MAC-based Access Control authentication status on all ports will be displayed.

Restrictions

None.

Example

To display the MAC-based Access Control authentication status on port 1-4:

```
DGS-3000-28XMP:admin# show mac_based_access_control auth_state ports 1-4
Command: show mac_based_access_control auth_state ports 1-4


 (P): Port-based

Port MAC Address          State          VID  Priority Aging Time/
                                                       Block Time
---- -------------------- -------------- ---- -------- ------------

Total Authenticating Hosts  : 0
Total Authenticated Hosts   : 0
Total Blocked Hosts         : 0


DGS-3000-28XMP:admin#
```

50-17 config mac_based_access_control max_users

Description

This command is used to configure the maximum number of authorized clients.

Format

config mac_based_access_control max_users [<value 1-1000> | no_limit]

Parameters

<value 1-1000> - Enter the maximum number of authorized clients on the whole device. This value must be between 1 and 1000.
no_limit - Specifies not to limit the maximum number of users on the system. This is the default option.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the maximum number of users of the MAC-based Access Control system supports to 128:

```
DGS-3000-28XMP:admin# config mac_based_access_control max_users 128
Command: config mac_based_access_control max_users 128

Success.

DGS-3000-28XMP:admin#
```

50-18 config mac_based_access_control trap state

Description

This command is used to enable or disable the sending of MAC-based Access Control traps.

Format

config mac_based_access_control trap state [enable | disable]

Parameters

enable - Specifies to enable the sending of MAC-based Access Control traps.
disable - Specifies to disable the sending of MAC-based Access Control traps.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable trap state of MAC-based Access Control:

```
DGS-3000-28XMP:admin# config mac_based_access_control trap state enable
Command: config mac_based_access_control trap state enable

Success.

DGS-3000-28XMP:admin#
```

50-19 config mac_based_access_control log state

Description

This command is used to enable or disable MAC-based Access Control logs.

Format

config mac_based_access_control log state [enable | disable]

Parameters

enable - Specifies to enable the log for MAC-based Access Control. The log of MAC-based Access Control will be generated.
disable - Specifies to disable the log for MAC-based Access Control.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To disable log state of MAC-based Access Control:

```
DGS-3000-28XMP:admin# config mac_based_access_control log state disable
Command: config mac_based_access_control log state disable

Success.

DGS-3000-28XMP:admin#
```

Chapter 51 MAC-based VLAN Command List

create mac_based_vlan mac_address <macaddr> [vlan <vlan_name 32> | vlanid <vlanid 1-4094>]
delete mac_based_vlan {mac_address <macaddr> [vlan <vlan_name 32> | vlanid <vlanid 1-4094>]}
show mac_based_vlan {mac_address <macaddr> | [vlan <vlan_name 32> | vlanid <vlanid 1-4094>]}

51-1 create mac_based_vlan mac_address

Description

This command is used to create a static MAC-based VLAN entry.

This command only needs to be supported by the model which supports MAC-based VLAN.

There is a global limitation of the maximum entries supported for the static MAC-based entry.

Format

create mac_based_vlan mac_address <macaddr> [vlan <vlan_name 32> | vlanid <vlanid 1-4094>]

Parameters

<macaddr> - Enter the MAC address here.
vlan - Specifies the VLAN to be associated with the MAC address. **<vlan_name 32>** - Enter the VLAN name here. This name can be up to 32 characters long.
vlanid - Specifies the VLAN by VLAN ID. **<vlanid 1-4094>** - Enter the VLAN ID here. This value must be between 1 and 4094.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To create a static MAC-based VLAN entry:

```
DGS-3000-28XMP:admin# create mac_based_vlan mac_address 00-11-22-33-44-55 vlanid 100
Command: create mac_based_vlan mac_address 00-11-22-33-44-55 vlanid 100

Success.

DGS-3000-28XMP:admin#
```

51-2 delete mac_based_vlan

Description

This command is used to delete the static MAC-based VLAN entry.

Format

delete mac_based_vlan {mac_address <macaddr> [vlan <vlan_name 32> | vlanid <vlanid 1-4094>]}

Parameters

mac_address - (Optional) Specifies the MAC address used. **<macaddr>** - Enter the MAC address used here.
vlan - (Optional) Specifies the VLAN to be associated with the MAC address. **<vlan_name 32>** - Enter the VLAN name here. This name can be up to 32 characters long.
vlanid - (Optional) Specifies the VLAN by VLAN ID. **<vlanid 1-4094>** - Enter the VLAN ID here. This value must be between 1 and 4094.
If no parameter is specified, all of the static entries will be removed.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete a static MAC-based VLAN entry:

```
DGS-3000-28XMP:admin# delete mac_based_vlan mac_address 00-11-22-33-44-55 vlanid 100
Command: delete mac_based_vlan mac_address 00-11-22-33-44-55 vlanid 100

Success.

DGS-3000-28XMP:admin#
```

51-3 show mac_based_vlan

Description

This command is used to display the static or dynamic MAC-Based VLAN entry.

Format

show mac_based_vlan {mac_address <macaddr> | [vlan <vlan_name 32> | vlanid <vlanid 1-4094>]}

Parameters

mac_address - (Optional) Specifies the entry that you would like to display. **<macaddr>** - Enter the MAC address used here.
vlan - (Optional) Specifies the VLAN that you would like to display. **<vlan_name 32>** - Enter the VLAN name here. This name can be up to 32 characters long.
vlanid - (Optional) Specifies the VLAN by VLAN ID. **<vlanid 1-4094>** - Enter the VLAN ID here. This value must be between 1 and 4094.
If no parameter is specified, all static and dynamic entries will be displayed.

Restrictions

None.

Example

In the following example, MAC address “00-80-c2-33-c3-45” is assigned to VLAN 300 by manual config. It is assigned to VLAN 400 by Voice VLAN. Since Voice VLAN has higher priority than manual configuration, the manual configured entry will become inactive. To display the MAC-based VLAN entry:

```
DGS-3000-28XMP:admin# show mac_based_vlan

    MAC Address       VLAN ID        Status        Type
-----------------     -------        --------      -------------------
00-80-e0-14-a7-57     200            Active        Static
00-80-c2-33-c3-45     300            Inactive      Static
00-80-c2-33-c3-45     400            Active        Voice VLAN

Total Entries : 3

DGS-3000-28XMP:admin#
```

Chapter 52 Mirror Command List

config mirror port <port> {[add | delete] source [ports <portlist> | vlan vlan_id <vid_list>] [rx|tx|both]}
enable mirror
disable mirror
show mirror

52-1 config mirror port

Description

This command is used to configure a mirror port and source port pair on the Switch. Traffic from any source port to a target port can be mirrored for real-time analysis. A logic analyzer or an RMON probe then can be attached to study the traffic crossing the source port in a completely unobtrusive manner. When mirroring port traffic, the target port must be configured in the same VLAN and operates at the same speed as the source port. If the target port is operating at a lower speed, the source port will be forced to drop its operating speed to match that of the target port. If the mirror source is a range of VLANs, only traffic received by the specified VLANs can be mirrored to the target port.

Format

config mirror port <port> {[add | delete] source [ports <portlist> | vlan vlan_id <vid_list>] [rx|tx|both]}

Parameters

<port> - Enter the port number that will receive the packets duplicated at the mirror port.
add - (Optional) Specifies the mirror entry to be added.
delete - (Optional) Specifies the mirror entry to be deleted.
source - (Optional) Specifies the source to be mirrored. **ports** - Specifies the port that will be mirrored. All packets entering and leaving the source port can be duplicated on the mirror port. **<portlist>** - Enter the list of ports to be configured here. **vlan vlan_id** - Specifies a range of VLAN ID to be configured as sources. All ingress packets with the specified VLAN ID will be mirrored. **<vid_list>** - Enter the list of VLANs to be configured here.
rx - (Optional) Specifies to allow the mirroring packets received (flowing into) the port or ports in the port list.
tx - (Optional) Specifies to allow the mirroring packets sent (flowing out of) the port or ports in the port list.
both - (Optional) Specifies to mirror all the packets received or sent by the port or ports in the port list.

Restrictions

Only Administrators and Operators can issue this command.

Example

To add the mirroring ports:

```
DGS-3000-28XMP:admin# config mirror port 3 add source ports 7-12 both
Command: config mirror port 3 add source ports 7-12 both

Success.

DGS-3000-28XMP:admin#
```

52-2 enable mirror

Description

This command is used to enable mirror function without having to modify the mirror session configuration.

Format

enable mirror

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable mirroring function:

```
DGS-3000-28XMP:admin# enable mirror
Command: enable mirror

Success.

DGS-3000-28XMP:admin#
```

52-3 disable mirror

Description

This command is used to disable mirror function without having to modify the mirror session configuration.

Format

disable mirror

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To disable mirroring function:

```
DGS-3000-28XMP:admin# disable mirror
Command: disable mirror

Success.

DGS-3000-28XMP:admin#
```

52-4 show mirror

Description

This command is used to display the current mirror function state and mirror session configuration on the Switch.

Format

show mirror

Parameters

None.

Restrictions

None.

Example

To display mirroring configuration:

```
DGS-3000-28XMP:admin# show mirror
Command: show mirror

Current Settings
Mirror Status: Enabled
Target Port  : 3
Mirrored Port
           RX: 7-12
           TX: 7-12

DGS-3000-28XMP:admin#
```

Chapter 53 MLD Snooping Command List

The Multicast Listener Discovery (MLD) is used by IPv6 routers to discover multicast listeners on a directly attached link, much as IGMP is used in IPv4. The protocol is embedded in ICMPv6 instead of using a separate protocol. MLDv1 is similar to IGMPv2 and MLDv2 similar to IGMPv3.

The Switch only supports IGMP and MLD snooping awareness. This means that multicast traffic forwarding is only based on L2 MAC addresses associated with the groups that the Switch has joined. The source IP address of the multicast traffic will be ignored.

config mld_snooping [vlan_name <vlan_name 32> | vlanid <vlanid_list> | all] {state [enable | disable] | fast_done [enable | disable] | report_suppression [enable | disable] | proxy_reporting {state [enable | disable] | source_ip <ipv6addr>}(1)}(1)
config mld_snooping querier [vlan_name <vlan_name 32> | vlanid <vlanid_list> | all] {query_interval <sec 1-65535> | max_response_time <sec 1-25> | robustness_variable <value 1-7> | last_listener_query_interval <sec 1-25> | state [enable | disable] | version <value 1-2>}(1)
config mld_snooping mrouter_ports [vlan <vlan_name 32> | vlanid <vlanid_list>] [add | delete] <portlist>
config mld_snooping mrouter_ports_forbidden [vlan <vlan_name 32> | vlanid <vlanid_list>] [add | delete] <portlist>
enable mld_snooping
disable mld_snooping
show mld_snooping {[vlan <vlan_name 32> | vlanid <vlanid_list>]}
show mld_snooping group {[vlan <vlan_name 32> | vlanid <vlanid_list> | ports <portlist>] {<ipv6addr>}} {data_driven}
show mld_snooping forwarding {[vlan <vlan_name 32> | vlanid <vlanid_list>]}
show mld_snooping mrouter_ports [vlan <vlan_name 32> | vlanid <vlanid_list> | all] {[static | dynamic | forbidden]}
create mld_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipv6addr>
delete mld_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipv6addr>
config mld_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipv6addr> [add | delete] <portlist>
show mld_snooping static_group {[vlan <vlan_name 32> | vlanid <vlanid_list>] <ipv6addr>}
config mld_snooping data_driven_learning [all | vlan_name <vlan_name> | vlanid <vlanid_list>] {state [enable | disable] | aged_out [enable | disable] | expiry_time <sec 1-65535>}(1)
config mld_snooping data_driven_learning max_learned_entry <value 1-1024>
clear mld_snooping data_driven_group [all | [vlan_name <vlan_name> | vlanid <vlanid_list>] [<ipv6addr>| all]]
show mld_snooping statistic counter [vlan <vlan_name> | vlanid <vlanid_list> | ports <portlist>]
clear mld_snooping statistics counter
config mld_snooping rate_limit [ports <portlist> | vlanid <vlanid_list>] [<value 1-1000> | no_limit]
show mld_snooping rate_limit [ports <portlist> | vlanid <vlanid_list>]
show mld_snooping host {[vlan <vlan_name 32>| vlanid <vlanid_list> | ports <portlist> | group <ipv6addr>]}

53-1 config mld_snooping

Description

This command is used to configure MLD snooping on the Switch.

Format

config mld_snooping [vlan_name <vlan_name 32> | vlanid <vlanid_list> | all] {state [enable | disable] | fast_done [enable | disable] | report_suppression [enable | disable] | proxy_reporting {state [enable | disable] | source_ip <ipv6addr>}(1)}(1)

Parameters

vlan_name - Specifies the name of the VLAN for which MLD snooping is to be configured.
- **<vlan_name 32>** - Enter the VLAN name here. The VLAN name can be up to 32 characters long.

vlanid - Specifies the ID of the VLAN for which MLD snooping is to be configured.
- **<vlanid_list>** - Enter the VLAN ID list here.

all - Specifies all VLANs for which MLD snooping is to be configured.

state - Specifies to enable or disable MLD snooping for the chosen VLAN.
- **enable** - Specifies to enable MLD snooping for the chosen VLAN.
- **disable** - Specifies to disable MLD snooping for the chosen VLAN.

fast_done - Specifies to enable or disable MLD snooping fast done function.
- **enable** - Specifies to enable the MLD snooping fast done function. If enable, the membership is immediately removed when the system receive the MLD leave message.
- **disable** - Specifies to disable the MLD snooping fast done function.

report_suppression - Specifies MLD snooping report suppression.
- **enable** - Specifies to enable the MLD snooping report suppression function.
- **disable** - Specifies to disable the MLD snooping report suppression function.

proxy_reporting - Specifies MLD proxy reporting.
- **state** - Specifies to enable or disable the proxy reporting.
  - **enable** - Specifies to enable the proxy reporting.
  - **disable** - Specifies to disable the proxy reporting.
- **source_ip** - Specifies the source IP of proxy reporting integrated report. Default value is zero IP.
  - **<ipv6addr>** - Enter the IPv6 address.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure MLD snooping:

```
DGS-3000-28XMP:admin# config mld_snooping vlan_name default state enable
Command: config mld_snooping vlan_name default state enable

Success.

DGS-3000-28XMP:admin#
```

53-2 config mld_snooping querier

Description

This command is used to configure the timer in seconds between general query transmissions, the maximum time in seconds to wait for reports from listeners, and the permitted packet loss that is guaranteed by MLD snooping.

Format

config mld_snooping querier [vlan_name <vlan_name 32> | vlanid <vlanid_list> | all] {query_interval <sec 1-65535> | max_response_time <sec 1-25> | robustness_variable <value 1-7> | last_listener_query_interval <sec 1-25> | state [enable | disable] | version <value 1-2>}(1)

Parameters

vlan_name - Specifies the name of the VLAN for which MLD snooping querier is to be configured.

<vlan_name 32> - Enter the VLAN name here. The VLAN name can be up to 32 characters long.

vlanid - Specifies the ID of the VLAN for which MLD snooping querier is to be configured.

<vlanid_list> - Enter the VLAN ID list here.

all - Specifies all VLANs for which MLD snooping querier is to be configured.

query_interval - Specifies the amount of time in seconds between general query transmissions. The default setting is 125 seconds.

<sec 1-65535> - Enter the query interval value here. This value must be between 1 and 65535 seconds.

max_reponse_time - Specifies the maximum time in seconds to wait for reports from listeners. The default setting is 10 seconds.

<sec 1-25> - Enter the maximum response time value here. This value must be between 1 and 25 seconds.

robustness_variable - Specifies to provide fine-tuning to allow for expected packet loss on a subnet. The value of the robustness variable is used in calculating the following MLD message intervals:

<value 1-7> - Enter the robustness variable value here. This value must be between 1 and 7.

- Group listener interval—Amount of time that must pass before a multicast router decides there are no more listeners of a group on a network. This interval is calculated as follows: (robustness variable * query interval) + (1 * query response interval).
- Other querier present interval—Amount of time that must pass before a multicast router decides that there is no longer another multicast router that is the querier. This interval is calculated as follows: (robustness variable * query interval) + (0.5 * query response interval).
- Last listener query count—Number of group-specific queries sent before the router assumes there are no local listeners of a group. The default number is the value of the robustness variable.
- By default, the robustness variable is set to 2. You might want to increase this value if you expect a subnet to be loosely.

last_listener_query_interval - Specifies the maximum amount of time between group-specific query messages, including those sent in response to done-group messages. You might lower this interval to reduce the amount of time it takes a router to detect the loss of the last listener of a group. The default setting is 1 second.

<sec 1-25> - Enter the last listener query interval value here. This value must be between 1 and 25 seconds.

state - Specifies the Switch as an MLD querier (sends MLD query packets) or a non-querier (does not send MLD query packets).

enable - Specifies to enable the MLD querier state.

disable - Specifies to disable the MLD querier state.

version - Specifies the version of MLD packet that will be sent by the Switch.

<value 1-2> - Enter the version number value here. This value must be between 1 and 2.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the MLD snooping querier:

```
DGS-3000-28XMP:admin# config mld_snooping querier vlan_name default query_interval 125 state
enable
Command: config mld_snooping querier vlan_name default query_interval 125 state enable

Success.

DGS-3000-28XMP:admin#
```

53-3 config mld_snooping router_ports

Description

This command is used to designate a range of ports as being connected to multicast-enabled routers. This will ensure that all packets with such a router as its destination will reach the multicast-enabled router, regardless of protocol, etc.

Format

config mld_snooping mrouter_ports [vlan <vlan_name 32> | vlanid <vlanid_list>] [add | delete] <portlist>

Parameters

vlan - Specifies the name of the VLAN on which the router port resides. **<vlan_name 32>** - Enter the VLAN name here. The VLAN name can be up to 32 characters long.
vlanid - Specifies the ID of the VLAN on which the router port resides. **<vlanid_list>** - Enter the VLAN ID list here.
add - Specifies to add the router ports.
delete - Specifies to delete the router ports.
<portlist> - Enter a range of ports to be configured.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To set up static router ports:

```
DGS-3000-28XMP:admin# config mld_snooping mrouter_ports vlan default add 1-10
Command: config mld_snooping mrouter_ports vlan default add 1-10

Success.

DGS-3000-28XMP:admin#
```

53-4 config mld_snooping router_ports_forbidden

Description

This command is used to designate a range of ports as being not connected to multicast-enabled routers. This ensures that the forbidden router port will not propagate routing packets out.

Format

config mld_snooping mrouter_ports_forbidden [vlan <vlan_name 32> | vlanid <vlanid_list>] [add | delete] <portlist>

Parameters

vlan - Specifies the name of the VLAN on which the forbidden router port resides. **<vlan_name 32>** - Enter the VLAN name here. The VLAN name can be up to 32 characters long.
vlanid - Specifies the ID of the VLAN on which the forbidden router port resides. **<vlanid_list>** - Enter the VLAN ID list here.
add - Specifies to add the forbidden router ports.
delete - Specifies to delete the forbidden router ports.
<portlist> - Enter a range of ports to be configured.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To set up port 11 as the forbidden router port of the default VLAN:

```
DGS-3000-28XMP:admin# config mld_snooping mrouter_ports_forbidden vlan default add 11
Command: config mld_snooping mrouter_ports_forbidden vlan default add 11

Success.

DGS-3000-28XMP:admin#
```

53-5 enable mld_snooping

Description

This command is used to enable MLD snooping on the Switch. When the Switch receives an MLD report packet from a port, this port will be learned as a member port of the multicast group that the port is reported, and the router will be a default member of this multicast group. The multicast packet destined for this multicast group will be forwarded to all the members of this multicast group.

Format

enable mld_snooping

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable MLD snooping on the Switch:

```
DGS-3000-28XMP:admin# enable mld_snooping
Command: enable mld_snooping

Success.

DGS-3000-28XMP:admin#
```

53-6 disable mld_snooping

Description

This command is used to disable MLD snooping on the Switch. This is the default option.

Format

disable mld_snooping

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To disable MLD snooping on the Switch:

```
DGS-3000-28XMP:admin# disable mld_snooping
Command: disable mld_snooping

Success.

DGS-3000-28XMP:admin#
```

53-7 show mld_snooping

Description

This command is used to display the current MLD snooping configuration on the Switch.

Format

show mld_snooping {[vlan <vlan_name 32> | vlanid <vlanid_list>]}

Parameters

vlan - (Optional) Specifies the name of the VLAN for which you want to view the MLD snooping configuration. **<vlan_name 32>** - Enter the VLAN name here. The VLAN name can be up to 32 characters long.
vlanid - (Optional) Specifies the ID of the VLAN for which you want to view the MLD snooping configuration. **<vlanid_list>** - Enter the VLAN ID list here.
If no parameter is specified, the system will display all current MLD snooping configurations.

Restrictions

None.

Example

To show MLD snooping:

```
DGS-3000-28XMP:admin#show mld_snooping
Command: show mld_snooping

 MLD Snooping Global State               : Enabled
 Data Driven Learning Max Entries        : 128

 VLAN Name                     : default
 Query Interval                : 125
 Max Response Time             : 10
 Robustness Value              : 2
 Last Listener Query Interval  : 1
 Querier State                 : Disabled
 Querier Role                  : Non-Querier
 Querier IP                    : ::
 Querier Expiry Time           : 0 secs
 State                         : Disabled
 Fast Done                     : Disabled
 Rate Limit                    : No Limitation
 Report Suppression            : Enabled
 Proxy Reporting               : Disabled
 Proxy Reporting Source IP     : ::
 Version                       : 2
 Data Driven Learning State    : Enabled
 Data Driven Learning Aged Out : Disabled
 Data Driven Group Expiry Time : 260

Total Entries: 1


DGS-3000-28XMP:admin#
```

53-8 show mld_snooping group

Description

This command is used to display the current MLD snooping group information on the Switch.

Format

show mld_snooping group {[vlan <vlan_name 32> | vlanid <vlanid_list> | ports <portlist>] {<ipv6addr>}} {data_driven}

Parameters

vlan - (Optional) Specifies the name of the VLAN for which you want to view MLD snooping group information. If VLAN and ports and IP address are not specified, the system will display all current MLD snooping group information. **<vlan_name 32>** - Enter the VLAN name here. The VLAN name can be up to 32 characters long.
vlanid - (Optional) Specifies the ID of the VLAN for which you want to view MLD snooping group information. **<vlanid_list>** - Enter the VLAN ID list here.
ports - (Optional) Specifies a list of ports for which you want to view MLD snooping group information. **<portlist>** - Enter the list of ports here.
<ipv6addr> - (Optional) Specifies the group IPv6 address for which you want to view MLD snooping group information.
data_driven - (Optional) Specifies to display the data driven groups.

Restrictions

None.

Example

To show an MLD snooping group when MLD v2 is supported:

The first two items mean that for ports 1-2 / port 3, the data from the FE1E::1 will be forwarded.

The third item means that for ports 4-5, the data from FE1E::2 will be forwarded.

The fourth item is a data-driven learned entry. The member port list is empty. The multicast packets will be forwarded to the router ports. If the router port list is empty, the packet will be dropped.

```
DGS-3000-28XMP:admin# show mld_snooping group
Command: show mld_snooping group

 Source/Group         : NULL/FF13::1
 VLAN Name/VID          : v103/103
 Member Ports                 : 6
 Router Ports                 : 8
 UP Time                      : 172
 Expiry Time                  : 89
 Filter Mode                  : EXCLUDE

 Source/Group          : NULL/FF13::2
 VLAN Name/VID             : v103/103
 Member Ports                 :
 Router Ports                 : 8
 UP Time                      : 6
 Expiry Time                  : 254
 Filter Mode                  : EXCLUDE

 Source/Group            : NULL/FF13::3
 VLAN Name/VID             : v103/103
 Member Ports                 :
 Router Ports                 : 8
 UP Time                      : 6
 Expiry Time                  : 254
 Filter Mode                  : EXCLUDE

 Source/Group            : NULL/FF13::4
 VLAN Name/VID                : v103/103
 Member Ports                 :
 Router Ports                 : 8
 UP Time                      : 17
 Expiry Time                  : 243
 Filter Mode                  : EXCLUDE

 Source/Group          : NULL/FF13::5
 VLAN Name/VID                : v103/103
 Member Ports                 :
 Router Ports                 : 8
 UP Time                      : 17
 Expiry Time                  : 243
 Filter Mode                  : EXCLUDE

Total Entries : 5

DGS-3000-28XMP:admin#
```

To show MLD snooping data driven groups:

```
DGS-3000-28XMP:admin# show mld_snooping group data_driven
Command: show mld_snooping group data_driven

 Source/Group             : NULL/FF13::1
 VLAN Name/VID                 : v103/103
 Member Ports                  :
 Router Ports                  : 8
 UP Time                       : 97
 Expiry Time                   : 163
 Filter Mode                   : EXCLUDE

 Total Entries: 1

DGS-3000-28XMP:admin#
```

53-9 show mld_snooping forwarding

Description

This command is used to display the Switch's current MLD snooping forwarding table. It provides an easy way for users to check the list of ports that the multicast group that comes from specific sources will be forwarded to. The packet comes from the source VLAN. They will be forwarded to the forwarding VLAN.

Format

show mld_snooping forwarding {[vlan <vlan_name 32> | vlanid <vlanid_list>]}

Parameters

vlan - (Optional) Specifies the name of the VLAN for which you want to view MLD snooping forwarding table information. **<vlan_name 32>** - Enter the VLAN name here. The VLAN name can be up to 32 characters long.
vlanid - (Optional) Specifies the ID of the VLAN for which you want to view MLD snooping forwarding table information. **<vlanid_list>** - Enter the VLAN ID list here.
If no parameter is specified, the system will display all current MLD snooping forwarding table entries of the Switch.

Restrictions

None.

Example

To show all MLD snooping forwarding entries located on the Switch.

```
DGS-3000-28XMP:admin# show mld_snooping forwarding
Command: show mld_snooping forwarding

VLAN Name      : default
Source IP      : *
Multicast Group: FE1E::1
Port Member    : 2,7

VLAN Name      : default
Source IP      : *
Multicast Group: FF1E::1
Port Member    : 5

Total Entries : 2

DGS-3000-28XMP:admin#
```

53-10 show mld_snooping mrouter_ports

Description

This command is used to display the currently configured router ports on the Switch.

Format

show mld_snooping mrouter_ports [vlan <vlan_name 32> | vlanid <vlanid_list> | all] {[static | dynamic | forbidden]}

Parameters

vlan - Specifies the name of the VLAN on which the router port resides. **<vlan_name 32>** - Enter the VLAN name here. The VLAN name can be up to 32 characters long.
vlanid - Specifies the ID of the VLAN on which the router port resides. **<vlanid_list>** - Enter the VLAN ID list here.
all - Specifies all VLANs on which the router port resides.
static - (Optional) Specifies to display router ports that have been statically configured.
dynamic - (Optional) Specifies to display router ports that have been dynamically configured.
forbidden - (Optional) Specifies to display forbidden router ports that have been statically configured.
If no parameter is specified, the system will display all currently configured router ports on the Switch.

Restrictions

None.

Example

To display the mld_snooping mrouter ports:

```
DGS-3000-28XMP:admin# show mld_snooping mrouter_ports vlan default
Command: show mld_snooping mrouter_ports vlan default


VLAN Name                : default
Static Router Port       : 1-10
Dynamic Router Port      :
Router IP                :
Forbidden Router Port    : 11

 Total Entries: 1


DGS-3000-28XMP:admin#
```

53-11 create mld_snooping static_group

Description

This command is used to create an MLD snooping static group. Member ports can be added to the static group. The static member and the dynamic member ports form the member ports of a group.

The static group will only take effect when MLD snooping is enabled on the VLAN. An **active** static group must be equal to a static MLD group with a link-up member port. For those static member ports, the device needs to emulate the MLD protocol operation to the querier, and forward the traffic destined to the multicast group to the member ports.

The Reserved IP multicast addresses FF0x::/16 must be excluded from the configured group.

The VLAN must be created first before a static group can be created.

Format

create mld_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipv6addr>

Parameters

vlan - Specifies the name of the VLAN on which the static group resides. **<vlan_name 32>** - Enter the VLAN name here. The VLAN name can be up to 32 characters long.
vlanid - Specifies the ID of the VLAN on which the static group resides. **<vlanid_list>** - Enter the VLAN ID list here.
<ipv6addr> - Specifies the multicast group IPv6 address.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To create an MLD snooping static group for VLAN 1, group FF1E::1:

```
DGS-3000-28XMP:admin# create mld_snooping static_group vlan default FF1E::1
Command: create mld_snooping static_group vlan default FF1E::1

Success.

DGS-3000-28XMP:admin#
```

53-12 delete mld_snooping static_group

Description

This command is used to delete a MLD Snooping multicast static group.

Format

delete mld_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipv6addr>

Parameters

vlan - Specifies the name of the VLAN on which the static group resides. **<vlan_name 32>** - Enter the VLAN name here. The VLAN name can be up to 32 characters long.
vlanid - Specifies the ID of the VLAN on which the static group resides. **<vlanid_list>** - Enter the VLAN ID list here.
<ipv6addr> - Enter the multicast group IP address.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete an MLD snooping static group for VLAN 1, group FF1E::1:

```
DGS-3000-28XMP:admin# delete mld_snooping static_group vlan default FF1E::1
Command: delete mld_snooping static_group vlan default FF1E::1

Success.

DGS-3000-28XMP:admin#
```

53-13 config mld_snooping static_group

Description

This command is used to configure an MLD snooping multicast group static member port. When a port is configured as a static member port, the MLD protocol will not operate on this port. For example, suppose that a port is a dynamic member port learned by MLD. If this port is configured as a static member later, then the MLD protocol will stop operating on this port. The MLD protocol will resume once this port is removed from static member ports.

Format

config mld_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipv6addr> [add | delete] <portlist>

Parameters

vlan - Specifies the name of the VLAN on which the static group resides. **<vlan_name 32>** - Enter the VLAN name here. The VLAN name can be up to 32 characters long.
vlanid - Specifies the ID of the VLAN on which the static group resides. **<vlanid_list>** - Enter the VLAN ID list here.
<ipv6addr> - Enter the multicast group IPv6 address.
add - Specifies to add the member ports.
delete - Specifies to delete the member ports.
<portlist> - Specifies a range of ports to be configured.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To unset port range 9-10 from MLD snooping static member ports for group FF1E::1 on default VLAN:

```
DGS-3000-28XMP:admin# config mld_snooping static_group vlan default FF1E::1 delete
9-10
Command: config mld_snooping static_group vlan default FF1E::1 delete 9-10

Success.

DGS-3000-28XMP:admin#
```

53-14 show mld_snooping static_group

Description

This command used to display the MLD snooping multicast group static members.

Format

show mld_snooping static_group {[vlan <vlan_name 32> | vlanid <vlanid_list>] <ipv6addr>}

Parameters

vlan - (Optional) Specifies the name of the VLAN on which the static group resides. **<vlan_name 32>** - Enter the VLAN name here. The VLAN name can be up to 32 characters long.
vlanid - (Optional) Specifies the ID of the VLAN on which the static group resides. **<vlanid_list>** - Enter the VLAN ID list here.
<ipv6addr> - (Optional) Enter the multicast group IPv6 address.

Restrictions

None.

Example

To display all the MLD snooping static groups:

```
DGS-3000-28XMP:admin# show mld_snooping static_group
VLAN ID/Name          IP Address             Static Member Ports
--------------   ------------------    ------------------------
1 / Default           FF1E ::1               9-10

Total Entries : 1

DGS-3000-28XMP:admin#
```

53-15 config mld_snooping data_driven_learning

Description

This command is used to enable or disable the data-driven learning of an MLD snooping group.

When data-driven learning is enabled for the VLAN, when the Switch receives the IP multicast traffic, on this VLAN, an MLD snooping group will be created. That is, the learning of an entry is not activated by MLD membership registration, but activated by the traffic. For an ordinary MLD snooping entry, the MLD protocol will take care the aging out of the entry. For a data-driven entry, the entry can be specified not to be aged out or to be aged out by the aged timer.

When the data driven learning is enabled, and the data driven table is not full, the multicast filtering mode for all ports is ignored. That is, the multicast packets will be forwarded to router ports. If the data driven learning table is full, the multicast packets will be forwarded according to the multicast filtering mode.

NOTE: If a data-driven group is created and MLD member ports are learned later, the entry will become an ordinary MLD snooping entry. That is, the aging out mechanism will follow the ordinary MLD snooping entry.

Format

config mld_snooping data_driven_learning [all | vlan_name <vlan_name> | vlanid <vlanid_list>] {state [enable | disable] | aged_out [enable | disable] | expiry_time <sec 1-65535>}(1)

Parameters

all - Specifies that all VLANs are to be configured.
vlan_name - Specifies the VLAN name to be configured. **<vlan_name>** - Enter the VLAN name here.
vlanid - Specifies the VLAN ID to be configured. **<vlanid_list>** - Enter the VLAN ID list here.
state - (Optional) Specifies to enable or disable the data driven learning of MLD snooping groups. **enable** - Enter enable to enable the data driven learning state. This is the default option. **disable** - Enter disable to disable the data driven learning state.
aged_out - (Optional) Enable or disable the aging out of entries.

enable - Specifies to enable the aged out option.

disable - Specifies to disable the aged out option. This is the default option.

expiry_time - (Optional) Specifies the data driven group lifetime, in seconds. This parameter is valid only when **aged_out** is enabled.

<sec 1-65535> - Enter the expiry time value here. This value must be between 1 and 65535 seconds.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable the data driven learning of an MLD snooping group on the default VLAN:

```
DGS-3000-28XMP:admin# config mld_snooping data_driven_learning vlan default state enable
Command: config mld_snooping data_driven_learning vlan default state enable

Success.

DGS-3000-28XMP:admin#
```

53-16 config mld_snooping data_driven_learning max_learned_entry

Description

This command is used to configure the maximum number of groups that can be learned by data driven.

When the table is full, the system will stop the learning of the new data-driven groups. Traffic for the new groups will be dropped.

Format

config mld_snooping data_driven_learning max_learned_entry <value 1-1024>

Parameters

<value 1-1024> - Enter the maximum number of groups that can be learned by data driven. This value must be between 1 and 1024. The default setting is 128.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

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

```
DGS-3000-28XMP:admin# config mld_snooping data_driven_learning max_learned_entry 50
Command: config mld_snooping data_driven_learning max_learned_entry 50

Success.

DGS-3000-28XMP:admin#
```

53-17 clear mld_snooping data_driven_group

Description

This command is used to delete the MLD snooping group(s) learned by data driven learning.

Format

clear mld_snooping data_driven_group [all | [vlan_name <vlan_name> | vlanid <vlanid_list>] [<ipv6addr>| all]]

Parameters

all - Specifies all VLANs to which MLD snooping groups will be deleted.
vlan_name - Specifies the VLAN name. **<vlan_name>** - Enter the VLAN name here.
vlanid - Specifies the VLAN ID. **<vlanid_list>** - Enter the VLAN ID list here.
<ipv6addr> - Enter the group's IPv6 address learned by data driven learning.
all - Specifies to clear all data driven groups of the specified VLAN.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To clear all the groups learned by data-driven:

```
DGS-3000-28XMP:admin# clear mld_snooping data_driven_group all
Command: clear mld_snooping data_driven_group all

Success.

DGS-3000-28XMP:admin#
```

53-18 show mld_snooping statistic counter

Description

This command is used to display the statistics counter for MLD protocol packets that are received by the Switch since MLD snooping was enabled.

Format

show mld_snooping statistic counter [vlan <vlan_name> | vlanid <vlanid_list> | ports <portlist>]

Parameters

vlan - Specifies a VLAN to be displayed. **<vlan_name>** - Enter the VLAN name here.
vlanid - Specifies a list of VLANs to be displayed. **<vlanid_list>** - Enter the VLAN ID list here.
ports - Specifies a list of ports to be displayed. **<portlist>** - Enter the list of ports here.

Restrictions

None.

Example

To show MLD snooping statistics counters:

```
DGS-3000-28XMP:admin# show mld_snooping statistic counter vlanid 1
Command: show mld_snooping statistic counter vlanid 1

VLAN Name  : Default
-----------------------------------------------
  Total Groups          : 10
Receive Statistics
      Query
MLD v1 Query                    : 1
MLD v2 Query                    : 1
Total                           : 2
Dropped By Rate Limitation      : 1
Dropped By Multicast VLAN       : 1

  Report & Leave
MLD v1 Report                   : 0
MLD v2 Report                   : 10
MLD v1 Done                     : 1
Total                           : 11
Dropped By Rate Limitation      : 0
Dropped By Max Group Limitation : 90
Dropped By Group Filter         : 0
Dropped By Multicast VLAN       : 1

Transmit Statistics
Query
MLD v1 Query                    : 1
MLD v2 Query                    : 1
Total                           : 2
Report & Leave
MLD v1 Report                   : 0
MLD v2 Report                   : 10
MLD v1 Done                     : 1
Total                           : 11

Total Entries : 1

DGS-3000-28XMP:admin#
```

53-19 clear mld_snooping statistics counter

Description

This command is used to clear MLD snooping statistics counters.

Format

clear mld _snooping statistics counter

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To clear MLD snooping statistics counter:

```
DGS-3000-28XMP:admin# clear mld_snooping statistics counter
Command: clear mld_snooping statistics counter

Success.

DGS-3000-28XMP:admin#
```

53-20 config mld_snooping rate_limit

Description

This command is used to configure the rate limit of MLD control packets that are allowed by each port or VLAN.

Format

config mld_snooping rate_limit [ports <portlist> | vlanid <vlanid_list>] [<value 1-1000> | no_limit]

Parameters

ports - Specifies a range of ports to be configured. **<portlist>** - Enter the range of ports to be configured here.
vlanid - Specifies a range of VLANs to be configured. **<vlanid_list>** - Enter the VLAN ID list here.
<value 1-1000> - Specifies the rate limit of MLD control packets that the Switch can process on a specific port or VLAN. The rate is specified in packet per second. The packets that exceed the limited rate will be dropped.
no_limit - Specifies the rate limit of MLD control packets that the Switch can process on a specific port or VLAN. The rate is specified in packet per second. The packets that exceed the limited rate will be dropped. The default setting is no_limit.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the MLD snooping per port rate limit:

```
DGS-3000-28XMP:admin# config mld_snooping rate_limit ports 1 100
Command: config mld_snooping rate_limit ports 1 100

Success.

DGS-3000-28XMP:admin#
```

53-21 show mld_snooping rate_limit

Description

This command is used to display the rate limit of MLD control packets that are allowed by each port or VLAN.

Format

show mld_snooping rate_limit [ports <portlist> | vlanid <vlanid_list>]

Parameters

ports - Specifies a list of ports. **<portlist>** - Enter the range of ports to be configured here.
vlanid - Specifies a list of VLANs. **<vlanid_list>** - Enter the VLAN ID list here.

Restrictions

None.

Example

To display the MLD snooping rate limit from port 1 to 5:

```
DGS-3000-28XMP:admin# show mld_snooping rate_limit ports 1-5
Command: show mld_snooping rate_limit ports 1-5

 Port      Rate Limit
 --------  ---------------
 1         100
 2         No Limit
 3         No Limit
 4         No Limit
 5         No Limit

Total Entries: 5

DGS-3000-28XMP:admin#
```

53-22 show mld_snooping host

Description

This command is used to display the MLD hosts that joined groups on the specific port or VALN.

Format

show mld_snooping host {[vlan <vlan_name 32> | vlanid <vlanid_list> | ports <portlist> | group <ipv6addr>]}

Parameters

vlan - (Optional) Specifies the name of VLAN. **<vlan_name 32>** - Enter the VLAN name.
vlanid - (Optional) Specifies the ID of VLAN. **<vlanid_list>** - Enter a list of VLANs.
ports - (Optional) Specifies ports to be displayed. **<portlist>** - Enter a range of ports to be displayed.
group - (Optional) Specifies the group to be displayed. **< ipv6addr >** - Enter the IPv6 address of the group.

Restrictions

None.

Example

To display the MLD host IP information:

```
DGS-3000-28XMP:admin#show mld_snooping host vlan default
Command: show mld_snooping host vlan default

VLAN ID          : 1
 Group            : FF12::1:FF11:11
 Port             : 3
 Host             : FE80::200:FF:FE70:3

 VLAN ID          : 1
 Group            : FF13::1:3
 Port             : 3
 Host             : FE80::845:B9BE:A863:A1FD

 Total Entries : 2

DGS-3000-28XMP:admin#
```

To display the host IP information for the group “FF32:3::1234:5600”:

```
DGS-3000-28XMP:admin# show mld_snooping host group FF32:3::1234:5600
Command: show mld_snooping host group FF32:3::1234:5600

 VLAN ID          : 1
 Group            : FF32:3::1234:5600
 Port             : 3
 Host             : FE80::200:4FF:FE01:1

 Total Entries : 1

DGS-3000-28XMP:admin#
```

Chapter 54 MSTP debug enhancement Command List

debug stp config ports [<portlist> | all] [event | bpdu | state_machine | all] state [disable | brief | detail]
debug stp show information
debug stp show flag {ports <portlist>}
debug stp show counter {ports [<portlist> | all]}
debug stp clear counter {ports[<portlist> | all]}
debug stp state [enable | disable]

54-1 debug stp config ports

Description

This command is used to configure per-port STP debug level on the specified ports.

Format

debug stp config ports [<portlist> | all] [event | bpdu | state_machine | all] state [disable | brief | detail]

Parameters

<portlist> - Enter the STP port range to debug.
all - Specifies to debug all ports on the Switch.
event - Specifies to debug the external operation and event processing.
bpdu - Specifies to debug the BPDU's that have been received and transmitted.
state_machine - Specifies to debug the state change of the STP state machine.
all - Specifies to debug all of the above.
state - Specifies the state of the debug mechanism. **disable** - Specifies to disable the debug mechanism. **brief** - Specifies the debug level to brief. **detail** - Specifies the debug level to detail.

Restrictions

Only Administrators can issue this command.

Example

To configure all STP debug flags to brief level on all ports:

```
DGS-3000-28XMP:admin# debug stp config ports all all state brief
Command: debug stp config ports all all state brief

Success.

DGS-3000-28XMP:admin#
```

54-2 debug stp show information

Description

This command is used to display STP detailed information, such as the hardware tables, the STP state, etc.

Format

debug stp show information

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To show STP debug information:

```
DGS-3000-28XMP:admin# debug stp show information
Command: debug stp show information

Warning: only support local device.
Spanning Tree Debug Information:
---------------------------------------
Port Status In Hardware Table:
Instance 0:
Port 1   : FOR  Port 2   : FOR  Port 3   : FOR  Port 4   : FOR  Port 5   : FOR
Port 6   : FOR
Port 7   : FOR  Port 8   : FOR  Port 9   : FOR  Port 10  : FOR  Port 11  : FOR
Port 12  : FOR
Port 13  : FOR  Port 14  : FOR  Port 15  : FOR  Port 16  : FOR  Port 17  : FOR
Port 18  : FOR
Port 19  : FOR  Port 20  : FOR  Port 21  : FOR  Port 22  : FOR  Port 23  : FOR
Port 24  : FOR
Port 25  : FOR  Port 26  : FOR  Port 27  : FOR  Port 28  : FOR
---------------------------------------
Root Priority And Times:
Instance 0:
 Designated Root Bridge : 29683/DD-FE-F7-F8-DF-DA
 External Root Cost     : -336244805
 Regional Root Bridge   : 57055/6F-D1-FD-2F-08-B7
 Internal Root Cost     : -107020353
 Designated Bridge      : 57851/FD-EF-EF-C9-FC-9B
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

54-3 debug stp show flag

Description

This command is used to display the STP debug level on specified ports.

Format

debug stp show flag {ports <portlist>}

Parameters

ports - (Optional) Specifies the STP ports to display. **<portlist>** - Enter the list of ports used for this configuration here.
If no parameter is specified, all ports on the Switch will be displayed.

Restrictions

Only Administrators can issue this command.

Example

To display the debug STP levels on all ports:

```
DGS-3000-28XMP:admin# debug stp show flag
DGS-3000-28XMP:admin# debug stp show flag
Command: debug stp show flag

Global State: Disabled

Port Index       Event Flag       BPDU Flag       State Machine Flag
-------------------------------------------------------------
 1               Disabled         Disabled        Disabled
 2               Disabled         Disabled        Disabled
 3               Disabled         Disabled        Disabled
 4               Disabled         Disabled        Disabled
 5               Disabled         Disabled        Disabled
 5               Disabled         Disabled        Disabled
 7               Disabled         Disabled        Disabled
 8               Disabled         Disabled        Disabled
 9               Disabled         Disabled        Disabled
 10              Disabled         Disabled        Disabled
 11              Disabled         Disabled        Disabled
 12              Disabled         Disabled        Disabled
 13              Disabled         Disabled        Disabled
 14              Disabled         Disabled        Disabled
 15              Disabled         Disabled        Disabled
 16              Disabled         Disabled        Disabled
 17              Disabled         Disabled        Disabled
 18              Disabled         Disabled        Disabled
 19              Disabled         Disabled        Disabled
 20              Disabled         Disabled        Disabled
 21              Disabled         Disabled        Disabled
 22              Disabled         Disabled        Disabled
 23              Disabled         Disabled        Disabled
 24              Disabled         Disabled        Disabled
 25              Disabled         Disabled        Disabled
 26              Disabled         Disabled        Disabled
 27              Disabled         Disabled        Disabled
 28              Disabled         Disabled        Disabled

DGS-3000-28XMP:admin#
```

54-4 debug stp show counter

Description

This command is used to display the STP counters.

Format

debug stp show counter {ports [<portlist> | all]}

Parameters

ports - (Optional) Specifies the STP ports to be displayed.
<portlist> - Enter the list of ports to be displayed here.

all - Specifies to display all port's counters.

If no parameter is specified, the global counters will be displayed.

Restrictions

Only Administrators can issue this command.

Example

To show the STP counters for port 9:

```
DGS-3000-28XMP:admin# debug stp show counter ports 9
Command: debug stp show counter ports 9

STP Counters
-------------------------------------
 Port 9    :
  Receive:                                Transmit:
  Total STP Packets         : 0           Total STP Packets  : 0
  Configuration BPDU        : 0           Configuration BPDU : 0
  TCN BPDU                  : 0           TCN BPDU           : 0
  RSTP TC-Flag              : 0           RSTP TC-Flag       : 0
  RST BPDU                  : 0           RST BPDU           : 0

  Discard:
  Total Discarded BPDU      : 0
  Global STP Disabled       : 0
  Port STP Disabled         : 0
  Invalid packet Format     : 0
  Invalid Protocol          : 0
  Configuration BPDU Length : 0
  TCN BPDU Length           : 0
  RST BPDU Length           : 0
  Invalid Type              : 0
  Invalid Timers            : 0

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

54-5 debug stp clear counter

Description

This command is used to clear the STP counters.

Format

debug stp clear counter {ports[<portlist> | all]}

Parameters

ports - (Optional) Specifies the port range.

<portlist> - Enter the list of ports used for this configuration here.

all - Specifies to clear all port counters.

Restrictions

Only Administrators can issue this command.

Example

To clear all STP counters on the Switch:

```
DGS-3000-28XMP:admin# debug stp clear counter ports all
Command: debug stp clear counter ports all

Success.

DGS-3000-28XMP:admin#
```

54-6 debug stp state

Description

This command is used to enable or disable the STP debug state.

Format

debug stp state [enable | disable]

Parameters

enable - Specifies to enable the STP debug state.
disable - Specifies to disable the STP debug state.

Restrictions

Only Administrators can issue this command.

Example

To configure the STP debug state to enable, and then disable the STP debug state:

```
DGS-3000-28XMP:admin# debug stp state enable
Command: debug stp state enable

Success.

DGS-3000-28XMP:admin# debug stp state disable
Command: debug stp state disable

Success.

DGS-3000-28XMP:admin#
```

Chapter 55 Multicast Filter Command List

create mcast_filter_profile {[ipv4 | ipv6]} profile_id <value 1-24> profile_name <name 1-32>
config mcast_filter_profile [profile_id <value 1-24> | profile_name <name 1-32>] {profile_name <name 1-32> | [add | delete] <mcast_address_list>}(1)
config mcast_filter_profile ipv6 [profile_id <value 1-24> | profile_name <name 1-32>] {profile_name <name 1-32> | [add | delete] <mcastv6_address_list>}(1)
delete mcast_filter_profile {[ipv4 | ipv6]} [profile_id [<value 1-24> | all] | profile_name <name 1-32>]
show mcast_filter_profile {[ipv4 | ipv6]} {[profile_id <value 1-24> | profile_name <name 1-32>]}
config limited_multicast_addr [ports <portlist> | vlanid <vlanid_list>] {[ipv4 | ipv6]} { [add | delete] [profile_id <value 1-24> | profile_name <name 1-32>] | access [permit | deny]}
config max_mcast_group [ports <portlist> | vlanid <vlanid_list] {[ipv4 | ipv6]} {max_group [<value 1-1024> | infinite] | action [drop | replace]}(1)
show max_mcast_group [ports <portlist> | vlanid <vlanid_list>] {[ipv4 | ipv6]}
show limited_multicast_addr [ports <portlist> | vlanid <vlanid_list>] {[ipv4 | ipv6]}
config cpu_filter l3_control_pkt <portlist> [{dvmrp|pim|igmp_query |ospf | rip | vrrp} | all] state [enable | disable]
show cpu_filter l3_control_pkt ports {<portlist>}

55-1 create mcast_filter_profile

Description

This command is used to configure a multicast address profile. Multiple ranges of multicast addresses can be defined in the profile. If the IPv4 or ipv6 option is not specified, IPv4 is implied.

Format

create mcast_filter_profile {[ipv4 | ipv6]} profile_id <value 1-24> profile_name <name 1-32>

Parameters

ipv4 - (Optional) Specifies to add an IPv4 multicast profile.
ipv6 - (Optional) Specifies to add an IPv6 multicast profile.
profile_id - Specifies the ID of the profile. **<value 1-24>** - Enter the profile ID value here. This value must be between 1 and 24.
profile_name - Specifies to provide a description for the profile. **<name 1-32>** - Enter the profile name here. The profile name can be up to 32 characters long.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To create a multicast address profile with a profile ID of 2 and a profile name of MOD:

```
DGS-3000-28XMP:admin# create mcast_filter_profile profile_id 2 profile_name MOD
Command: create mcast_filter_profile profile_id 2 profile_name MOD

Success.

DGS-3000-28XMP:admin#
```

55-2 config mcast_filter_profile

Description

This command is used to add or delete a range of multicast IP addresses to or from the profile.

Format

config mcast_filter_profile [profile_id <value 1-24> | profile_name <name 1-32>] {profile_name <name 1-32> | [add | delete] <mcast_address_list>}(1)

Parameters

profile_id - Specifies the ID of the profile. **<value 1-24>** - Enter the profile ID value here. This value must be between 1 and 24.
profile_name - Specifies a meaningful description for the profile. **<name 1-32>** - Enter the profile name here. The profile name can be up to 32 characters long.
profile_name - Specifies a meaningful description for the profile. **<name 1-32>** - Enter the profile name here. The profile name can be up to 32 characters long.
add - Specifies to add a multicast address.
delete - Specifies to delete a multicast address.
<mcast_address_list> - Enter a list of the multicast addresses to be put in the profile. You can either specify a single multicast IP address or a range of multicast addresses using -.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To add the multicast address range 225.1.1.1 to 225.1.1.10 to the profile:

```
DGS-3000-28XMP:admin# config mcast_filter_profile profile_id 2 add 225.1.1.1 - 225.1.1.10
Command: config mcast_filter_profile profile_id 2 add 225.1.1.1 - 225.1.1.10

Success.

DGS-3000-28XMP:admin#
```

55-3 config mcast_filter_profile ipv6

Description

This command is used to add or delete a range of IPv6 multicast addresses to the profile.

Format

config mcast_filter_profile ipv6 [profile_id <value 1-24> | profile_name <name 1-32>] {profile_name <name 1-32> | [add | delete] <mcastv6_address_list>}(1)

Parameters

profile_id - Specifies the ID of the profile. **<value 1-24>** - Enter the profile ID value here. This value must be between 1 and 24.
profile_name - Specifies a meaningful description for the profile. **<name 1-32>** - Enter the profile name here. The profile name can be up to 32 characters long.
profile_name - Specifies a meaningful description for the profile. **<name 1-32>** - Enter the profile name here. The profile name can be up to 32 characters long.
add - Specifies to add an IPv6 multicast address.
delete - Specifies to delete an IPv6 multicast address.
<mcastv6_address_list> - Enter a list of the IPv6 multicast addresses to add to the profile. You can either specify a single IPv6 multicast IP address or a range of IPv6 multicast addresses connected by '-'.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To add the IPv6 multicast address range FFF0E::100:0:0:20 – FFF0E::100:0:0:22 to profile ID 3:

```
DGS-3000-28XMP:admin# config mcast_filter_profile ipv6 profile_id 3 add FF0E::100:0:0:20–
FFF0E::100:0:0:22
Command: config mcast_filter_profile ipv6 profile_id 3 add FF0E::100:0:0:20–
FFF0E::100:0:0:22


Success.


DGS-3000-28XMP:admin#
```

55-4 delete mcast_filter_profile

Description

This command is used to delete a multicast address profile. If the IPv4 or IPv6 option is not specified, IPv4 is implied.

Format

delete mcast_filter_profile {[ipv4 | ipv6]} [profile_id [<value 1-24> | all] | profile_name <name 1-32>]

Parameters

ipv4 - (Optional) Specifies to delete an IPv4 multicast profile.
ipv6 - (Optional) Specifies to delete an IPv6 multicast profile.

profile_id - Specifies the ID of the profile **<value 1-24>** - Enter the profile ID value here. This value must be between 1 and 24. **all** - Specifies that all multicast address profiles will be deleted.
profile_name - Specifies to display a profile based on the profile name. **<name 1-32>** - Enter the profile name value here. The profile name can be up to 32 characters long.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete the multicast address profile with a profile ID of 3:

```
DGS-3000-28XMP:admin# delete mcast_filter_profile profile_id  3
Command: delete mcast_filter_profile profile_id  3
Success.

DGS-3000-28XMP:admin#
```

To delete the multicast address profile called MOD:

```
DGS-3000-28XMP:admin# delete mcast_filter_profile profile_name MOD
Command: delete mcast_filter_profile profile_name MOD

Total entries: 2

DGS-3000-28XMP:admin#
```

55-5 show mcast_filter_profile

Description

This command is used to display the defined multicast address profiles. If the IPv4 or IPv6 option is not specified, IPv4 is implied.

Format

show mcast_filter_profile {[ipv4 | ipv6]} {[profile_id <value 1-24> | profile_name <name 1-32>]}

Parameters

ipv4 - (Optional) Specifies to delete an IPv4 multicast profile.
ipv6 - (Optional) Specifies to delete an IPv6 multicast profile.
profile_id - (Optional) Specifies the ID of the profile **<value 1-24>** - Enter the profile ID value here. This value must be between 1 and 24.
profile_name - (Optional) Specifies to display a profile based on the profile name. **<name 1-32>** - Enter the profile name here. The profile name can be up to 32 characters long.

Restrictions

None.

Example

To display all the defined multicast address profiles:

```
DGS-3000-28XMP:admin# show mcast_filter_profile
Command: show mcast_filter_profile

Profile ID       Name        Multicast Addresses
----  ----------------  ----------------  ----------------
1                MOD        234.1.1.1 - 238.244.244.244
                            234.1.1.1 - 238.244.244.244
2              customer     224.19.62.34 - 224.19.162.200

Total Entries : 2

DGS-3000-28XMP:admin#
```

55-6 config limited_multicast_addr

Description

This command is used to configure the multicast address filtering function on a port or VLAN. When there are no profiles specified with a port or VLAN, the limited function is not effective. When the function is configured on a port, it limits the multicast group operated by the IGMP or MLD snooping function. When this function is configured on a VLAN, the multicast group is limited to only operate the IGMP or MLD layer 3 functions. If the IPv4 or IPv6 option is not specified, IPv4 is implied.

Format

config limited_multicast_addr [ports <portlist> | vlanid <vlanid_list>] {[ipv4 | ipv6]} {[add | delete] [profile_id <value 1-24> | profile_name <name 1-32>] | access [permit | deny]}

Parameters

ports - Specifies the range of ports to configure the multicast address filtering function. **<portlist>** - Enter the list of ports to be configured here.
vlanid - Specifies the VLAN ID of the VLAN that the multicast address filtering function will be configured on. **<vlanid_list>** - Enter the VLAN ID list here.
ipv4 - (Optional) Specifies the IPv4 multicast profile.
ipv6 - (Optional) Specifies the IPv6 multicast profile.
add - (Optional) Specifies to add a multicast address profile to a port.
delete - (Optional) Specifies to delete a multicast address profile to a port.
profile_id - (Optional) Specifies a profile to be added to or deleted from the port. **<value 1-24>** - Enter the profile ID value here. This value must be between 1 and 24.
profile_name - (Optional) Specifies the profile name to be used. **<name 1-32>** - Enter the profile name here. The profile name can be up to 32 characters long.
access - (Optional) Specifies the access of packets matching the addresses defined in the profiles. **permit** - Specifies that packets matching the addresses defined in the profiles will be permitted. The default

mode is permit.

deny - Specifies that packets matching the addresses defined in the profiles will be denied.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To add multicast address profile 2 to ports 1 and 3:

```
DGS-3000-28XMP:admin# config limited_multicast_addr ports 1,3  add profile_id 2
Command: config limited_multicast_addr ports 1,3  add profile_id 2

Success.

DGS-3000-28XMP:admin#
```

55-7 config max_mcast_group

Description

This command is used to configure the maximum number of multicast groups that a port can join.

If the IPv4 or IPv6 option is not specified, IPv4 is implied.

When the joined groups for a port or a VLAN have reached the maximum number, the newly learned group will be dropped if the action is specified as drop. The newly learned group will replace the eldest group if the action is specified as replace.

Format

config max_mcast_group [ports <portlist> | vlanid <vlanid_list] {[ipv4 | ipv6]} {max_group [<value 1-1024> | infinite] | action [drop | replace]}(1)

Parameters

ports - Specifies the range of ports to configure the max_mcast_group.
- **<portlist>** - Enter the list of ports to be configured here.

vlanid - Specifies the VLAN ID to configure max_mcast_group.
- **<vlanid_list>** - Enter the VLAN ID list here.

ipv4 - (Optional) Specifies that the maximum number of IPv4 learned addresses should be limited.

ipv6 - (Optional) Specifies that the maximum number of IPv6 learned addresses should be limited.

max_group - Specifies the maximum number of multicast groups.
- **<value 1-1024>** - Enter the maximum group value here. This value must be between 1 and 1024.
- **infinite** - Specifies that the maximum number of multicast groups per port or VLAN is not limited by the Switch.

action - Specifies the action for handling newly learned groups when the register is full.
- **drop** - Specifies the new group will be dropped.
- **replace** - Specifies the new group will replace the eldest group in the register table.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the maximum number of multicast group that ports 1 and 3 can join to 100:

```
DGS-3000-28XMP:admin# config max_mcast_group ports 1, 3 max_group 100
Command: config max_mcast_group ports 1, 3 max_group 100

Success.

DGS-3000-28XMP:admin#
```

55-8 show max_mcast_group

Description

This command is used to display the maximum number of multicast groups that a port can join. If the IPv4 or IPv6 option is not specified, IPv4 is implied.

Format

show max_mcast_group [ports <portlist> | vlanid <vlanid_list>] {[ipv4 | ipv6]}

Parameters

ports - Specifies the range of ports for displaying information about the maximum number of multicast groups that the specified ports can join. **<portlist>** - Enter the list of ports to be configured here.
vlanid - Specifies the VLAN ID for displaying the maximum number of multicast groups. **<vlanid_list>** - Enter the VLAN ID list here.
ipv4 - (Optional) Specifies to display the maximum number of IPv4 learned addresses.
ipv6 - (Optional) Specifies to display the maximum number of IPv6 learned addresses.

Restrictions

None.

Example

To display the maximum number of multicast groups that ports 1 and 2 can join:

```
DGS-3000-28XMP:admin# show max_mcast_group ports 1-2
Command: show max_mcast_group ports 1-2

Port      Max Multicast Group Number    Action
------    --------------------------  ---------
1         100                           Drop
2         Infinite                      Drop

Total Entries: 2


DGS-3000-28XMP:admin#
```

To display the maximum number of multicast groups that VLANs 1 and 2 can join:

```
DGS-3000-28XMP:admin# show max_mcast_group vlanid 1-2
Command: show max_mcast_group vlanid 1-2

VLAN      Max Multicast Group Number    Action
------    --------------------------  ---------
1         Infinite                      Drop
2         10                            Drop

Total Entries: 2

DGS-3000-28XMP:admin#
```

55-9 show limited_multicast_addr

Description

This command is used to display the multicast address range by port or by VLAN.

When the function is configured on a port, it limits the multicast groups operated by the IGMP or MLD snooping function and layer 3 functions. When the function is configured on a VLAN, it limits the multicast groups operated by the IGMP or MLD layer 3 functions.

If the IPv4 or IPv6 option is not specified, IPv4 is implied.

Format

show limited_multicast_addr [ports <portlist> | vlanid <vlanid_list>] {[ipv4 | ipv6]}

Parameters

ports - Specifies the range of ports that require information displaying about the multicast address filtering function. **<portlist>** - Enter the list of ports to be configured here.
vlanid - Specifies the VLAN ID of VLANs that require information displaying about the multicast address filtering function. **<vlanid_list>** - Enter the VLAN ID list here.
ipv4 - (Optional) Specifies to display the IPv4 multicast profile associated with the port.
ipv6 - (Optional) Specifies to display the IPv6 multicast profile associated with the port.

Restrictions

None.

Example

To show the limited multicast address range on ports 1 and 3:

```
DGS-3000-28XMP:admin# show limited_multicast_addr ports 1,3
Command: show limited_multicast_addr ports 1,3

Port    : 1
Access  : Deny

Profile ID      Name                 Multicast Addresses
-----------    -----------        ---------------------------
1              customer             224.19.62.34 - 224.19.162.200

Port    : 3
Access  : Deny

Profile ID      Name                 Multicast Addresses
-----------    ----------------   ---------------------------
1              customer          224.19.62.34 - 224.19.162.200

DGS-3000-28XMP:admin#
```

To show the limited multicast settings configured on VLAN 1:

```
DGS-3000-28XMP:admin# show limited_multicast_addr vlan 1
Command: show limited_multicast_addr vlan 1

VLAN ID     : 1
Access      : Deny

Profile ID      Name               Multicast Addresses
----------  -----------------    ---------------------------
1           customer               224.19.62.34 - 224.19.162.200


Success.

DGS-3000-28XMP:admin#
```

55-10 config cpu_filter l3_control_pkt

Description

This command is used to configure the port state for the Layer 3 control packet filter.

Format

config cpu_filter l3_control_pkt <portlist> [{dvmrp|pim|igmp_query |ospf | rip | vrrp} | all] state [enable | disable]

Parameters

<portlist> - Specifies the port list to filter control packets.
dvmrp – (Optional) Specifies to filter the DVMRP control packets.
pim - (Optional) Specifies to filter the PIM control packets.
igmp_query - (Optional) Specifies to filter the IGMP query control packets.
ospf - (Optional) Specifies to filter the OSPF control packets.
rip - (Optional) Specifies to filter the RIP control packets.
vrrp - (Optional) Specifies to filter the VRRP control packets.
all - Specifies to filter all the L3 protocol control packets.
state - Specifies the filter function status. **enable** - Specifies to enable the filtering function. **disable** - Specifies to disable the filtering function. This is the default option.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To filter the DVMRP control packets on ports 1 to 2:

```
DGS-3000-28XMP:admin# config cpu_filter l3_control_pkt 1-2 dvmrp state enable
Command: config cpu_filter l3_control_pkt 1-2 dvmrp state enable

Success.

DGS-3000-28XMP:admin#
```

55-11 show cpu_filter l3_control_pkt ports

Description

This command is used to display the L3 control packet CPU filtering state.

Format

show cpu_filter l3_control_pkt ports {<portlist>}

Parameters

<portlist> - (Optional) Specifies the port list to display the L3 control packet CPU filtering state.

Restrictions

None.

Example

To display the filtering status for port 1 and 2:

```
DGS-3000-28XMP:admin#show cpu_filter l3_control_pkt ports 1-2
Command: show cpu_filter l3_control_pkt ports 1-2

 Port    IGMP Query    DVMRP         PIM        OSPF         RIP       VRRP
 ----   ----------    --------    --------    --------    --------    --------
 1       Disabled      Enabled      Disabled      Disabled    Disabled    Disabled
 2       Disabled      Enabled      Disabled      Disabled    Disabled    Disabled

DGS-3000-28XMP:admin#
```

Chapter 56 Multicast VLAN Command List

enable igmp_snooping multicast_vlan
enable mld_snooping multicast_vlan
disable igmp_snooping multicast_vlan
disable mld_snooping multicast_vlan
create igmp_snooping multicast_vlan <vlan_name 32> <vlanid 2-4094> {remap_priority [<value 0-7> | none] {replace_priority}}
create igmp_snooping multicast_vlan_group_profile <profile_name 1-32>
create mld_snooping multicast_vlan <vlan_name 32> <vlanid 2-4094> {remap_priority [<value 0-7> | none] {replace_priority}}
create mld_snooping multicast_vlan_group_profile <profile_name 1-32>
config igmp_snooping multicast_vlan <vlan_name 32> {[add | delete] [member_port <portlist> | [source_port <portlist> | untag_source_port <portlist>] | tag_member_port <portlist>] | state [enable|disable] | replace_source_ip <ipaddr> | remap_priority [<value 0-7> | none] {replace_priority}}(1)
config igmp_snooping multicast_vlan_group_profile <profile_name 1-32> [add | delete] <mcast_address_list>
config igmp_snooping multicast_vlan_group <vlan_name 32> [add | delete] profile_name <profile_name 1-32>
config igmp_snooping multicast_vlan forward_unmatched [enable | disable]
config mld_snooping multicast_vlan <vlan_name 32> {[add | delete] [member_port <portlist> | [source_port <portlist> | untag_source_port <portlist>] | tag_member_port <portlist>] | state [enable | disable] | replace_source_ipv6 <ipv6addr> | remap_priority [<value 0-7> | none] {replace_priority}}(1)
config mld_snooping multicast_vlan_group_profile <profile_name 1-32> [add | delete] <mcastv6_address_list>
config mld_snooping multicast_vlan_group <vlan_name 32> [add | delete] profile_name <profile_name 1-32>
config mld_snooping multicast_vlan forward_unmatched [disable | enable]
show igmp_snooping multicast_vlan_group {<vlan_name 32>}
delete igmp_snooping multicast_vlan_group_profile [profile_name <profile_name 1-32> | all]
delete igmp_snooping multicast_vlan <vlan_name 32>
delete mld_snooping multicast_vlan_group_profile [profile_name <profile_name 1-32> | all]
delete mld_snooping multicast_vlan <vlan_name 32>
show igmp_snooping multicast_vlan_group_profile {< profile_name 1-32>}
show igmp_snooping multicast_vlan {<vlan_name 32>}
show mld_snooping multicast_vlan_group_profile {<profile_name 1-32>}
show mld_snooping multicast_vlan_group {<vlan_name 32>}
show mld_snooping multicast_vlan {<vlan_name 32>}

56-1 enable igmp_snooping multicast_vlan

Description

This command is used to control the status of the multicast VLAN function.

Format

enable igmp_snooping multicast_vlan

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To enable the IGMP snooping multicast VLAN function globally:

```
DGS-3000-28XMP:admin# enable igmp_snooping multicast_vlan
Command: enable igmp_snooping multicast_vlan

Success.

DGS-3000-28XMP:admin#
```

56-2 enable mld_snooping multicast_vlan

Description

This command is used to enable the MLD snooping multicast VLAN function. By default, the multicast VLAN is disabled.

Format

enable mld_snooping multicast_vlan

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To enable MLD snooping multicast VLAN:

```
DGS-3000-28XMP:admin#enable mld_snooping multicast_vlan
Command: enable mld_snooping multicast_vlan

Success.

DGS-3000-28XMP:admin#
```

56-3 disable igmp_snooping multicast_vlan

Description

This command is used to disable the IGMP multicast VLAN function. By default, the multicast VLAN is disabled.

Format

disable igmp_snooping multicast_vlan

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To disable the IGMP snooping multicast VLAN function:

```
DGS-3000-28XMP:admin# disable igmp_snooping multicast_vlan
Command: disable igmp_snooping multicast_vlan

Success.

DGS-3000-28XMP:admin#
```

56-4 disable mld_snooping multicast_vlan

Description

This command is used to disable the MLD snooping multicast VLAN function. By default, the multicast VLAN is disabled.

Format

disable mld_snooping multicast_vlan

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To disable MLD snooping multicast VLAN:

```
DGS-3000-28XMP:admin#disable mld_snooping multicast_vlan
Command: disable mld_snooping multicast_vlan

Success.

DGS-3000-28XMP:admin#
```

56-5 create igmp_snooping multicast_vlan

Description

This command is used to create a multicast VLAN and implements relevant parameters as specified. More than one multicast VLANs can be configured. The maximum number of configurable VLANs is 5.

Newly created IGMP snooping multicast VLANs must use a unique VLAN ID and name, i.e. they cannot use the VLAN ID or name of any existing 802.1q VLAN.

Also keep in mind the following conditions:

- Multicast VLANs cannot be configured or displayed using 802.1Q VLAN commands.
- An IP interface cannot be bound to a multicast VLAN.
- The multicast VLAN snooping function co-exists with the 802.1q VLAN snooping function.

Format

create igmp_snooping multicast_vlan <vlan_name 32> <vlanid 2-4094> {remap_priority [<value 0-7> | none] {replace_priority}}

Parameters

<vlan_name 32> - Enter the multicast VLAN here. The VLAN name can be up to 32 characters long.

<vlanid 2-4094> - Enter the VLAN ID of the multicast VLAN to be created. This value must be between 2 and 4094.

remap_priority - (Optional) Specifies the remap priority (0 to 7) to be associated with the data traffic to be forwarded on the multicast VLAN. If none is specified, the packet's original priority will be used. The default setting is none.

<value 0-7> - Enter the remap priority value here. This value must be between 0 and 7.

none - Specifies that the remap priority value will be set to none.

replace_priority - (Optional) Specifies that packet's priority will be changed by the Switch, based on the remap priority. This flag will only take effect when the remap priority is set.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To create an IGMP snooping multicast VLAN with the VLAN name mv1 and the VID 2:

```
DGS-3000-28XMP:admin# create igmp_snoop multicast_vlan mv1 2
Command: create igmp_snoop multicast_vlan mv1 2

Success.

DGS-3000-28XMP:admin#
```

56-6 create igmp_snooping multicast_vlan_group_profile

Description

This command is used to create an IGMP snooping multicast group profile on the Switch.

Format

create igmp_snooping multicast_vlan_group_profile <profile_name 1-32>

Parameters

<profile_name 1-32> - Enter the multicast VLAN group profile name here. The name can be up to 32 characters long.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To create an IGMP snooping multicast group profile with the name “test”:

```
DGS-3000-28XMP:admin# create igmp_snooping multicast_vlan_group_profile test
Command: create igmp_snooping multicast_vlan_group_profile test

Success.

DGS-3000-28XMP:admin#
```

56-7 create mld_snooping multicast_vlan

Description

This command is used to create an MLD snooping multicast VLAN and implements relevant parameters as specified. More than one multicast VLAN can be configured. Newly created MLD snooping multicast VLANs must use a unique VLAN ID and name, i.e. they cannot use the VLAN ID or name of any existing 802.1Q VLAN. Also keep in mind the following conditions: multicast VLANs cannot be configured or displayed using 802.1Q VLAN commands; an IP interface cannot be bound to a multicast VLAN; and the multicast VLAN snooping function co-exists with the 802.1Q VLAN snooping function.

Format

create mld_snooping multicast_vlan <vlan_name 32> <vlanid 2-4094> {remap_priority [<value 0-7> | none] {replace_priority}}

Parameters

<vlan_name 32> - Enter the multicast VLAN here. The VLAN name can be up to 32 characters long.
<vlanid 2-4094> - Enter the VLAN ID of the multicast VLAN to be created. This value must be between 2 and 4094.
remap_priority - (Optional) Specifies the remap priority (0 to 7) to be associated with the data traffic to be forwarded on the multicast VLAN. If none is specified, the packet's original priority will be used. The default setting is none. **<value 0-7>** - Enter the remap priority value here. This value must be between 0 and 7. **none** - Specifies that the remap priority value will be set to none. **replace_priority** - (Optional) Specifies that packet's priority will be changed by the Switch, based on the remap priority. This flag will only take effect when the remap priority is set.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To create an MLD snooping multicast VLAN with the VLAN name mv1 and the VID 2:

```
DGS-3000-28XMP:admin#create mld_snooping multicast_vlan mv1 2
Command: create mld_snooping multicast_vlan mv1 2

Success.

DGS-3000-28XMP:admin#
```

56-8 create mld_snooping multicast_vlan_group_profile

Description

This command is used to create a multicast group profile. The profile name for MLD snooping must be unique.

Format

create mld_snooping multicast_vlan_group_profile <profile_name 1-32>

Parameters

<profile_name 1-32> - Enter the multicast VLAN group profile name here. The name can be up to 32 characters long.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To create an MLD snooping multicast group profile with the name “mtest”:

```
DGS-3000-28XMP:admin#create mld_snooping multicast_vlan_group_profile mtest
Command: create mld_snooping multicast_vlan_group_profile mtest

Success.

DGS-3000-28XMP:admin#
```

56-9 config igmp_snooping multicast_vlan

Description

This command is used to add member ports and source ports to a list of multicast VLAN member ports. Member ports automatically become untagged members of the multicast VLAN and source ports automatically become tagged members of the multicast VLAN. However, member ports of one multicast VLAN are allowed to overlap with member ports on a different multicast VLAN.

A multicast VLAN must first be created using the **create igmp_snooping multicast_vlan** command before the multicast VLAN can be configured.

Format

config igmp_snooping multicast_vlan <vlan_name 32> {[add | delete] [member_port <portlist> | [source_port <portlist> | untag_source_port <portlist>] | tag_member_port <portlist>] | state [enable|disable] | replace_source_ip <ipaddr> | remap_priority [<value 0-7> | none] {replace_priority}}(1)

Parameters

<vlan_name 32> - Enter the multicast VLAN here. The VLAN name can be up to 32 characters long.

add - Specifies that the port will be added to the specified multicast VLAN.

delete - Specifies that the port will be deleted from the specified multicast VLAN.

member_port - Specifies a member port or range of member ports to be added to the multicast VLAN. The specified range of ports will become untagged members of the multicast VLAN.

<portlist> - Enter the list of ports to be configured here.

source_port - Specifies a port or range of ports to be added to the multicast VLAN.

<portlist> - Enter the list of ports to be configured here.

untag_source_port - Specifies the source port or range of source ports as untagged members of the multicast VLAN. The PVID of the untagged source port is automatically changed to the multicast VLAN. Source ports must be either tagged or untagged for any single multicast VLAN, i.e. both types cannot be members of the same multicast VLAN.

<portlist> - Enter the list of ports to be configured here.

tag_member_port - Specifies the port or range of ports that will become tagged members of the multicast VLAN.

<portlist> - Enter the list of ports to be configured here.

state - Specifies to enable or disable the multicast VLAN for a chosen VLAN.

enable - Specifies to enable the multicast VLAN for a chosen VLAN.

disable - Specifies to disable the multicast VLAN for a chosen VLAN.

replace_source_ip - Specifies that the source IP address in the join packet must be replaced by this IP address before forwarding the packet sent by the host. If 0.0.0.0 is specified, the source IP address will not be replaced.

<ipaddr> - Enter the replace source IP address here.

remap_priority - Specifies the remap priority value to be associated with the data traffic to be forwarded on the multicast VLAN. If none is specified, the packet's original priority is used. The default setting is none.

<value 0-7> - Enter the remap priority value here. This value must be between 0 and 7.

none - Specifies that the remap priority value will be set to none.

replace_priority - (Optional) Specifies that the packet priority will be changed to the remap_priority, but only if remap_priority is set.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure an IGMP snooping multicast VLAN with the name “mv1”, make ports 1 and 3 members of the VLAN, and set the state to **enable**:

```
DGS-3000-28XMP:admin# config igmp_snooping multicast_vlan mv1 add member_port 1,3 state
enable
Command: config igmp_snooping multicast_vlan mv1 add member_port 1,3 state enable

Success.

DGS-3000-28XMP:admin#
```

56-10 config igmp_snooping multicast_vlan_group_profile

Description

This command is used to configure an IGMP snooping multicast group profile on the Switch and add or delete multicast addresses for the profile.

Format

config igmp_snooping multicast_vlan_group_profile <profile_name 1-32> [add | delete] <mcast_address_list>

Parameters

<profile_name 1-32> - Enter the multicast VLAN group name here. This name can be up to 32 characters long.

add - Specifies to add a multicast address list to or from this multicast VLAN profile.

delete - Specifies to delete a multicast address list to or from this multicast VLAN profile.

<mcast_address_list> - Enter the multicast VLAN IP address here. This can be a single multicast address or a list/range of multicast addresses. A list of multicast addresses should be separated with commas. A range of multicast address should be separated with a hyphen.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To add multicast addresses to the IGMP snooping multicast VLAN profile named “test”:

```
DGS-3000-28XMP:admin# config igmp_snooping multicast_vlan_group_profile test add
225.1.1.1,225.1.1.8-225.1.1.10
Command: config igmp_snooping multicast_vlan_group_profile test add 225.1.1.1,225.1.1.8-
225.1.1.10

Success.

DGS-3000-28XMP:admin#
```

56-11 config igmp_snooping multicast_vlan_group

Description

This command is used to configure the multicast group learned with the specific multicast VLAN. The following two cases can be considered as examples:

Case 1: The multicast group is not configured, multicast VLANs do not have any member ports overlapping, and the join packet received by the member port is learned only on the multicast VLAN that this port is a member of.

Case 2: The join packet is learned on the multicast VLAN that contains the destination multicast group. If the destination multicast group of the join packet cannot be classified into any multicast VLAN to which this port belongs, then the join packet will be learned on the VLAN of the packet.

NOTE: A profile cannot overlap in different multicast VLANs. Multiple profiles can be added to a multicast VLAN.

Format

config igmp_snooping multicast_vlan_group <vlan_name 32> [add | delete] profile_name <profile_name 1-32>

Parameters

<vlan_name 32> - Enter the multicast VLAN name here. The VLAN name can be up to 32 characters long.
add - Specifies to associate a profile to a multicast VLAN.
delete - Specifies to de-associate a profile from a multicast VLAN.
profile_name - Specifies the multicast VLAN profile name. **<profile_name 1-32>** - Enter the multicast VLAN profile name here. The name can be up to 32 characters long.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To add an IGMP snooping profile to a multicast VLAN group with the name “v1”:

```
DGS-3000-28XMP:admin# config igmp_snooping multicast_vlan_group v1 add profile_name channel_1
Command: config igmp_snooping multicast_vlan_group v1 add profile_name channel_1
Success.

DGS-3000-28XMP:admin#
```

56-12 config igmp_snooping multicast_vlan forward_unmatched

Description

This command is used to configure the forwarding mode for multicast VLAN unmatched packets. When the Switch receives an IGMP snooping packet, it will match the packet against the multicast profile to determine which multicast VLAN to associate with. If the packet does not match any profile, the packet will be forwarded or dropped based on this setting.

By default, the packet will be dropped.

Format

config igmp_snooping multicast_vlan forward_unmatched [enable | disable]

Parameters

enable - Specifies that the packet will be flooded on the VLAN.
disable - Specifies that the packet will be dropped.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the forwarding mode for multicast VLAN unmatched packets：

```
DGS-3000-28XMP:admin# config igmp_snooping multicast_vlan forward_unmatched enable
Command: config igmp_snooping multicast_vlan forward_unmatched enable

Success.

DGS-3000-28XMP:admin#
```

56-13 config mld_snooping multicast_vlan

Description

This command is used to configure MLD snooping multicast VLAN parameters. The member port list and source port list cannot overlap. However, the member port of one multicast VLAN can overlap with another multicast VLAN. The multicast VLAN must be created first using the **create mld_snooping multicast_vlan** command before the multicast VLAN can be configured.

Format

config mld_snooping multicast_vlan <vlan_name 32> {[add | delete] [member_port <portlist> | [source_port <portlist> | untag_source_port <portlist>] | tag_member_port <portlist>] | state [enable | disable] | replace_source_ipv6 <ipv6addr> | remap_priority [<value 0-7> | none] {replace_priority}}(1)

Parameters

<vlan_name 32> - Enter the multicast VLAN here. The VLAN name can be up to 32 characters long.

add - Specifies that the port will be added to the specified multicast VLAN.

delete - Specifies that the port will be deleted from the specified multicast VLAN.

member_port - Specifies a member port or range of member ports to be added to the multicast VLAN. The specified range of ports will become untagged members of the multicast VLAN.

<portlist> - Enter the list of ports to be configured here.

source_port - Specifies a port or range of ports to be added to the multicast VLAN.

<portlist> - Enter the list of ports to be configured here.

untag_source_port - Specifies the source port or range of source ports as untagged members of the multicast VLAN. The PVID of the untagged source port is automatically changed to the multicast VLAN. Source ports must be either tagged or untagged for any single multicast VLAN, i.e. both types cannot be members of the same multicast VLAN.

<portlist> - Enter the list of ports to be configured here.

tag_member_port - Specifies the port or range of ports that will become tagged members of the multicast VLAN.

<portlist> - Enter the list of ports to be configured here.

state - Specifies to enable or disable the multicast VLAN for a chosen VLAN.

enable - Specifies to enable the multicast VLAN for a chosen VLAN.

disable - Specifies to disable the multicast VLAN for a chosen VLAN.

replace_source_ipv6 - Specifies that the source IPv6 address in the join packet must be replaced by this IPv6 address before forwarding the packet sent by the host.

<ipv6addr> - Enter the IPv6 address here.

remap_priority - Specifies the remap priority value to be associated with the data traffic to be forwarded on the multicast VLAN. If none is specified, the packet's original priority is used. The default setting is none.

<value 0-7> - Enter the remap priority value here. This value must be between 0 and 7.

none - Specifies that the remap priority value will be set to none.

replace_priority - (Optional) Specifies that the packet priority will be changed to the remap_priority, but only if remap_priority is set.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure an MLD snooping multicast VLAN with the name "v1", make ports 1 and 3 members of the VLAN, and set the state to enable:

```
DGS-3000-28XMP:admin#config mld_snooping multicast_vlan v1 add member_port 1,3 state enable
Command: config mld_snooping multicast_vlan v1 add member_port 1,3 state enable

Success.

DGS-3000-28XMP:admin#
```

56-14 config mld_snooping multicast_vlan_group_profile

Description

This command is used to configure an MLD snooping multicast group profile on the switch.

Format

config mld_snooping multicast_vlan_group_profile <profile_name 1-32> [add | delete] <mcastv6_address_list>

Parameters

<profile_name 1-32> - Enter the multicast VLAN group name here. This name can be up to 32 characters long.
add - Specifies to add a multicast address list to or from this multicast VLAN profile.
delete - Specifies to delete a multicast address list to or from this multicast VLAN profile.
<mcastv6_address_list> - Enter the multicast VLAN IPv6 address here. This can be a single multicast address or a list/range of multicast addresses. A list of multicast addresses should be separated with commas. A range of multicast address should be separated with a hyphen.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To add the single multicast address FF1E::11 and multicast range FF1E::12-FF1E::20 to the MLD snooping multicast VLAN profile named “mtest”:

```
DGS-3000-28XMP:admin#config mld_snooping multicast_vlan_group_profile mtest add FF1E::11, FF1E::12-FF1E::20
Command: config mld_snooping multicast_vlan_group_profile mtest add FF1E::11, FF1E::12-FF1
E::20

Success.

DGS-3000-28XMP:admin#
```

56-15 config mld_snooping multicast_vlan_group

Description

This command is used to configure the multicast group learned with the specific multicast VLAN. The following two cases can be considered as examples:

Case 1: The multicast group is not configured, multicast VLANs do not have any member ports overlapping, and the join packet received by the member port is learned only on the multicast VLAN that this port is a member of.

Case 2: The join packet is learned on the multicast VLAN that contains the destination multicast group. If the destination multicast group of the join packet cannot be classified into any multicast VLAN to which this port belongs, then the join packet will be learned on the VLAN of the packet.

NOTE: A profile cannot overlap in different multicast VLANs. Multiple profiles can be added to a multicast VLAN.

Format

config mld_snooping multicast_vlan_group <vlan_name 32> [add | delete] profile_name <profile_name 1-32>

Parameters

<vlan_name 32> - Enter the multicast VLAN name here. The VLAN name can be up to 32 characters long.
add - Specifies to associate a profile to a multicast VLAN.
delete - Specifies to de-associate a profile from a multicast VLAN.
profile_name - Specifies the multicast VLAN profile name. **<profile_name 1-32>** - Enter the multicast VLAN profile name here. The name can be up to 32 characters long.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the forwarding mode for MLD snooping multicast VLAN unmatched packets:

```
DGS-3000-28XMP:admin#config mld_snooping multicast_vlan_group v1 add profile_name mtest
Command: config mld_snooping multicast_vlan_group v1 add profile_name mtest

Success.

DGS-3000-28XMP:admin#
```

56-16 config mld_snooping multicast_vlan forward_unmatched

Description

This command is used to configure the forwarding mode for multicast VLAN unmatched packets. When the Switch receives an MLD snooping packet, it will match the packet against the multicast profile to determine which multicast VLAN to associate with. If the packet does not match any profile, the packet will be forwarded or dropped based on this setting.

By default, the packet will be dropped.

Format

config mld_snooping multicast_vlan forward_unmatched [disable | enable]

Parameters

enable - Specifies that the packet will be flooded on the VLAN.
disable - Specifies that the packet will be dropped.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the forwarding mode for MLD snooping multicast VLAN unmatched packets:

```
DGS-3000-28XMP:admin#config mld_snooping multicast_vlan forward_unmatched enable

Command: config mld_snooping multicast_vlan forward_unmatched enable

Success.

DGS-3000-28XMP:admin#
```

56-17 delete igmp_snooping multicast_vlan_group_profile

Description

This command is used to delete an IGMP snooping multicast group profile on the Switch.

Format

delete igmp_snooping multicast_vlan_group_profile [profile_name <profile_name 1-32> | all]

Parameters

profile_name - Specifies the multicast VLAN profile name. **<profile_name 1-32>** - Enter the multicast VLAN profile name here. This name can be up to 32 characters long.	
all - Specifies to delete all the multicast VLAN profiles.	

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete an IGMP snooping multicast group profile with the name “MOD”:

```
DGS-3000-28XMP:admin# delete igmp_snooping multicast_vlan_group_profile profile_name MOD
Command: delete igmp_snooping multicast_vlan_group_profile profile_name MOD

Success.

DGS-3000-28XMP:admin#
```

56-18 delete igmp_snooping multicast_vlan

Description

This command is used to delete an IGMP snooping multicast VLAN.

Format

delete igmp_snooping multicast_vlan <vlan_name 32>

Parameters

<vlan_name 32> - Enter the multicast VLAN name here. The VLAN name can be up to 32 characters long.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete an IGMP snooping multicast VLAN called “v1”:

```
DGS-3000-28XMP:admin# delete igmp_snooping multicast_vlan v1
Command: delete igmp_snooping multicat_vlan v1

Success.

DGS-3000-28XMP:admin#
```

56-19 delete mld_snooping multicast_vlan_group_profile

Description

This command is used to delete an MLD snooping multicast group profile on the Switch.

Format

delete mld_snooping multicast_vlan_group_profile [profile_name <profile_name 1-32> | all]

Parameters

profile_name - Specifies the multicast VLAN profile name.

<profile_name 1-32> - Enter the multicast VLAN profile name here. This name can be up to 32 characters long.

all - Specifies to delete all the multicast VLAN profiles.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete an MLD snooping multicast group profile named “mtest”:

```
DGS-3000-28XMP:admin#delete mld_snooping multicast_vlan_group_profile profile_name mtest
Command: delete mld_snooping multicast_vlan_group_profile profile_name mtest

Success.

DGS-3000-28XMP:admin#
```

56-20 delete mld_snooping multicast_vlan

Description

This command is used to delete an MLD snooping multicast VLAN.

Format

delete mld_snooping multicast_vlan <vlan_name 32>

Parameters

<vlan_name 32> - Enter the multicast VLAN name here. The VLAN name can be up to 32 characters long.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete an MLD snooping multicast VLAN called “v1”:

```
DGS-3000-28XMP:admin#delete mld_snooping multicast_vlan v1
Command: delete mld_snooping multicast_vlan v1

Success.

DGS-3000-28XMP:admin#
```

56-21 show igmp_snooping multicast_vlan_group_profile

Description

This command is used to show IGMP snooping multicast group profiles.

Format

show igmp_snooping multicast_vlan_group_profile {< profile_name 1-32>}

Parameters

<profile_name 1-32> - (Optional) Enter the multicast VLAN group profile name here. The name can be up to 32 characters long.

Restrictions

None.

Example

To display all IGMP snooping multicast VLAN profiles:

```
DGS-3000-28XMP:admin# show igmp_snooping multicast_vlan_group_profile
Command: show igmp_snooping multicast_vlan_group_profile

Profile Name              Multicast Addresses
--------------------  --------------------------------
MOD                        234.1.1.1 - 238.244.244.244
                           239.1.1.1 - 239.2.2.2
Customer                   224.19.62.34 - 224.19.162.200

Total Entries : 2


DGS-3000-28XMP:admin#
```

56-22 show igmp_snooping multicast_vlan_group

Description

This command is used to show the IGMP snooping multicast VLAN group information.

Format

show igmp_snooping multicast_vlan_group {<vlan_name 32>}

Parameters

<vlan_name 32> - (Optional) Enter the VLAN name here. The VLAN name can be up to 32 characters long.

Restrictions

None.

Example

To show all IGMP snooping multicast VLAN groups setup on the Switch:

```
DGS-3000-28XMP:admin# show igmp_snooping multicast_vlan_group
Command: show igmp_snooping multicast_vlan_group


VLAN Name                       VLAN ID        Multicast Group Profiles
------------------------------  -------  --------------------------------
mv1                             2         test


DGS-3000-28XMP:admin#
```

56-23 show igmp_snooping multicast_vlan

Description

This command is used to display the IGMP snooping multicast VLAN information.

Format

show igmp_snooping multicast_vlan {<vlan_name 32>}

Parameters

<vlan_name 32> - (Optional) Enter the VLAN name here. The VLAN name can be up to 32 characters long.

Restrictions

None.

Example

To display all IGMP snooping multicast VLANs:

```
DGS-3000-28XMP:admin# show igmp_snooping multicast_vlan
Command: show igmp_snooping multicast_vlan

IGMP Multicast VLAN Global State        : Disabled
IGMP Multicast VLAN Forward Unmatched   : Disabled

VLAN Name                               : test
VID                                     : 100

Member(Untagged) Ports                  : 1
Tagged Member Ports                     :
Source Ports                            : 3
Untagged Source Ports                   :
Status                                  : Disabled
Replace Source IP                       : 0.0.0.0
Remap Priority                          : None

Total Entries: 1

DGS-3000-28XMP:admin#
```

56-24 show mld_snooping multicast_vlan_group_profile

Description

This command is used to show MLD snooping multicast group profiles.

Format

show mld_snooping multicast_vlan_group_profile {<profile_name 1-32>}

Parameters

<profile_name 1-32> - (Optional) Enter the multicast VLAN group profile name here. The name can be up to 32 characters long.

Restrictions

None.

Example

To display all MLD snooping multicast VLAN profiles:

```
DGS-3000-28XMP:admin#show mld_snooping multicast_vlan_group_profile
Command: show mld_snooping multicast_vlan_group_profile

Profile Name                    Multicast Addresses
------------------------------- -------------------------------
mtest                           FF1E::11
                                FF1E::12-FF1E::20


 Total Entries: 1


DGS-3000-28XMP:admin#
```

56-25 show mld_snooping multicast_vlan_group

Description

This command is used to show the MLD snooping multicast VLAN group information.

Format

show mld_snooping multicast_vlan_group {<vlan_name 32>}

Parameters

<vlan_name 32> - (Optional) Enter the VLAN name here. The VLAN name can be up to 32 characters long.

Restrictions

None.

Example

To display all MLD snooping multicast VLANs' group profile information:

```
DGS-3000-28XMP:admin#show mld_snooping multicast_vlan_group
Command: show mld_snooping multicast_vlan_group


VLAN Name                       VLAN ID  Multicast Group Profiles
------------------------------  -------  --------------------------------
v1                              10        mtest


Total Entries: 1

DGS-3000-28XMP:admin#
```

56-26 show mld_snooping multicast_vlan

Description

This command is used to display the MLD snooping multicast VLAN information.

Format

show mld_snooping multicast_vlan {<vlan_name 32>}

Parameters

<vlan_name 32> - (Optional) Enter the VLAN name here. The VLAN name can be up to 32 characters long.

Restrictions

None.

Example

To display all MLD snooping multicast VLANs:

```
DGS-3000-28XMP:admin#show mld_snooping multicast_vlan
Command: show mld_snooping multicast_vlan

MLD Multicast VLAN Global State         : Enabled
MLD Multicast VLAN Forward Unmatched    : Enabled

VLAN Name                     :v1
VID                           :10
Member(Untagged) Ports        :1,3
Tagged Member Ports           :
Source Ports                  :
Untagged Source Ports         :
Status                        :Enabled
Replace Source IP             :::
Remap Priority                :None


 Total Entries: 1


DGS-3000-28XMP:admin#
```

Chapter 57 Multiple Spanning Tree Protocol (MSTP) Command List

enable stp
disable stp
config stp {maxage <value 6-40> | maxhops <value 6-40> | hellotime <value 1-2> | forwarddelay <value 4-30> | txholdcount <value 1-10> | fbpdu [enable | disable] | nni_bpdu_addr [dot1d | dot1ad]}
show stp
create stp instance_id <value 1-7>
config stp instance_id <value 1-7> [add_vlan | remove_vlan] <vidlist>
delete stp instance_id <value 1-7>
config stp mst_config_id {revision_level <int 0-65535> | name <string>}
show stp mst_config_id
config stp mst_ports <portlist> instance_id <value 0-7> { internalCost [auto | <value 1-200000000>] | priority <value 0-240>}
config stp ports <portlist> {externalCost [auto | <value 1-200000000>] | hellotime <value 1-2> | migrate [yes | no] |edge [true | false | auto] | p2p [true | false | auto] | state [enable | disable] | restricted_role [true | false] | restricted_tcn [true | false] | fbpdu [enable | disable]}
show stp ports {<portlist>}
config stp priority <value 0-61440> instance_id <value 0-7>
config stp version [mstp | rstp | stp]
show stp instance {<value 0-7>}

57-1 enable stp

Description

This command is used to enable STP globally.

Format

enable stp

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable STP:

```
DGS-3000-28XMP:admin# enable stp
Command: enable stp

Success.

DGS-3000-28XMP:admin#
```

57-2 disable stp

Description

This command is used to disable STP globally.

Format

disable stp

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To disable STP:

```
DGS-3000-28XMP:admin# disable stp
Command: disable stp

Success.

DGS-3000-28XMP:admin#
```

57-3 config stp

Description

This command is used to configure the bridge parameters global settings.

Format

config stp {maxage <value 6-40> | maxhops <value 6-40> | hellotime <value 1-2> | forwarddelay <value 4-30> | txholdcount <value 1-10> | fbpdu [enable | disable] | nni_bpdu_addr [dot1d | dot1ad]}

Parameters

maxage - (Optional) Specifies to determine if a BPDU is valid. The default value is 20. **<value 6-40>** - Enter the maximum age value here. This value must be between 6-40.
maxhops - (Optional) Specifies to restrict the forwarded times of one BPDU. The default value is 20.

<value 6-40> - Enter the maximum hops value here. This value must be between 6 and 40.
hello_time - (Optional) Specifies the time interval for sending configuration BPDUs by the Root Bridge. The default value is 2 seconds. This parameter is for STP and RSTP. MSTP uses per-port hellotime parameter. **<value 1-2>** - Enter the hello time value here. This value must be between 1 and 2.
forwarddelay - (Optional) Specifies the maximum delay time for one BPDU to be transmitted by a bridge and received from another bridge. The default value is 15. **<value 4-30>** - Enter the maximum delay time here. This value must be between 4 and 30.
txholdcount - (Optional) Specifies to restrict the numbers of BPDU transmitted in a time interval. **<value 1-10>** - Enter the transmitted BPDU restriction value here. This value must be between 1 and 10.
fbpdu - (Optional) Specifies whether the bridge will flood STP BPDU when STP functionality is disabled. **enable** - Specifies that the bridge will flood STP BPDU when STP functionality is disabled. **disable** - Specifies that the bridge will not flood STP BPDU when STP functionality is disabled.
nni_bpdu_addr - (Optional) Specifies to determine the BPDU protocol address for GVRP at the service provider site. It can use an 802.1d GVRP address, an 802.1ad service provider GVRP address, or a user-defined multicast address. The range of user-defined addresses are from 0180C2000000 to 0180C2FFFFFF. **dot1d** - Specifies that the NNI BPDU protocol address value will be set to Dot1d. **dot1ad** - Specifies that the NNI BPDU protocol address value will be set to Dot1ad.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure STP:

```
DGS-3000-28XMP:admin# config stp maxage 25
Command: config stp maxage 25

Success.

DGS-3000-28XMP:admin#
```

57-4 show stp

Description

This command is used to show the bridge parameters global settings.

Format

show stp

Parameters

None.

Restrictions

None.

Example

To show STP:

```
DGS-3000-28XMP:admin# show stp
Command: show stp

 STP Bridge Global Settings
 --------------------------
 STP Status         : Enabled
 STP Version        : RSTP
 Max Age            : 25
 Hello Time         : 2
 Forward Delay      : 15
 Max Hops           : 20
 TX Hold Count      : 6
 Forwarding BPDU    : Disabled
 NNI BPDU Address   : dot1d


DGS-3000-28XMP:admin#
```

57-5 create stp instance_id

Description

This command is used to create an MST Instance without mapping the corresponding VLANs.

Format

create stp instance_id <value 1-7>

Parameters

<value 1-7> - Enter the MSTP instance ID here. This value must be between 1 and 7.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To create MSTP instance:

```
DGS-3000-28XMP:admin# create stp instance_id 2
Command: create stp instance_id 2

Success.

DGS-3000-28XMP:admin#
```

57-6 config stp instance_id

Description

This command is used to map or remove the VLAN range of the specified MST instance for the existed MST instances.

Format

config stp instance_id <value 1-7> [add_vlan | remove_vlan] <vidlist>

Parameters

<value 1-7> - Enter the MSTP instance ID here. This value must be between 1 and 7.
add_vlan - Specifies to map the specified VLAN list to an existing MST instance.
remove_vlan - Specifies to delete the specified VLAN list from an existing MST instance.
<vidlist> - Specifies a list of VLANs by VLAN ID.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To map a VLAN ID to an MSTP instance:

```
DGS-3000-28XMP:admin# config stp instance_id 2 add_vlan 1-3
Command: config stp instance_id 2 add_vlan 1-3

Success.

DGS-3000-28XMP:admin#
```

To remove a VLAN ID from an MSTP instance:

```
DGS-3000-28XMP:admin# config stp instance_id 2 remove_vlan 2
Command: config stp instance_id 2 remove_vlan 2

Success.

DGS-3000-28XMP:admin#
```

57-7 delete stp instance_id

Description

This command is used to delete an MST instance.

Format

delete stp instance_id <value 1-7>

Parameters

<value 1-7> - Enter the MSTP instance ID here. This value must be between 1 and 7.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete an MSTP instance:

```
DGS-3000-28XMP:admin# delete stp instance_id 2
Command: delete stp instance_id 2

Success.

DGS-3000-28XMP:admin#
```

57-8 config stp mst_config_id

Description

This command is used to change the name or the revision level of the MST configuration ID.

Format

config stp mst_config_id {revision_level <int 0-65535> | name <string>}

Parameters

revision_level - (Optional) Specifies the same given name with different revision level also represents different MST regions.

<int 0-65535> - Enter the revision level here. This value must be between 0 and 65535.

name - (Optional) Specifies the name given for a specific MST region.

<string> - Enter the MST region name here.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To change the name and revision level of the MST configuration identification:

```
DGS-3000-28XMP:admin# config stp mst_config_id name R&D_BlockG revision_level 1
Commands: config stp mst_config_id name R&D_BlockG revision_level 1

Success.

DGS-3000-28XMP:admin#
```

57-9 show stp mst_config_id

Description

This command is used to show the MST configuration identification.

Format

show stp mst_config_id

Parameters

None.

Restrictions

None.

Example

show STP MST configuration ID:

```
DGS-3000-28XMP:admin# show stp mst_config_id
Command: show stp mst_config_id

Current MST Configuration Identification
---------------------------------------

Configuration Name : 00-22-22-22-22-00                        Revision Level :0
MSTI ID     Vid list
-------     -----------
   CIST     1-4094

DGS-3000-28XMP:admin#
```

57-10 config stp mst_ports

Description

This command is used to configure the port management parameters.

Format

config stp mst_ports <portlist> instance_id <value 0-7> {internalCost [auto | <value 1-200000000>] | priority <value 0-240>}

Parameters

<portlist> - Enter the list of ports that will be used in this configuration.
instance_id - Specifies the instance ID used. **<value 0-7>** - Enter the instance ID used here. This value must be between 0 and 7.
internalCost - (Optional) Specifies the port path cost used in MSTP. **auto** - Specifies that the internal cost value will be set to auto.

<value 1-200000000> - Enter the internal cost value here. This value must be between 1 and 200000000.

priority - (Optional) Specifies the port priority value.

<value 0-240> - Enter the port priority value here. This value must be between 0 and 240.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure STP MST ports:

```
DGS-3000-28XMP:admin# config stp mst_ports 1 instance_id 0 internalCost auto
Command: config stp mst_ports 1 instance_id 0 internalCost auto

Success.

DGS-3000-28XMP:admin#
```

57-11 config stp ports

Description

This command is used to configure all the parameters of ports, except for Internal Path Cost and Port Priority.

Format

config stp ports <portlist> {externalCost [auto | <value 1-200000000>] | hellotime <value 1-2> | migrate [yes | no] | edge [true | false | auto] | p2p [true | false | auto] | state [enable | disable]| restricted_role [true | false] | restricted_tcn [true | false] | fbpdu [enable | disable]}

Parameters

<portlist> - Enter the list of ports to be configured.

external_cost - (Optional) Specifies the path cost between MST regions from the transmitting bridge to the CIST Root Bridge. It is only used at CIST level.

auto - Specifies that the external cost value will be set to automatic.

<value 1-200000000> - Enter the external cost value here. This value must be between 1 and 200000000.

hellotime - (Optional) Specifies the hello time. The default value is 2. This parameter is for MSTP. STP and RSTP use a per-system hellotime parameter.

<value 1-2> - Enter the hello time value here. This value must be between 1 and 2.

migrate - (Optional) Specifies whether the port will send MSTP BPDUs for a delay time.

yes - Specifies that the MSTP BPDU for a delay time will be sent.

no - Specifies that the MSTP BPDU for a delay time will not be sent.

edge - (Optional) Specifies whether this port is connected to a LAN or a bridged LAN.

true - Specifies the port as an edge port.

false - Specifies the port as a link type port.

auto - Specifies that the bridge will wait before configuring the port as edge or not if no bridge BPDU packet is received. This is the default value.

p2p - (Optional) Specifies whether this port is in Full-Duplex or Half-Duplex mode.

true - Specifies that the port(s) is in Full-Duplex mode.

false - Specifies that the port(s) is in Half-Duplex mode. **auto** - Specifies that the port(s) is in Full-Duplex and Half-Duplex mode.
state - (Optional) Specifies whether this port supports the STP functionality. **enable** - Specifies that STP functionality on the port(s) is enabled. **disable** - Specifies that STP functionality on the port(s) is disabled.
restricted_role - (Optional) Specifies whether this port is selected as Root Port. **true** - Specifies that the port can be specified as the root port. **false** - Specifies that the port cannot be specified as the root port. This is the default value.
restricted_tcn - (Optional) Specifies whether this port propagates topology changes. The default value is false. **true** - Specifies that the port can be set to propagate a topology change. **false** - Specifies that the port cannot be set to propagate a topology change.
fbpdu - (Optional) Specifies whether this port will flood STP BPDUs when STP functionality is disabled. When the state is set to enable, the received BPDU will be forwarded. When the state is set to disable, the received BPDUs will be dropped. **enable** - Specifies that the port can be set to flood the STP BPDU when the STP functionality is disabled. **disable** - Specifies that the port cannot be set to flood the STP BPDU when the STP functionality is disabled.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure STP ports:

```
DGS-3000-28XMP:admin# config stp ports 1 externalCost auto
Command: config stp ports 1 externalCost auto

Success.

DGS-3000-28XMP:admin#
```

57-12 show stp ports

Description

This command is used to show the port information includes parameters setting and operational value.

Format

show stp ports {<portlist>}

Parameters

<portlist> - (Optional) Enter a list of ports used for the configuration here.

Restrictions

None.

Example

To show STP ports:

```
DGS-3000-28XMP:admin# show stp ports
Command: show stp ports

 MSTP Port Information
 ---------------------
 Port Index     : 1     , Hello Time: 2 /2 , Port STP : Enabled  ,
 External PathCost : Auto/200000   , Edge Port : Auto /No , P2P : Auto /Yes
 Port RestrictedRole : False,  Port RestrictedTCN : False
 Port Forward BPDU : Disabled
 MSTI   Designated Bridge   Internal PathCost  Prio  Status      Role
 -----  ------------------  -----------------  ----  ----------  ----------
 0      N/A                 200000             128   Forwarding  NonStp









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

57-13 config stp priority

Description

This command is used to configure the instance priority.

Format

config stp priority <value 0-61440> instance_id <value 0-7>

Parameters

<value 0-61440> - Enter the bridge priority value here. This value must be divisible by 4096. This value must be between 0 and 61440.
instance_id - Identifier to distinguish different STP instances. **<value 0-7>** - Enter the STP instance ID here. This value must be between 0 and 7.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the STP instance ID:

```
DGS-3000-28XMP:admin# config stp priority 61440 instance_id 0
Command: config stp priority 61440 instance_id 0

Success.

DGS-3000-28XMP:admin#
```

57-14 config stp version

Description

This command is used to configure the STP version.

Format

config stp version [mstp | rstp | stp]

Parameters

mstp - Specifies to use MSTP as the version.
rstp - Specifies to use RSTP as the version.
stp - Specifies to use STP as the version.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure STP version:

```
DGS-3000-28XMP:admin# config stp version mstp
Command: config stp version mstp

Success.

DGS-3000-28XMP:admin#
```

To configure the STP version as MSTP, when MSTP is the current version:

```
DGS-3000-28XMP:admin# config stp version mstp
Command: config stp version mstp

Configure value is the same with current value.
Success.

DGS-3000-28XMP:admin#
```

57-15 show stp instance

Description

This command is used to display each instance parameters settings. Value means the instance ID, if there is no input of this value, all instance will be shown.

Format

show stp instance {<value 0-7>}

Parameters

<value 0-7> - (Optional) Enter the MSTP instance ID value here. This value must be between 0 and 7.

Restrictions

None.

Example

To show STP instance:

```
DGS-3000-28XMP:admin# show stp instance
Command: show stp instance

STP Instance Settings
---------------------------
Instance Type          : CIST
Instance Status        : Enabled
Instance Priority      : 32768(bridge priority : 32768, sys ID ext : 0 )

STP Instance Operational Status
-------------------------------
Designated Root Bridge : 32768/00-22-22-22-22-00
External Root Cost     : 0
Regional Root Bridge   : 32768/00-22-22-22-22-00
Internal Root Cost     : 0
Designated Bridge      : 32768/00-22-22-22-22-00
Root Port                : None
Max Age                  : 20
Forward Delay           : 15
Last Topology Change   : 2430
Topology Changes Count : 0

DGS-3000-28XMP:admin#
```

Chapter 58 Network Load Balancing (NLB) Command List

create nlb unicast_fdb <macaddr>
config nlb unicast_fdb <macaddr> [add | delete] <portlist>
delete nlb unicast_fdb <macaddr>
create nlb multicast_fdb [<vlan_name 32> | vlanid <vlanid>] <macaddr>
config nlb multicast_fdb [<vlan_name 32> | vlanid <vlanid>] <macaddr> [add | delete] <portlist>
delete nlb multicast_fdb [<vlan_name 32> | vlanid <vlanid>] <macaddr>
show nlb fdb

58-1 create nlb unicast_fdb

Description

This command is used to create the NLB unicast FDB entry.

The network load balancing command set is used to support the Microsoft server load balancing application where multiple servers can share the same IP address and MAC address. The requests from clients will be forwarded to all servers, but will only be processed by one of them. The server can work in two different modes – unicast mode and multicast mode. In unicast mode, the client use unicast MAC address as the destination MAC to reach the server. In multicast mode, the client use the multicast MAC address as the destination MAC to reach the server. Regarding of the mode, this destination MAC is the named the shared MAC. The server uses its own MAC address (rather than the shared MAC) as the source MAC address of the reply packet.

Format

create nlb unicast_fdb <macaddr>

Parameters

<macaddr> - Specifies the MAC address of the NLB unicast FDB entry to be created.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To create an NLB unicast MAC forwarding entry, for the product that support the VLAN information on the unicast forwarding:

```
DGS-3000-28XMP:admin# create nlb unicast_fdb 02-bf-01-01-01-01
Command: create nlb unicast_fdb 02-BF-01-01-01-01

Success.

DGS-3000-28XMP:admin#
```

58-2 config nlb unicast_fdb

Description

This command is used to add or delete the forwarding ports for the specified NLB unicast FDB entry.

Format

config nlb unicast_fdb <macaddr>[add | delete] <portlist>

Parameters

<macaddr> - Enter the MAC address of the NLB unicast FDB entry to be configured.
add - Specifies to add the ports.
delete - Specifies to delete the ports.
<portlist> - Enter a list of forwarding ports to be added or removed.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure NLB unicast FDB entry, for the product that support the VLAN information on the unicast forwarding:

```
DGS-3000-28XMP:admin# config nlb unicast_fdb 02-bf-01-01-01-01 add 1-5
Command: config nlb unicast_fdb 02-BF-01-01-01-01 add 1-5

Success.

DGS-3000-28XMP:admin#
```

58-3 delete nlb unicast_fdb

Description

This command is used to delete the NLB unicast FDB entry.

Format

delete nlb unicast_fdb <macaddr>

Parameters

<macaddr> - Enter the MAC address of the NLB unicast FDB entry to be deleted.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete the NLB unicast FDB entry, for the product that support the VLAN information on the unicast forwarding:

```
DGS-3000-28XMP:admin# delete nlb unicast_fdb 02-bf-01-01-01-01
Command: delete nlb unicast_fdb 02-BF-01-01-01-01

Success.

DGS-3000-28XMP:admin#
```

58-4 create nlb multicast_fdb

Description

This command is used to create a NLB multicast FDB entry.

The NLB multicast FDB entry will be mutual exclusive with the L2 multicast entry.

Format

create nlb multicast_fdb [<vlan_name 32> | vlanid <vlanid>] <macaddr>

Parameters

<vlan_name 32> - Enter the VLAN name here. The VLAN name can be up to 32 characters long.
vlanid - Specifies the VLAN by the VLAN ID. **<vlanid>** - Enter the VLAN ID here.
<macaddr> - Enter the MAC address of the NLB multicast FDB entry to be created.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To create a NLB multicast FDB entry:

```
DGS-3000-28XMP:admin# create nlb multicast_fdb default 03-bf-01-01-01-01
Command: create nlb multicast_fdb default 03-bf-01-01-01-01

Success.

DGS-3000-28XMP:admin#
```

58-5 config nlb multicast_fdb

Description

This command is used to add or delete the forwarding ports for the specified NLB multicast FDB entry.

Format

config nlb multicast_fdb [<vlan_name 32> | vlanid <vlanid>] <macaddr> [add | delete] <portlist>

Parameters

<vlan_name 32> - Enter the VLAN of the NLB multicast FDB entry to be configured.
vlanid - Specifies the VLAN by the VLAN ID. **<vlanid>** - Enter the VLAN ID here.
<macaddr> - Enter the MAC address of the NLB multicast FDB entry to be configured.
add - Specifies a list of forwarding ports to be added.
delete - Specifies a list of forwarding ports to be deleted.
<portlist> - Enter the list of ports used for this configuration.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure NLB multicast MAC forwarding database:

```
DGS-3000-28XMP:admin# config nlb multicast_fdb default 03-bf-01-01-01-01 add 1-5
Command: config nlb multicast_fdb default 03-bf-01-01-01-01 add 1-5

Success.

DGS-3000-28XMP:admin#
```

58-6 delete nlb multicast_fdb

Description

This command is used to delete the NLB multicast FDB entry.

Format

delete nlb multicast_fdb [<vlan_name 32> | vlanid <vlanid>] <macaddr>

Parameters

<vlan_name 32> - Enter the VLAN of the NLB multicast FDB entry to be deleted.
vlanid - Specifies the VLAN by VLAN ID. **<vlanid>** - Enter the VLAN ID here.
<macaddr> - Enter the MAC address of the NLB multicast FDB entry to be deleted.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete NLB multicast FDB entry:

```
DGS-3000-28XMP:admin# delete nlb multicast_fdb default 03-bf-01-01-01-01
Command: delete nlb multicast_fdb default 03-bf-01-01-01-01

Success.

DGS-3000-28XMP:admin#
```

58-7 show nlb fdb

Description

This command is used to show the NLB configured entry.

Format

show nlb fdb

Parameters

None.

Restrictions

None.

Example

To display the NLB forwarding table:

```
DGS-3000-28XMP:admin# show nlb fdb
Command: show nlb fdb

 MAC Address       VLAN ID    Egress Ports
 ----------------- ---------- ----------------------------------------------
 02-BF-01-01-01-01 -          1-5

Total Entries :1

DGS-3000-28XMP:admin#
```

Chapter 59 Network Monitoring Command List

show packet ports <portlist>
show error ports <portlist>
show utilization [cpu | ports]
show utilization dram
show utilization flash
clear counters {ports <portlist>}

59-1 show packet ports

Description

This command is used to display statistics about the packets sent and received by the Switch.

Format

show packet ports <portlist>

Parameters

<portlist> - Enter a range of ports to be displayed.

Restrictions

None.

Example

To display the packets analysis for port 7:

```
DGS-3000-28XMP:admin# show packet ports 7
Command: show packet ports 7

 Port Number : 7
 ================================================================
 Frame Size/Type       Frame Counts                Frames/sec
 ---------------       ----------------------      -----------
 64                    0                           0
 65-127                0                           0
 128-255               0                           0
 256-511               0                           0
 512-1023              0                           0
 1024-1518             0                           0
 Unicast RX            0                           0
 Multicast RX          0                           0
 Broadcast RX          0                           0

 Frame Type            Total                       Total/sec
 ---------------       ----------------------      -----------
 RX Bytes              0                           0
 RX Frames             0                           0
 TX Bytes              0                           0
 TX Frames             0                           0


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

59-2 show error ports

Description

This command is used to display the error statistics for a range of ports.

Format

show errors ports <portlist>

Parameters

<portlist> - Enter a range of ports to be displayed.

Restrictions

None.

Example

To display the errors of the port:

```
DGS-3000-28XMP:admin# show error ports 3
Command: show error ports 3


 Port Number : 3
                RX Frames                                   TX Frames
                ---------                                   ---------
 CRC Error      0                    Excessive Deferral     0
 Undersize      0                    CRC Error              0
 Oversize       0                    Late Collision         0
 Fragment       0                    Excessive Collision    0
 Jabber         0                    Single Collision       0
 Drop Pkts      0                    Collision              0
 Symbol Error   0



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

59-3 show utilization

Description

This command is used to display real-time CPU or port utilization statistics.

Format

show utilization [cpu | ports]

Parameters

cpu - Specifies to display information regarding the CPU.
ports - Specifies all ports to be displayed.

Restrictions

None.

Example

To display the ports utilization:

```
DGS-3000-28XMP:admin# show utilization ports
Command: show utilization ports

 Port     TX/sec     RX/sec   Util      Port     TX/sec     RX/sec   Util
 -----  ---------- ---------- ----      -----  ---------- ---------- ----
 1      0          0          0         21     0          0          0
 2      0          0          0         22     0          0          0
 3      0          0          0         23     0          0          0
 4      0          0          0         24     0          0          0
 5      0          0          0         25     0          0          0
 6      0          0          0         26     0          0          0
 7      0          0          0         27     0          0          0
 8      0          0          0         28     0          0          0
 9      0          0          0
 10     0          0          0
 11     0          0          0
 12     0          0          0
 13     0          0          0
 14     0          0          0
 15     0          0          0
 16     0          0          0
 17     0          0          0
 18     0          0          0
 19     0          0          0
 20     0          0          0
CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

To display the CPU utilization:

```
DGS-3000-28XMP:admin# show utilization cpu
Command: show utilization cpu

CPU Utilization
-------------------------------------------------------------------------------
Five seconds -  10 %         One minute -  10 %         Five minutes -  10 %









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

59-4 show utilization dram

Description

This command is used to show DRAM memory utilization.

Format

show utilization dram

Parameters

None.

Restrictions

None.

Example

To display DRAM utilization:

```
DGS-3000-28XMP:admin# show utilization dram
Command: show utilization dram

DRAM Utilization :
        Total DRAM      : 262144    KB
        Used DRAM       : 162461    KB
        Utilization     : 61 %




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

59-5 show utilization flash

Description

This command is used to show the flash memory utilization.

Format

show utilization flash

Parameters

None.

Restrictions

None.

Example

To display FLASH utilization:

```
DGS-3000-28XMP:admin#show utilization flash
Command: show utilization flash

Flash Memory Utilization :
        Total Flash     : 29937     KB
        Used Flash      : 28834     KB
        Utilization     : 96 %



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

59-6 clear counters

Description

This command is used to clear the Switch's statistics counters.

Format

clear counters {ports <portlist>}

Parameters

ports - (Optional) Specifies a range of ports to clear. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range is separated by a dash.

<portlist> - Enter a list of ports used for the configuration here.

If no parameter is specified, system will display counters of all ports.

Restrictions

Only Administrators and Operators can issue this command.

Example

To clear the Switch's statistics counters:

```
DGS-3000-28XMP:admin# clear counters ports 7-9
Command: clear counters ports 7-9

Success.

DGS-3000-28XMP:admin#
```

Chapter 60 Network Time Protocol (NTP) Command List

enable ntp
disable ntp
config ntp access_group add [default | <ipaddr> | <network_address> | <ipv6addr> | <ipv6networkaddr>] {ignore | noserve | notrust | version | nopeer | noquery | nomodify}
config ntp access_group delete [default | <ipaddr> | <network_address> | <ipv6addr> | <ipv6networkaddr>]
config ntp authentication state [enable | disable]
config ntp authentication key add <key_id 1-255> md5 <string 32>
config ntp authentication key delete <key_id 1-255>
config ntp control_key [<key_id 1-255> | clear]
config ntp ipif <ipif_name 12> state [enable | disable]
config ntp master_stratum <value 0-15>
config ntp max_associations <value 1-64>
config ntp peer add [<ipaddr> | <ipv6addr>] {version <int 1-4> | key <key_id 1-255> | prefer | min_poll <value 3-16> | max_poll <value 4-17>}
config ntp peer delete [<ipaddr> | <ipv6addr>]
config ntp request_key [<key_id 1-255> | clear]
config ntp server add [<ipaddr> | <ipv6addr>] {version <int 1-4> | key <key_id 1-255> | prefer | min_poll <value 3-16> | max_poll <value 4-17>}
config ntp server delete [<ipaddr> | <ipv6addr>]
config ntp trusted_key <key_id 1-255>
config ntp update_calendar state [enable | disable]
show ntp
show ntp associations {detail}
show ntp status
debug ntp level <value 0-255>

60-1 enable ntp

Description

This command is used to enable the NTP function.

Format

enable ntp

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable NTP:

```
DGS-3000-28XMP:admin#enable ntp
Command: enable ntp

Success.

DGS-3000-28XMP:admin#
```

60-2 disable ntp

Description

This command is used to disable the NTP function.

Format

disable ntp

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To disable NTP:

```
DGS-3000-28XMP:admin#disable ntp
Command: disable ntp

Success.

DGS-3000-28XMP:admin#
```

60-3 config ntp access_group add

Description

This command is used to add the NTP access group. The NTP implements a general purpose Access Control List (ACL) containing address/match entries sorted first by increasing address values and then by increasing mask values. A match occurs when the bitwise AND of the mask and the packet source address is equal to the bitwise AND of the mask and address in the list. The list is searched in order with the last match found defining the restriction flags associated with the entry.

Format

config ntp access_group add [default | <ipaddr> | <network_address> | <ipv6addr> | <ipv6networkaddr>] {ignore | noserve | notrust | version | nopeer | noquery | nomodify}

Parameters

default - Specifies to use the default IPv4 (0.0.0.0/0.0.0.0) or IPv6 (::/::) address. The default IP address is always included with the lowest priority in the list.
<ipaddr> - Specifies a host IP address.
<network_address> - Specifies a network IP address.
<ipv6addr> - Specifies a host IPv6 address.
<ipv6networkaddr> - Specifies a network IPv6 address.
ignore - (Optional) Specifies to deny all packets, including NTP control queries.
noserve - (Optional) Specifies to deny all packets except NTP control queries.
notrust - (Optional) Specifies to deny packets that are not cryptographically authenticated. If the **config ntp authentication state** command is enabled, authentication is required for all packets that might mobilize an association. If the **config ntp authentication state** command is disabled, but the notrust flag is not present, an association can be mobilized no matter it is authenticated or not. If If the **config ntp authentication state** command is disabled, but the notrust flag is present, authentication is required only for the specified address/mask range.
version - (Optional) Specifies to deny packets that mismatch the current NTP version.
nopeer - (Optional) Specifies to deny packets that might mobilize an association unless authenticated. The packets include broadcast, symmetric-active and manycast server packets when a configured association does not exist. Note that this flag does not apply to packets that do not attempt to mobilize an association.
noquery - (Optional) Specifies to deny all NTP control queries.
nomodify - (Optional) Specifies to deny the NTP control queries that attempt to modify the state of the server.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To create the NTP access group with the default IPv4 address:

```
DGS-3000-28XMP:admin#config ntp access_group add default nopeer
Command: config ntp access_group add default nopeer

Success.

DGS-3000-28XMP:admin#
```

60-4 config ntp access_group delete

Description

This command is used to delete the NTP access group.

Format

config ntp access_group delete [default | <ipaddr> | <network_address> | <ipv6addr> | <ipv6networkaddr>]

Parameters

default - Specifies to use the default IPv4 (0.0.0.0/0.0.0.0) or IPv6 (::/::) address. The default IP address is always included with the lowest priority in the list.
<ipaddr> - Specifies a host IP address.
<network_address> - Specifies a network IP address.
<ipv6addr> - Specifies a host IPv6 address.
<ipv6networkaddr> - Specifies a network IPv6 address.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To remove the NTP access group:

```
DGS-3000-28XMP:admin#config ntp access_group delete default
Command: config ntp access_group delete default

Success.

DGS-3000-28XMP:admin#
```

60-5 config ntp authentication state

Description

This command is used to configure the NTP authentication state. When enabled, networking nodes will not synchronize with the Switch unless it carries one of the authentication keys specified in the **config ntp authentication key add** command.

Format

config ntp authentication state [enable | disable]

Parameters

enable - Specifies to enable the NTP authentication state.
disable - Specifies to disable the NTP authentication state.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable the NTP authentication state:

```
DGS-3000-28XMP:admin#config ntp authentication state enable
Command: config ntp authentication state enable

Success.

DGS-3000-28XMP:admin#
```

60-6 config ntp authentication key add

Description

This command is used to define an authentication key for NTP.

Format

config ntp authentication key add <key_id 1-255> md5 <string 32>

Parameters

<key_id 1-255> - Enter the NTP key ID. The value is from 1 to 255.
md5 - Specifies the authentication key type to MD5. **<string 32>** - Enter the key string here. This string can be up to 32 characters long.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To define an authentication key with the key ID “42” and key string “NTPKey”:

```
DGS-3000-28XMP:admin#config ntp authentication key add 42 md5 NTPKey
Command: config ntp authentication key add 42 md5 NTPKey

Success.

DGS-3000-28XMP:admin#
```

60-7 config ntp authentication key delete

Description

This command is used to remove an authentication key for NTP.

Format

config ntp authentication key delete <key_id 1-255>

Parameters

<key_id 1-255> - Enter the NTP key ID. The value is from 1 to 255.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To remove an authentication key for NTP:

```
DGS-3000-28XMP:admin#config ntp authentication key delete 42
Command: config ntp authentication key delete 42

Success.

DGS-3000-28XMP:admin#
```

60-8 config ntp control_key

Description

This command is used to define the key ID for NTP control messages.

Format

config ntp control_key [<key_id 1-255> | clear]

Parameters

<key_id 1-255> - Enter the NTP key ID. The value is from 1 to 255.
clear - Specifies to remove the key.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To define the key ID for NTP control messages:

```
DGS-3000-28XMP:admin#config ntp control_key 42
Command: config ntp control_key 42

Success.

DGS-3000-28XMP:admin#
```

60-9 config ntp ipif

Description

This command is used to enable or disable an IP interface to receive NTP packets.

Format

config ntp ipif <ipif_name 12> state [enable | disable]

Parameters

<ipif_name 12> - Enter the IP interface name used here. This name can be up to 12 characters long.
state - Specifies to enable or disable an IP interface to receive NTP packets. **enable** - Specifies to enable the interface. This is the default value. **disable** - Specifies to disable the interface.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable the IP interface, System, to receive NTP packets:

```
DGS-3000-28XMP:admin#config ntp ipif System state enable
Command: config ntp ipif System state enable

Success.

DGS-3000-28XMP:admin#
```

60-10 config ntp master_stratum

Description

This command is used to configure Real-Time Clock (RTC) as an NTP master clock when an external NTP is not available.

Format

config ntp master_stratum <value 0-15>

Parameters

<value 0-15> - Enter the NTP stratum number between 1 and 15. 0 prepresents to disable the function.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure a router as an NTP master clock:

```
DGS-3000-28XMP:admin#config ntp master_stratum 8
Command: config ntp master_stratum 8

Success.

DGS-3000-28XMP:admin#
```

60-11 config ntp max_associations

Description

This command is used to configure the maximum number of NTP peers and clients on the Switch.

Format

config ntp max_associations <value 1-64>

Parameters

<value 1-64> - Enter the number of NTP associations.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the maximum number of NTP associations to 20:

```
DGS-3000-28XMP:admin#config ntp max_associations 20
Command: config ntp max_associations 20

Success.

DGS-3000-28XMP:admin#
```

60-12 config ntp peer add

Description

This command is used to configure the NTP peer settings.

Format

config ntp peer add [<ipaddr> | <ipv6addr>] {version <int 1-4> | key <key_id 1-255> | prefer | min_poll <value 3-16> | max_poll <value 4-17>}

Parameters

<ipaddr> - Enter the IP address of the peer.
<ipv6addr> - Enter the IPv6 address of the peer.

version - (Optional) Specifies the NTP version number **<int 1-4>** - Enter the NTP version number from 1 to 4. The default value is 4.
key - (Optional) Specifies the authentication key. **<key_id 1-255>** - Enter the NTP key ID. The value is from 1 to 255.
prefer - (Optional) Specifies to be the preferred peer for synchronization.
min_poll - (Optional) Specifies the minimum poll interval for NTP messages. **<value 3-16>** - Enter the minimum poll interval value. This value is calculated as 2 to the power of the minimum poll interval value specified. For example, if the value specified here is 6, the minimum poll interval that will be used is 64 seconds (2^6=64).
max_poll - (Optional) Specifies the maximum poll interval for NTP messages. **<value 4-17>** - Enter the maximum poll interval value. This value is calculated as 2 to the power of the maximum poll interval value specified. For example, if the value specified here is 6, the maximum poll interval that will be used is 64 seconds (2^6=64).

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the IP address of the NTP peer to 192.168.22.33 using NTP version 3:

```
DGS-3000-28XMP:admin#config ntp peer add 192.168.22.33 version 3
Command: config ntp peer add 192.168.22.33 version 3

Success.

DGS-3000-28XMP:admin#
```

60-13 config ntp peer delete

Description

This command is used to delete the NTP peer.

Format

config ntp peer delete [<ipaddr> | <ipv6addr>]

Parameters

<ipaddr> - Enter the IP address of the peer.
<ipv6addr> - Enter the IPv6 address of the peer.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete the IP address of the NTP peer:

```
DGS-3000-28XMP:admin#config ntp peer delete 192.168.22.33
Command: config ntp peer delete 192.168.22.33

Success.

DGS-3000-28XMP:admin#
```

60-14 config ntp request_key

Description

This command is used to define the key ID for NTP mode 7 packets, used by the *ntpdc* utility program.

Format

config ntp request_key [<key_id 1-255> | clear]

Parameters

<key_id 1-255> - Enter the NTP key ID. The value is from 1 to 255.
clear - Specifies to remove the key.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To define the NTP request key:

```
DGS-3000-28XMP:admin#config ntp request_key 45
Command: config ntp request_key 45

Success.

DGS-3000-28XMP:admin#
```

60-15 config ntp server add

Description

This command is used to add the NTP server.

Format

config ntp server add [<ipaddr> | <ipv6addr>] {version <int 1-4> | key <key_id 1-255> | prefer | min_poll <value 3-16> | max_poll <value 4-17>}

Parameters

<ipaddr> - Enter the IP address of the server.

<ipv6addr> - Enter the IPv6 address of the server.
version - (Optional) Specifies the NTP version number **<int 1-4>** - Enter the NTP version number from 1 to 4. The default value is 4.
key - (Optional) Specifies the authentication key. **<key_id 1-255>** - Enter the NTP key ID. The value is from 1 to 255.
prefer - (Optional) Specifies to be the preferred server for synchronization.
min_poll - (Optional) Specifies the minimum poll interval for NTP messages. **<value 3-16>** - Enter the minimum poll interval value. This value is calculated as 2 to the power of the minimum poll interval value specified. For example, if the value specified here is 6, the minimum poll interval that will be used is 64 seconds (2^6=64).
max_poll - (Optional) Specifies the maximum poll interval for NTP messages. **<value 4-17>** - Enter the maximum poll interval value. This value is calculated as 2 to the power of the maximum poll interval value specified. For example, if the value specified here is 6, the maximum poll interval that will be used is 64 seconds (2^6=64).

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the IP address of the NTP server to 192.168.10.33 using NTP version 2:

```
DGS-3000-28XMP:admin#config ntp server add 192.168.10.33 version 2
Command: config ntp server add 192.168.10.33 version 2

Success.

DGS-3000-28XMP:admin#
```

60-16 config ntp server delete

Description

This command is used to delete the NTP server.

Format

config ntp server delete [<ipaddr> | <ipv6addr>]

Parameters

<ipaddr> - Enter the IP address of the server.
<ipv6addr> - Enter the IPv6 address of the server.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete the IP address of the NTP server:

```
DGS-3000-28XMP:admin#config ntp server delete 192.168.10.33
Command: config ntp server delete 192.168.10.33

Success.

DGS-3000-28XMP:admin#
```

60-17 config ntp trusted_key

Description

This command is used to specify the trusted key for a peer NTP system to authenticate.

Format

config ntp trusted_key <key_id 1-255>

Parameters

<key_id 1-255> - Enter the NTP key ID. The value is from 1 to 255.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the NTP trusted key:

```
DGS-3000-28XMP:admin#config ntp trusted_key 45
Command: config ntp trusted_key 45

Success.

DGS-3000-28XMP:admin#
```

60-18 config ntp update_calendar state

Description

This command is used to periodically update the hardware clock from an NTP source.

Format

config ntp update_calendar state [enable | disable]

Parameters

enable - Specifies to periodically update the hardware clock from an NTP source.

disable - Specifies to disable the feature. This is the default value.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To periodically update the hardware clock from an NTP source:

```
DGS-3000-28XMP:admin#config ntp update_calendar state enable
Command: config ntp update_calendar state enable

Success.

DGS-3000-28XMP:admin#
```

60-19 show ntp

Description

This command is used to display NTP settings.

Format

show ntp

Parameters

None.

Restrictions

None.

Example

To display display NTP settings:

```
DGS-3000-28XMP:admin#show ntp
Command: show ntp

NTP State           :Enabled
Authentication State:Enabled
NTP Update Calendar :Enabled
NTP Max Association :32

NTP Server List:

Ver Key  Poll Prefer NTP server
--- --- ----- ------ -----------------------------------
2   0    6~10 False  192.168.10.33
--- --- ----- ------ -----------------------------------

NTP Peer List:

Ver Key  Poll Prefer NTP server
--- --- ----- ------ -----------------------------------
3   0    6~10 False  192.168.22.33
--- --- ----- ------ -----------------------------------

NTP Key List:
Key ID Key Type Trusted Key Value
------ -------- ------- ----------------------------------------
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

60-20 show ntp associations

Description

This command is used to display the status of NTP associations.

Format

show ntp associations {detail}

Parameters

detail - (Optional) Specifies to display detail information about each NTP association.

Restrictions

None.

Example

To display the status of NTP associations:

```
DGS-3000-28XMP:admin#show ntp associations
Command: show ntp associations
Remote           Local          St   Poll  Reach  Delay      Offset      Disp
===============================================================================
=192.168.10.33   10.90.90.90    16   64    0      0.00000    0.000000    3.99217
+192.168.22.33   10.90.90.90    16   64    0      0.00000    0.000000    3.99217
+ Symmetric active, - Symmetric passive, = Client, * System Peer


DGS-3000-28XMP:admin#
```

To display the detail status of NTP associations:

```
DGS-3000-28XMP:admin#show ntp associations detail
Command: show ntp associations detail

Remote 192.168.10.33, Local 10.90.90.90
Our mode client, Peer mode unspec, Stratum 16, Precision -7
Leap 11, RefID [XFAC], RootDistance 0.00000, RootDispersion 0.00000
PPoll 10, HPoll 6, KeyID 0, Version 2, Association 8359
Reach 000, Unreach 3, Flash 0x1e00, Timer 1s, flags  Config
Reference Timestamp:  00000000.00000000  Thu, Feb  7 2036  6:28:16.00000
Originate Timestamp: 00000000.00000000  Thu, Feb  7 2036  6:28:16.00000
Receive Timestamp:   00000000.00000000  Thu, Feb  7 2036  6:28:16.00000
Transmit Timestamp:  00000000.00000000  Thu, Feb  7 2036  6:28:16.00000
Filter Delay:  0.00000  0.00000  0.00000  0.00000
               0.00000  0.00000  0.00000  0.00000
Filter Offset: 0.000000 0.000000 0.000000 0.000000
               0.000000 0.000000 0.000000 0.000000
Filter Order:  0        1        2        3
               4        5        6        7
Offset 0.000000, Delay 0.00000, Error Bound 3.99217, Filter Error 0.00000

Remote 192.168.22.33, Local 10.90.90.90
Our mode sym_active, Peer mode unspec, Stratum 16, Precision -7
Leap 11, RefID [XFAC], RootDistance 0.00000, RootDispersion 0.00000
PPoll 10, HPoll 6, KeyID 0, Version 3, Association 8356
Reach 000, Unreach 4, Flash 0x1e00, Timer 66s, flags  Config
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

60-21 show ntp status

Description

This command is used to display the NTP status.

Format

show ntp status

Parameters

None.

Restrictions

None.

Example

To display the NTP status:

```
DGS-3000-28XMP:admin#show ntp status
Command: show ntp status
Leap Indicator:       Unsynchronized
Stratum:              16
Precision:            -8
Root Distance:        0.00000 s
Root Dispersion:      0.00475 s
Reference ID:         [INIT]
Reference Time:       00000000.00000000  Thu, Feb  7 2036  6:28:16.00000
System Flags:         Auth Monitor NTP Kernel Stats
Jitter:               0.000000 s
Stability:            0.000 ppm
Auth Delay:           0.000000 s


DGS-3000-28XMP:admin#
```

60-22 debug ntp level

Description

This command is used to configure the NTP debug function.

Format

debug ntp level <value 0-255>

Parameters

<value 0-255> - Enter the level of the debug message. When configured to 0, the NTP debug function is disabled. The higher value is configured, the more detail debug message is.

Restrictions

Only Administrators can issue this command.

Example

To configure the value of the debug message to 1:

```
DGS-3000-28XMP:admin#debug ntp level 1
Command: debug ntp level 1

Success.

DGS-3000-28XMP:admin#
```

Chapter 61 OAM Commands

config ethernet_oam ports [<portlist> | all] [mode [active | passive] | state [enable | disable] | link_monitor [error_symbol {threshold <range 0-4294967295> | window <millisecond 1000-60000> | notify_state [enable | disable]}(1) | error_frame {threshold <range 0-4294967295> | window <millisecond 1000-60000> | notify_state [enable | disable]}(1) | error_frame_seconds {threshold <range 1-900> | window <millisecond 10000-900000> | notify_state [enable | disable]}(1) | error_frame_period {threshold <range 0-4294967295> | window <number 148810-100000000> | notify_state [enable | disable]}(1)] | critical_link_event [dying_gasp | critical_event] notify_state [enable | disable] | remote_loopback [start | stop] | received_remote_loopback [process | ignore]]
show ethernet_oam ports {<portlist>} [status | configuration | statistics | event_log {index <value_list>}]
clear ethernet_oam ports [<portlist> | all] [event_log | statistics]

61-1 config ethernet_oam ports

Description

This command is used to configure Ethernet OAM. The parameter to configure port Ethernet OAM mode operates in active or passive mode. The following two actions are allowed by ports in active mode, but disallowed by ports in passive mode: Initiate OAM discovery and start or stop remote loopback. When a port is OAM-enabled, changing the OAM mode will cause the OAM discovery to be re-started.

The command used to enable or disable port's Ethernet OAM function. The parameter enabling a port's OAM will cause the port to start OAM discovery. If a port's is active, it initiates the discovery. Otherwise it reacts to the discovery received from peer. Disabling a port's OAM will cause the port to send out a dying gasp event to peers and then disconnect the established OAM link.

The link monitoring parameter is used to configure port Ethernet OAM link monitoring error symbols. 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. The Ethernet OAM link monitoring error frames parameter provides a mechanism to detect and indicate link faults under a variety of conditions. OAM monitors the counter on 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.

The link event parameter configures the capability of the Ethernet OAM critical link event. If the capability for an event is disabled, the port will never send out the corresponding critical link event. This command is used to configure the client to process or to ignore the received Ethernet OAM remote loopback command. In remote loopback mode, all user traffic will not be processed. Ignoring the received remote loopback command will prevent the port from entering remote loopback mode.

Format

config ethernet_oam ports [<portlist> | all] [mode [active | passive] | state [enable | disable] | link_monitor [error_symbol {threshold <range 0-4294967295> | window <millisecond 1000-60000> | notify_state [enable | disable]}(1) | error_frame {threshold <range 0-4294967295> | window <millisecond 1000-60000> | notify_state [enable | disable]}(1) | error_frame_seconds {threshold <range 1-900> | window <millisecond 10000-900000> | notify_state [enable | disable]}(1) | error_frame_period {threshold <range 0-4294967295> | window <number 148810-100000000> | notify_state [enable | disable]}(1)] | critical_link_event [dying_gasp | critical_event] notify_state [enable | disable] | remote_loopback [start | stop] | received_remote_loopback [process | ignore]]

Parameters

<portlist> - Enter a range of ports to be configured.

all - Specifies all ports are to be configured.

mode - Specifies the operation mode. The default mode is active.
- **active** - Specifies to operate in active mode.
- **passive** - Specifies to operate in passive mode.

state - Specifies the OAM function status.
- **enable** - Specifies to enable the OAM function.
- **disable** - Specifies to disable the OAM function.

link_monitor - Specifies to detect and indicate link faults under a variety of conditions.
- **error_symbol** - Specifies to generate an error symbol period event to notify the remote OAM peer.
  - **threshold** - Specifies the number of symbol errors in the period that is required to be equal to or greater than in order for the event to be generated. The default value of threshold is 1 symbol error.
    - **<range 0-4294967295>** - Enter the range from 0 to 4294967295.
  - **window** - Specifies the range from 1000 to 60000 ms. The default value is 1000ms.
    - **<millisecond 1000-60000>** - Enter the range from 1000 to 60000 ms.
  - **notify_state** - Specifies the event notification status. The default state is enable.
    - **enable** -Specifies to enable event notification.
    - **disable** -Specifies to disable event notification.
- **error_frame** - Specifies the error frame.
  - **threshold** - Specifies a threshold range.
    - **<range 0-4294967295>** - Enter a threshold range between 0 and 4294967295.
  - **window** - Specifies the range from 1000 to 60000 milliseconds. The default value is 1000 milliseconds.
    - **<millisecond 1000-60000>** - Enter the range from 1000 to 60000 milliseconds.
  - **notify_state** - Specifies the event notification status. The default state is enable.
    - **enable** - Specifies to enable event notification.
    - **disable** - Specifies to disable event notification.
- **error_frame_seconds** - Specifies error frame time.
  - **threshold** - Specifies a threshold range between 1 and 900.
    - **<range 1-900>** - Enter a threshold range between 1 and 900.
  - **window** - Specifies the range from 1000 to 900000 milliseconds.
    - **<millisecond 10000-900000>** - Enter the range from 1000 to 900000 milliseconds.
  - **notify_state** - Specifies the event notification status. The default state is enable.
    - **enable** - Specifies to enable event notification.
    - **disable** - Specifies to disable event notification.
- **error_frame_period** - Specifies error frame period.
  - **threshold** - Specifies a threshold range between 0 and 4294967295.
    - **<range 0-4294967295>** -Enter a threshold range between 0 and 4294967295.
  - **window** - Specifies the range from 148810 to 100000000 milliseconds.
    - **<number 148810-100000000>** - Enter the range from 148810 to 100000000 milliseconds.
  - **notify_state** - Specifies the event notification status. The default state is enable.
    - **enable** - Specifies to enable event notification.
    - **disable** - Specifies to disable event notification.

critical_link_event - Specifies critical link event.
- **dying_gasp** - Specifies that an unrecoverable local failure condition has occurred.
- **critical_event** - Specifies that an unspecified critical event has occurred.
- **notify_state** - Specifies the event notification status. The default state is enable.
  - **enable** - Specifies to enable event notification.
  - **disable** - Specifies to disable event notification.

remote_loopback - Specifies remote loop.
- **start** - Specifies to request the peer to change to the remote loopback mode.

stop - Specifies to request the peer to change to the normal operation mode.

received_remote_loopback - Specifies receive remote loop-back.

process - Specifies to process the received Ethernet OAM remote loopback command.

ignore - Specifies to ignore the received Ethernet OAM remote loopback command. The is the default method.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure Ethernet OAM on ports 1 to 2 in active mode:

```
DGS-3000-28XMP:admin# config ethernet_oam ports 1-2 mode active
Command: config ethernet_oam ports 1-2 mode active

Success.

DGS-3000-28XMP:admin#
```

To enable Ethernet OAM on port 1:

```
DGS-3000-28XMP:admin# config ethernet_oam ports 1 state enable
Command: config ethernet_oam ports 1 state enable

Success.

DGS-3000-28XMP:admin#
```

To configure the error symbol threshold to 2 and period to 1000ms for port 1:

```
DGS-3000-28XMP:admin# 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-3000-28XMP:admin#
```

To configure the error frame threshold to 2 and period to 1000 ms for port 1:

```
DGS-3000-28XMP:admin# 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-3000-28XMP:admin#
```

To configure the error frame seconds threshold to 2 and period to 10000 ms for port 1:

```
DGS-3000-28XMP:admin# config ethernet_oam ports 1 link_monitor error_frame_seconds threshold
2 window 10000 notify_state enable
Command: config ethernet_oam ports 1 link_monitor error_frame_seconds threshold 2 window
10000 notify_state enable

Success.

DGS-3000-28XMP:admin#
```

To configure the error frame threshold to10 and period to 1000000 ms for port 1:

```
DGS-3000-28XMP:admin# 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-3000-28XMP:admin#
```

To configure a dying gasp event for port 1:

```
DGS-3000-28XMP:admin# config ethernet_oam ports 1 critical_link_event dying_gasp notify_state
enable
Command: config ethernet_oam ports 1 critical_link_event dying_gasp notify_state enable

Success.

DGS-3000-28XMP:admin#
```

To start remote loopback on port 1:

```
DGS-3000-28XMP:admin# config ethernet_oam ports 1 remote_loopback start
Command: config ethernet_oam ports 1 remote_loopback start

Success.

DGS-3000-28XMP:admin#
```

To configure the method of processing the received remote loopback command as “process” on port 1:

```
DGS-3000-28XMP:admin# config ethernet_oam ports 1 received_remote_loopback process
Command: config ethernet_oam ports 1 received_remote_loopback process

Success.

DGS-3000-28XMP:admin#
```

61-2 show ethernet_oam ports

Description

This command is used to display Ethernet OAM information, including status, configuration, statistics, and event log, on specified ports.

The status 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 mode change.
7. 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.

The event log displays Ethernet OAM event log information. The switch can buffer 1000 event logs. The event log is different from sys-log as it provides more detailed information than sys-log. Each OAM event will be recorded in both OAM event log and syslog.

Format

show ethernet_oam ports {<portlist>} [status | configuration | statistics | event_log {index <value_list>}]

Parameters

<portlist> - (Optional) Enter a range of ports to be displayed.

status - Specifies to display the Ethernet OAM status.
configuration - Specifies to display the Ethernet OAM configuration.
statistics - Specifies to display Ethernet OAM statistics.
event_log - Specifies to display the Ethernet OAM event log information. **index** - (Optional) Specifies an index range to display. **<value_list>** - (Optional) Enter an index range to display.

Restrictions

Only Administrators and Operators can issue this command.

Example

To display Ethernet OAM statistics information for port 1:

```
DGS-3000-28XMP:admin# show ethernet_oam ports 1 statistics
Command: show ethernet_oam ports 1 statistics

Port 1
------------------------------------------------------------
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-3000-28XMP:admin#
```

61-3 clear ethernet_oam ports

Description

This command is used to clear Ethernet OAM information.

Format

clear ethernet_oam ports [<portlist> | all] [event_log | statistics]

Parameters

<portlist> - Enter a range of Ethernet OAM ports to be cleared.
all - Specifies to clear all Ethernet OAM ports.
event_log - Specifies to clear Ethernet OAM event log information.
statistics - Specifies to clear Ethernet OAM statistics.

Restrictions

Only Administrators and Operators can issue this command.

Example

To clear port 1 OAM statistics:

```
DGS-3000-28XMP:admin# clear ethernet_oam ports 1 statistics
Command: clear ethernet_oam ports 1 statistics

Success.

DGS-3000-28XMP:admin#
```

To clear port 1 OAM events:

```
DGS-3000-28XMP:admin# clear ethernet_oam ports 1 event_log
Command: clear ethernet_oam ports 1 event_log

Success.

DGS-3000-28XMP:admin#
```

Chapter 62 Password Recovery Command List

enable password_recovery
disable password_recovery
show password_recovery

62-1 enable password_recovery

Description

This command is used to enable the password recovery mode.

Format

enable password_recovery

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To enable the password recovery mode:

```
DGS-3000-28XMP:admin# enable password_recovery
Command: enable password_recovery

Success.

DGS-3000-28XMP:admin#
```

62-2 disable password_recovery

Description

This command is used to disable the password recovery mode.

Format

disable password_recovery

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To disable the password recovery mode:

```
DGS-3000-28XMP:admin# disable password_recovery
Command: disable password_recovery

Success.

DGS-3000-28XMP:admin#
```

62-3 show password_recovery

Description

This command is used to display the password recovery state.

Format

show password_recovery

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To display the password recovery state:

```
DGS-3000-28XMP:admin# show password_recovery
Command: show password_recovery

 Running Configuration  : Enabled
 NV-RAM Configuration   : Enabled

DGS-3000-28XMP:admin#
```

Chapter 63 Peripherals Command List

show device_status
show environment
config temperature threshold {high <temperature -500-500> | low <temperature -500-500>}(1)
config temperature [trap | log] state [enable | disable]

63-1 show device_status

Description

This command is used to display the current power status and fans in the system. Only the failed fan(s) will display in the fan field. For example, the DGS-3000-28XMP has two fans on the right side. If two fans are working normally, the Right Fan field displays “OK”. If fan 2 fails, the Right Fan field displays “2 Fail”.

Format

show device_status

Parameters

None.

Restrictions

None.

Example

To show device status:

```
DGS-3000-28XMP:admin#show device_status
Command: show device_status

    External Power: None
    Right Fan     : OK

DGS-3000-28XMP:admin#
```

63-2 show environment

Description

This command is used to display the temperature trap/log state, external power setting, current temperature, and high/low warning temperature threshold setting. Combined, these form the environment settings.

Format

show environment

Parameters

None.

Restrictions

None.

Example

To display the environment settings:

```
DGS-3000-28XMP:admin#show environment
Command: show environment

Temperature Trap State      : Enabled
Temperature Log State       : Enabled
External Power      : None
Current Temperature(Celsius) :   25
High Warning Temperature Threshold(Celsius) :    79
Low Warning Temperature Threshold(Celsius)  :    11

DGS-3000-28XMP:admin#
```

63-3 config temperature threshold

Description

This command is used to configure the warning threshold for high and low temperature.

Format

config temperature threshold {high <temperature -500-500> | low <temperature -500-500>}(1)

Parameters

high - Specifies the high threshold value. The high threshold must bigger than the low threshold. **<temperature -500-500>** - Enter the high threshold temperature.
low - Specifies the low threshold value. **<temperature -500-500>** - Enter the low threshold temperature.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the warning temperature threshold:

```
DGS-3000-28XMP:admin# config temperature threshold high 80
Command: config temperature threshold high 80

Success.

DGS-3000-28XMP:admin#
```

63-4 config temperature

Description

This command is used to configure the trap state for temperature warning event.

Format

config temperature [trap | log] state [enable | disable]

Parameters

trap - Specifies the trap state for the warning temperature event.
log - Specifies the log state for the warning temperature event.
state - Specifies the trap or log state for the warning temperature event. **enable** - Specifies to enable trap or log state for warning temperature event. The default state is enabled. **disable** - Specifies to disable trap or log state for warning temperature event.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the warning temperature trap state:

```
DGS-3000-28XMP:admin# config temperature trap state enable
Command: config temperature trap state enable

Success.

DGS-3000-28XMP:admin#
```

Chapter 64 Ping Command List

ping [<ipaddr> | <domain_name 255>] {times <value 1-255> | timeout <sec 1-99>}
ping6 [<ipv6addr> | <domain_name 255>] {times <value 1-255>| size <value 1-6000>| timeout <sec 1-99>}

64-1 ping

Description

This command is used to send Internet Control Message Protocol (ICMP) echo messages to a remote IP address. The remote IP address will then “echo” or return the message. This is used to confirm connectivity between the Switch and the remote device.

Format

ping [<ipaddr> | <domain_name 255>] {times <value 1-255> | timeout <sec 1-99>}

Parameters

<ipaddr> - Enter the IP address of the host.
<domain_name 255> - Enter the domain name of the host.
times - (Optional) Specifies the number of individual ICMP echo messages to be sent. A value of 0 will send an infinite ICMP echo messages. The maximum value is 255. The default is 0, indicating infinity. Press "CTRL+C” to break the ping test. **<value 1-255>** - Enter the number of individual ICMP echo messages to be sent here. This value must be between 1 and 255.
timeout - (Optional) Specifies 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. **<sec 1-99>** - Enter the time-out period here. This value must be between 1 and 99 seconds.

Restrictions

None.

Example

To send 4 ICMP echo messages to “10.51.17.1”:

```
DGS-3000-28XMP:admin# ping 10.51.17.1 times 4
Command: ping 10.51.17.1 times 4

Reply from 10.51.17.1, time<10ms
Reply from 10.51.17.1, time<10ms
Reply from 10.51.17.1, time<10ms
Reply from 10.51.17.1, time<10ms

Ping Statistics for 10.51.17.1
Packets: Sent =4, Received =4, Lost =0

DGS-3000-28XMP:admin#
```

64-2 ping6

Description

This command is used to send 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.

Format

ping6 [<ipv6addr> | <domain_name 255>] {times <value 1-255>| size <value 1-6000>| timeout <sec 1-99>}

Parameters

<ipv6addr> - Enter the IPv6 address here. If the IPv6 address is a link-local address or a multicast address, the IP interface name needs to be specified in the following format: IPv6Address%Interface-ID.

<domain_name 255> - Enter the domain name of the host.

times - (Optional) Specifies the number of individual ICMP echo messages to be sent. A value of 0 will send an infinite ICMP echo messages. The maximum value is 255. The default is 0, indicating infinity. Press "CTRL+C” to break the ping test.

- **<value 1-255>** - Enter the number of individual ICMP echo messages to be sent here. This value must be between 1 and 255.

size - (Optional) Specifies the size of the test packet.

- **<value 1-6000>** - Enter the size of the test packet here. This value must be between 1 and 6000.

timeout - (Optional) Specifies the time-out period while waiting for a response from the remote device.

- **<sec 1-99>** - Enter the time-out period here. This value must be between 1 and 99 seconds. The default is 1 second.

Restrictions

None.

Example

To send ICMP echo message to “3000::1” for 4 times:

```
DGS-3000-28XMP:admin# ping6 3000::1 times 4
Command: ping6 3000::1 times 4

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

Ping Statistics for 3000::1
Packets: Sent =4, Received =4, Lost =0

DGS-3000-28XMP:admin#
```

Chapter 65 Port Security Command List

config port_security system max_learning_addr [<max_lock_no 1-3328> | no_limit]
config port_security ports [<portlist>| all] [{admin_state [enable | disable] | max_learning_addr <max_lock_no 0-3328> | action [drop | shutdown] | lock_address_mode [permanent | deleteontimeout | deleteonreset]}(1) | {vlan [<vlan_name 32> | vlanid <vidlist>] max_learning_addr [<max_lock_no 0-3328> | no_limit]}(1)]
config port_security vlan [<vlan_name 32> | vlanid <vidlist>] max_learning_addr [<max_lock_no 0-3328> | no_limit]
delete port_security_entry [vlan <vlan_name 32> | vlanid <vlanid 1-4094>] mac_address <macaddr>
clear port_security_entry {ports [<portlist> | all] {[vlan <vlan_name 32> | vlanid <vidlist>]}}
show port_security_entry {ports {<portlist>} {[vlan <vlan_name 32> | vlanid <vidlist>]}}
show port_security {ports {<portlist>} {[vlan <vlan_name 32> | vlanid <vidlist>]}}
enable port_security trap_log
disable port_security trap_log

65-1 config port_security system max_learning_addr

Description

This command is used to set the maximum number of port security entries that can be authorized system wide.

There are four levels of limitations on the learned entry number; for the entire system, for a port, for a VLAN, and for a specific VLAN on a port. If any limitation is exceeded, the new entry will be discarded.

The setting for system level maximum learned users must be greater than the total of maximum learned users allowed on all ports.

Format

config port_security system max_learning_addr [<max_lock_no 1-3328> | no_limit]

Parameters

<max_lock_no 1-3328> - Specifies the maximum number of port security entries that can be learned by the system. If the setting is smaller than the number of current learned entries on all enabled ports, the command will be rejected. This value must be between 1 and 3328.
no_limit - Specifies that there is no limitation on the number of port security entries that can be learned by the system. This is the default option.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the maximum number of port security entries on the Switch to be 256:

```
DGS-3000-28XMP:admin# config port_security system max_learning_addr 256
Command: config port_security system max_learning_addr 256

Success.

DGS-3000-28XMP:admin#
```

65-2 config port_security ports

Description

This command is used to configure the admin state, the maximum number of addresses that can be learnt and the lock address mode.

There are four levels that limit the number of learned entries; the entire system, a port, a VLAN, and a specific VLAN on a port. If any limitation is exceeded, the new entry will be discarded.

Format

config port_security ports [<portlist> | all] [{admin_state [enable | disable] | max_learning_addr <max_lock_no 0-3328> | action [drop | shutdown] | lock_address_mode [permanent | deleteontimeout | deleteonreset]}(1) | {vlan [<vlan_name 32> | vlanid <vidlist>] max_learning_addr [<max_lock_no 0-3328> | no_limit]}(1)]

Parameters

<portlist> - Enter the list of ports used for this configuration here.

all - Specifies that all ports will be configured.

admin_state - Specifies the state of the port security function on the port.

- **enable** - Specifies to enable the port security function on the port.
- **disable** - Specifies to disable the port security function on the port. By default, the setting is disabled.

max_learning_addr - Specifies the maximum number of port security entries that can be learned on this port. If the value is set to 0, it means that no user can be authorized by the port security function on this port. If the setting is smaller than the number of current learned entries on the port, the command will be rejected. The default value is 32.

- **<max_lock_no 0-3328>** - Enter the maximum number of port security entries that can be learned here. This value must be between 0 and 3328.

action - Specifies the action to be taken when the number of learned, secure MAC address reaches the maximum on the port.

- **drop** - When the number of learned, secure MAC address reaches the maximum on the port, new entries will be dropped. This is the default setting.
- **shutdown** - When the number of learned, secure MAC address reaches the maximum on the port, the port will be shut down and enter error-disabled state immediately. The port state is recovered only by enabling the port manually. The shutdown action only applies to port level security setting.

lock_address_mode - Specifies the lock address mode.

- **permanent** - Specifies that the address will never be deleted unless the user removes it manually, the VLAN of the entry is removed, the port is removed from the VLAN, or port security is disabled on the port where the address resides.
- **deleteontimeout** - Specifies that this entry will be removed if the entry is idle for the specified aging time.
- **deleteonreset** - Specifies that this address will be removed if the Switch is reset or rebooted. Events that cause permanent entries to be deleted also apply to the deleteonreset entries. This is the default mode.

vlan - Specifies the VLAN name used here.

- **<vlan_name 32>** - Enter the VLAN name used here. This name can be up to 32 characters long.

vlanid - Specifies the VLAN ID used here.

<vidlist> - Enter the VLAN ID used here.

max_learning_addr - Specifies the maximum learning address value.

<max_lock_no 0-3328> - Enter the maximum learning address value here. This value must be between 0 and 3328.

no_limit - Specifies that the maximum learning address value will be set to no limit.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the port-based port security setting so that the maximum number of port security entries is restricted to 10, and the lock address mode is set to permanent on port 6:

```
DGS-3000-28XMP:admin# config port_security ports 6 admin_state enable max_learning_addr 10
lock_address_mode permanent
Command: config port_security ports 6 admin_state enable max_learning_addr 10
lock_address_mode permanent

Success.

DGS-3000-28XMP:admin#
```

65-3 config port_security vlan

Description

This command is used to set the maximum number of port security entries that can be learned on a specific VLAN.

There are four levels that limit the number of learned entries; the entire system, a port, a VLAN, and a specific VLAN on a port. If any limitation is exceeded, the new entry will be discarded.

Format

config port_security vlan [<vlan_name 32> | vlanid <vidlist>] max_learning_addr [<max_lock_no 0-3328> | no_limit]

Parameters

<vlan_name 32> - Enter the VLAN name here. This name can be up to 32 characters long.

vlanid - Specifies a list of VLANs by VLAN ID.

<vidlist> - Enter the VLAN ID list here.

max_learning_addr - Specifies the maximum number of port security entries that can be learned by this VLAN. If this parameter is set to 0, it means that no user can be authorized on this VLAN. If the setting is lower than the number of current learned entries on the VLAN, the command will be rejected.

<max_lock_no 0-3328> - Enter the maximum number of port security entries that can be learned here. This value must be between 0 and 3328.

no_limit - Specifies that there is no limitation on the number of port security entries that can be learned by a specific VLAN. This is the default.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the maximum number of VLAN-based port security entries on VLAN 1 to be 64:

```
DGS-3000-28XMP:admin# config port_security vlan vlanid 1 max_learning_addr 64
Command: config port_security vlan vlanid 1 max_learning_addr 64

Success.

DGS-3000-28XMP:admin#
```

65-4 delete port_security_entry

Description

This command is used to delete a port security entry.

Format

delete port_security_entry [vlan <vlan_name 32> | vlanid <vlanid 1-4094>] mac_address <macaddr>

Parameters

vlan - Specifies the VLAN by VLAN name. **<vlan_name 32>** - Enter the VLAN name here. This name can be up to 32 characters long.
vlanid - Specifies the VLAN by VLAN ID. **<vlanid 1-4094>** - Enter the VLAN ID list here. This value must be between 1 and 4094.
mac_address - Specifies the MAC address of the entry. **<macaddr>** - Enter the MAC address used here.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete the port security entry with a MAC address of 00-00-00-00-00-01 on VLAN 1:

```
DGS-3000-28XMP:admin# delete port_security_entry vlanid 1 mac_address 00-00-00-00-00-01
Command: delete port_security_entry vlanid 1 mac_address 00-00-00-00-00-01

Success.

DGS-3000-28XMP:admin#
```

65-5 clear port_security_entry

Description

This command is used to clear the MAC entries learned by the port security function.

Format

clear port_security_entry {ports [<portlist> | all] {[vlan <vlan_name 32> | vlanid <vidlist>]}}

Parameters

ports - (Optional) Specifies a range of ports to be configured. **<portlist>** - Enter the port security entries learned on the specified port will be cleared. **all** - Specifies that all the port security entries learned by the system will be cleared.
vlan - (Optional) Specifies that the port security entries learned on the specified VLANs will be cleared. **<vlan_name 32>** - Enter the VLAN name here. This name can be up to 32 characters long.
vlanid - (Optional) Specifies a list of VLANs by VLAN ID. **<vidlist>** - Enter the VLAN ID list here.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To clear the port security entries on port 6:

```
DGS-3000-28XMP:admin# clear port_security_entry ports 6
Command: clear port_security_entry ports 6

Success.

DGS-3000-28XMP:admin#
```

65-6 show port_security_entry

Description

This command is used to display the port security entries.

If more than one parameter is selected, only the entries matching all the selected parameters will be displayed.

If the user specifies ports and VLAN (either the VLAN name or VLAN ID list), only the entries matching all the parameters will be displayed.

Format

show port_security_entry {ports {<portlist>} {[vlan <vlan_name 32> | vlanid <vidlist>]}}

Parameters

ports - (Optional) Specifies the range of ports that will display the port security entries.

<portlist> - (Optional) Enter the list of ports used for this configuration here.

vlan - (Optional) Specifies the name of the VLAN that the port security settings will be displayed for.

<vlan_name 32> - Enter the VLAN name here. This name can be up to 32 characters long.

vlanid - (Optional) Specifies the ID of the VLAN that the port security entries will be displayed for.

<vidlist> - Enter the VLAN ID list here.

If no parameter is specified, the entries on all ports will be displayed.

Restrictions

None.

Example

To show all the port security entries:

```
DGS-3000-28XMP:admin# show port_security_entry
Command: show port_security_entry

MAC Address          VID   Port   Lock Mode
-----------------  ----  -----  ---------------
00-00-00-00-00-01  1      25     DeleteOnTimeout

Total Entries: 1

DGS-3000-28XMP:admin#
```

65-7 show port_security

Description

This command is used to display the port security related information, including state, maximum learned addresses and lock address mode on a port and/or on a VLAN.

If both ports and vlanid (or vlan_name) are specified, configurations matching any of these parameters will be displayed.

Format

show port_security {ports {<portlist>} {[vlan <vlan_name 32> | vlanid <vidlist>]}}

Parameters

ports - (Optional) Specifies the range of ports that will show their configuration.

<portlist> - (Optional) Enter the list of ports used for this configuration here.

vlan - (Optional) Specifies the name of the VLAN that will show its configuration.

<vlan_name 32> - Enter the VLAN name here. This name can be up to 32 characters long.

vlanid - (Optional) Specifies the ID of the VLAN that will show its configuration.

<vidlist> - Enter the VLAN ID list here.

If no parameter is specified, the entries on all ports will be displayed.

Restrictions

None.

Example

To display the global configuration of port security:

```
DGS-3000-28XMP:admin# show port_security
Command: show port_security

 Port Security Trap/Log        : Disabled
 System Maximum Address        : 256

 VLAN Configuration (Only VLANs with limitation are displayed)
 VID   VLAN Name                         Max. Learning Addr.
 ----  --------------------------------  ------------------
 1     default                           64

DGS-3000-28XMP:admin#
```

65-8 enable port_security trap_log

Description

This command is used to enable port security traps/logs. When this command is enabled, if there's a new MAC that violates the pre-defined port security configuration, a trap will be sent out with the MAC and port information and the relevant information will be logged.

Format

enable port_security trap_log

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable a port security trap:

```
DGS-3000-28XMP:admin# enable port_security trap_log
Command: enable port_security trap_log

Success.

DGS-3000-28XMP:admin#
```

65-9 disable port_security trap_log

Description

This command is used to disable a port security trap/log. If the port security trap is disabled, no trap will be sent out for MAC violations, and no log will be recorded.

Format

disable port_security trap_log

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To prevent a port security trap from being sent from the Switch:

```
DGS-3000-28XMP:admin# disable port_security trap_log
Command: disable port_security trap_log

Success.

DGS-3000-28XMP:admin#
```

Chapter 66 Power over Ethernet (PoE) Command List (DGS-3000-28LP and DGS-3000-28XMP Only)

config poe system {power_limit <value 37-193> | power_disconnect_method [deny_next_port | deny_low_priority_port] | legacy_pd [enable | disable]} (DGS-3000-28LP Only)
config poe system {power_limit <value 37-370> | power_disconnect_method [deny_next_port | deny_low_priority_port] | legacy_pd [enable | disable]} (DGS-3000-28XMP Only)
config poe ports [all | <portlist>] { state [enable | disable]| [time_range <range_name 32> | clear_time_range]| priority [critical | high | low] | power_limit [class_0 | class_1 | class_2 | class_3 | user_define <value 1000-35000>]}
config poe pd_alive ports [all | <portlist>] {state [enable | disable] | pd ip <ipaddr> | interval <sec 10-300> | retry <int 0-5> | waiting_time <sec 30-300> | action [reset | notify | both]}
show poe system
show poe ports {<portlist>}
show poe pd_alive ports {<portlist>}

66-1 config poe system

Description

This command is used to configure the parameters for the PoE system-wide function.

Format

config poe system {power_limit <value 37-193> | power_disconnect_method [deny_next_port | deny_low_priority_port] | legacy_pd [enable | disable]} (DGS-3000-28LP Only)

config poe system {power_limit <value 37-370> | power_disconnect_method [deny_next_port | deny_low_priority_port] | legacy_pd [enable | disable]} (DGS-3000-28XMP Only)

Parameters

power_limit - (Optional) Specifies to configure the power budget of PoE system. The range of value which can be specified is determined by the system.

- **<value 37-193>** - Enter the power limit value here. This value must be between 37 and 193. **(DGS-3000-28LP Only)**
- **<value 37-370>** - Enter the power limit value here. This value must be between 37 and 370. **(DGS-3000-28XMP Only)**

power_disconnect_method - (Optional) Specifies to configure the disconnection method that will be used when the power budget is close to being exhaused. When the system attempts to supply power to a new port, if the power budget is insufficient to do this, PoE controller will initiate port disconnection procedure to prevent overloading the power supply.

- **deny_next_port** - Specifies that the port with max port number will be denied regardless of its priority. When this is configured, the power provision will not utilize the system's maximum power. There is a 19 W safe margin. That is, when the system has only 19 W remaining, this power cannot be utilized.
- **deny_low_priority_port** - Specifies that if there are ports that have been supplied power that have a priority lower than the new port, the port with the lowest priority will be disconnected. This process will continue until enough power is released for the new port. When this is configured, the power provision can utilize the

system's maximum power.
legacy_pd - Specifies to configure the legacy PD's detection status. **enable** - Specifies that the legacy PD's detection status will be enabled. **disable** - Specifies that the legacy PDs detection status will be disabled.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To config PoE system-wise was setting:

```
DGS-3000-28XMP:admin# config poe system power_limit 150 power_disconnect_method
deny_low_priority_port
Command: config poe system power_limit 150 power_disconnect_method deny_low_priority_port

Success.

DGS-3000-28XMP:admin#
```

66-2 config poe ports

Description

This command is used to configure PoE port settings.

Based on 802.3af, there are 4 kinds of PD classes, class 0, class 1, class 2, and class 3. The power consumption ranges for them are 0.44~12.95 W, 0.44~3.84 W, 3.84~6.49 W, and 6.49~12.95 W, respectively.

The power limit for each class is a little more than the power consumption range for the class. Power loss on the cable is taken into account. The typical power limit values for each class are listed below:

Class 0: 15400 mW

Class 1: 4000 mW

Class 2: 7000 mW

Class 3: 15400 mW

Other than these four pre-defined settings, users can directly specify any value that the chip supported, Normally, the minimum setting is 1000 mW, and the maximum setting is 15400 mW for 802.3af and >=35000 mW for 802.3at.

NOTE: If the switch fails to supply power to the Powered Device (PD) that supports the IEEE 802.3at standard,

1. Check if the PD connected to the port supports the IEEE 802.3at standard.
2. Manually configure the corresponding port's power limit value to 30 watts using the **config poe ports [all | <portlist>] power_limit user_define 30000** command.

Format

config poe ports [all | <portlist>] { state [enable | disable] | [time_range <range_name 32> | clear_time_range] | priority [critical | high | low] | power_limit [class_0 | class_1 | class_2 | class_3 | user_define <value 1000-35000>]}

Parameters

ports - Specifies the list of ports whose setting is under configuration.

all - Specifies that all the ports will be included in this configuration.

<portlist> - Enter the list of ports used for this configuration here.

state - (Optional) Specifies to enable or disable the power supply to the powered device of the specific ports.

enable - Specifies that state will be enabled.

disable - Specifies that state will be disabled.

time_range - (Optional) Specifies the time range that applies to the port of the PoE. If time range is configured, the power can only be supplied during the period specified by time range.

<range_name 32> - Enter the time range name here. This name can be up to 32 characters long.

clear_time_range - (Optional) Specifies to remove the time range.

priority - (Optional) Specifies the priority that the system attempts to supply power to the specific ports. There are three levels of priority that can be selected, critical, high, and low. When multiple ports happen to have the same level of priority, the port ID will be used to determine the priority. The lower port ID has higher priority. The setting of priority will affect the order of how power is supplied. Whether the disconnect_method is set to deny_low_priority_port, priority of port will be used by the system to manage to supply power to ports.

critical - Specifies that the priority will be set to critical.

high - Specifies that the priority will be set to high.

low - Specifies that the priority will be set to low.

power_limit - (Optional) Specifies to configure the per-port power limit. If a port exceeds its power limit, it will be shut down.

class_0 - Specifies that the power limit will be set to class 0.

class_1 - Specifies that the power limit will be set to class 1.

class_2 - Specifies that the power limit will be set to class 2.

class_3 - Specifies that the power limit will be set to class 3.

user_define - (Optional) Specifies that a user defined per-port power limit will be used.

<value 1000-35000> - Enter the user defined per-port power limit here. This value must be between 1000 and 35000.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To config PoE port:

```
DGS-3000-28XMP:admin# config poe ports 1-4 state enable priority critical power_li
mit class_1
Command: config poe ports 1-4 state enable priority critical power_limit class_1

Success.

DGS-3000-28XMP:admin# config poe ports 5 state enable priority critical power_lim
it user_define 1000
Command: config poe ports 5 state enable priority critical power_limit user_define 1000

Success.

DGS-3000-28XMP:admin#
```

66-3 config poe pd_alive ports

Description

This command is used to enable or disable the PD alive check function for the PD connected to the PoE port.

Format

config poe pd_alive ports [all | <portlist>] {state [enable | disable] | pd ip <ipaddr> | interval <sec 10-300> | retry <int 0-5> | waiting_time <sec 30-300> | action [reset | notify | both]}

Parameters

all - Specifies that all the ports will be used for this configuration.
<portlist> - Enter a list of ports to be used.
state - (Optional) Specifies to the state of the PD alive check function. **enable** - Specifies to enable the PD alive check function. **disable** - Specifies to disable the PD alive check function
pd - (Optional) Specifies the IP address of the target PD for the Switch executing the ping action. **ip** - Specifies the IP address. **<ipaddr>** - Enter the IP address
interval - (Optional) Specifies the interval for the system to issue ping requests to detect the target PD. **<sec 10-300>** - Enter the interval in seconds. The value is from 10 to 300 seconds.
retry - (Optional) Specifies the retry counts of ping requests when PD has no response. **<int 0-5>** - Enter the retry counts. The value is from 0 to 5.
waiting_time - (Optional) Specifies the waiting time for PD to recover from rebooting. **<sec 30-300>** - Enter the waiting time in seconds. The value is from 30 to 300.
action - (Optional) Specifies the action of the system when PD does not reply the ping request. **reset** - Specifies to reset the PoE port state. **notify** - Specifies to send logs and traps to notify the administrator. **both** - Specifies to send log and trap first, and then reset the PoE port state.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable the PoE PD alive check function on port 2:

```
DGS-3000-28XMP:admin#config poe pd_alive ports 2 state enable pd ip 10.90.90.92 interval 30
retry 3 waiting_time 60 action both
Command: config poe pd_alive ports 2 state enable pd ip 10.90.90.92 interval 30 retry 3
waiting_time 60 action both

Success.

DGS-3000-28XMP:admin#
```

66-4 show poe system

Description

This command is used to display the setting and actual values of the whole PoE system.

Format

show poe system

Parameters

None.

Restrictions

None.

Example

To display PoE system:

```
DGS-3000-28XMP:admin#show poe system
Command: show poe system

PoE System Information
-------------------------------------------------
Power Limit                : 370(Watts)
Power Consumption          : 0(Watts)
Power Remained             : 351(Watts)
Power Disconnection Method : Deny Next Port
Detection Legacy PD        : Disabled









If Power Disconnection Method is set to deny next port, then the system can not utilize out
of its maximum power capacity. The maximum unused watt is 19W.

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

66-5 show poe ports

Description

This command is used to display the setting and actual values of the PoE port.

Format

show poe ports {<portlist>}

Parameters

<portlist> - (Optional) Specifies a list of ports to be displayed.
If no parameter is specified, the system will display the status for all ports.

Restrictions

None.

Example

To display PoE port:

```
DGS-3000-28XMP:admin# show poe ports 1-6
Command: show poe ports 1-6

Port   State     Priority  Power Limit(mW)     Time Range
       Class     Power(mW) Voltage(decivolt)   Current(mA)
       Status
================================================================================
1      Enabled   Low       16200(Class 0)
       0         0         0                   0
       OFF  : Interim state during line detection
2      Enabled   Low       16200(Class 0)
       0         0         0                   0
       OFF  : Interim state during line detection
3      Enabled   Low       16200(Class 0)
       0         0         0                   0
       OFF  : Interim state during line detection
4      Enabled   Low       16200(Class 0)
       0         0         0                   0
       OFF  : Interim state during line detection
5      Enabled   Low       16200(Class 0)
       0         0         0                   0
       OFF  : Interim state during line detection
6      Enabled   Low       16200(Class 0)
       0         0         0                   0
       OFF  : Interim state during line detection
CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

66-6 show poe pd_alive ports

Description

This command is used to display PD alive check settings.

Format

show poe pd_alive ports {<portlist>}

Parameters

<portlist> - (Optional) Specifies a list of ports to be displayed.
If no parameter is specified, the system will display PD alive check settings for all ports.

Restrictions

None.

Example

To display PD alive check settings:

```
DGS-3000-28XMP:admin#show poe pd_alive ports
Command: show poe pd_alive ports

Port : 1
------------------------------------------
    PD Alive State              : Disabled
    PD IP Address               : 0.0.0.0
    Poll Interval               : 30
    Retry Count                 : 2
    Waiting Time                : 90
    Action                      : Both
    Status                      : -

Port : 2
------------------------------------------
    PD Alive State              : Enabled
    PD IP Address               : 10.90.90.92
    Poll Interval               : 30
    Retry Count                 : 3
    Waiting Time                : 60
    Action                      : Both
    Status                      : Normal



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

Chapter 67 Power Saving Command List

config power_saving mode {link_detection | led | port | hibernation} [enable | disable]
config power_saving hibernation [[add | delete] time_range <range_name 32> | clear_time_range]
config power_saving led [[add | delete] time_range <range_name 32> | clear_time_range]
config power_saving port [<portlist> | all] [[add | delete] time_range <range_name 32> | clear_time_range]
config led state [enable | disable]
show power_saving {link_detection | led | port | hibernation}
show led

67-1 config power_saving mode

Description

This command is used to set the power saving state.

For link detection function, they apply to the ports with copper media. If the power saving link detection state is enabled, the power is saved by the following mechanism:

- When no links are detected on the port, the port will automatically turn off and will only wake up the second a single link pulse is sent. While the port is turned off, a simple energy-detect circuit will continuously monitor energy on the cable. The moment energy is detected; the port will turn on fully as to the IEEE specification's requirements. The power saving function is performed while no link is detected and it will not affect the port capabilities while the link is up.

If the power saving state of port is disabled, all power saving schedules of port will not take effect.

If the power saving state of port LED is disabled, all power saving schedules of port LED will not take effect.

If the power saving state of system hibernation is disabled, all power saving schedules of system hibernation will not take effect.

Format

config power_saving mode {link_detection | led | port | hibernation} [enable | disable]

Parameters

link_detection - (Optional) Specifies the power saving link detection state.
led - (Optional) Specifies to configure the power saving state of port LED.
port - (Optional) Specifies to configure the power saving state of port.
hibernation - (Optional) Specifies to configure the power saving state of system hibernation.
enable - Specifies to enable power saving state.
disable - Specifies to disable power saving state.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable the power saving state of port, hibernation:

```
DGS-3000-28XMP:admin#config power_saving mode port hibernation enable
Command: config power_saving mode port hibernation enable

Success.

DGS-3000-28XMP:admin#
```

67-2 config power_saving hibernation

Description

This command is used to add or delete the power saving schedule on system hibernation. When the system enters hibernation mode, the Switch changes to a low power state and is idle. It shuts down all the ports, and all network function does not work. Only the console connection will work via the RS232 port.

Format

config power_saving hibernation [[add | delete] time_range <range_name 32> | clear_time_range]

Parameters

add - Specifies to add a time range.
delete - Specifies to delete a time range.
time_range - Specifies the name of the time range. **<range_name32>** - Enter a name for maximum 32 characters.
clear_time_range - Specifies to clear all the time range of system hibernation.

Restrictions

Only Administrators and Operators can issue this command.

Example

To add a time range named “range_1” on system hibernation:

```
DGS-3000-28XMP:admin#config power_saving hibernation add time_range range_1
Command: config power_saving hibernation add time_range range_1

Success.

DGS-3000-28XMP:admin#
```

67-3 config power_saving led

Description

This command is used to add or delete the power saving schedule on the LED of all ports. When any schedule is up, all port’s LED will be turned off even device’s LED working on PoE mode.

NOTE: The port LED admin state (configured using the command 'config led state') gets high priority. If the port LED admin state is disabled, all ports' LED will always be turned off. Currently only three time ranges are supported.

Format

config power_saving led [[add | delete] time_range <range_name 32> | clear_time_range]

Parameters

add - Specifies to add a time range.
delete - Specifies to delete a time range.
time_range - Specifies the name of the time range. **<range_name32>** - Enter a name for maximum 32 characters.
clear_time_range - Specifies to clear all the time range of port LED.

Restrictions

Only Administrators and Operators can issue this command.

Example

To add a time range named "range_1" on port LED:

```
DGS-3000-28XMP:admin#config power_saving led add time_range range_1
Command: config power_saving led add time_range range_1

Success.

DGS-3000-28XMP:admin#
```

67-4 config power_saving port

Description

This command is used to add or delete the power saving schedule on the port. When any schedule is up, the specific port will be shut down (disabled).

NOTE: The port's admin state has high priority. If the port's admin state is disabled, the specific port will always be shut down (disabled). Currently only three time ranges are supported.

Format

config power_saving port [<portlist> | all] [[add | delete] time_range <range_name 32> | clear_time_range]

Parameters

<portlist> - Enter a range of ports.
all - Specifies all ports.
add - Specifies to add a time range.
delete - Specifies to delete a time range.

time_range - Specifies the name of the time range. **<range_name32>** - Enter a name for maximum 32 characters.
clear_time_range - Specifies to clear all the time range of port.

Restrictions

Only Administrators and Operators can issue this command.

Example

To add a time range named “range_1” on port 1:

```
DGS-3000-28XMP:admin#config power_saving port 1 add time_range range_1
Command: config power_saving port 1 add time_range range_1

Success.

DGS-3000-28XMP:admin#
```

To delete a time range named “range_2” on port 1:

```
DGS-3000-28XMP:admin#config power_saving port 1 delete time_range range_2
Command: config power_saving port 1 delete time_range range_2

Success.

DGS-3000-28XMP:admin#
```

67-5 config led state

Description

This command is used to configure the LED admin state of all ports. When the port LED admin state is disabled, the LEDs of all ports are turned off. If the port LED admin state is enabled, the port LEDs are controlled by the ports' link status.

Format

config led state [enable | disable]

Parameters

enable - Specifies to enable the LED admin state of all ports.
disable - Specifies to disable the LED admin state of all ports.

Restrictions

Only Administrators and Operators can issue this command.

Example

To disable the LED admin state:

```
DGS-3000-28XMP:admin#config led state disable
Command: config led state disable

Success.

DGS-3000-28XMP:admin#
```

67-6 show power_saving

Description

This command is used to display the current state of power saving.

Format

show power_saving {link_detection | led | port | hibernation}

Parameters

link_detection - (Optional) Displays the link detection configuration of power saving.
led - (Optional) Displays the port LED configuration of power saving.
port - (Optional) Displays the port configuration of power saving.
hibernation - (Optional) Displays the system hibernation configuration of power saving.
If no parameter is specified, all configurations of power saving will be displayed.

Restrictions

None.

Example

To display the power saving function setting:

```
DGS-3000-28XMP:admin#show power_saving
Command: show power_saving

 Function Version: 3.00

 Link Detection State: Enabled

 Power Saving Configuration On System Hibernation
 ------------------------------------------------
 State: Enabled
 Time Range
 --------------------------------
 range_1

 Power Saving Configuration On Port LED
 --------------------------------------
 State: Disabled
 Time Range
 --------------------------------
 range_1

 Power Saving Configuration On Port
 ----------------------------------------
 State: Enabled
 Port       Time Range
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

67-7 show led

Description

This command is used to display the LED admin state.

Format

show led

Parameters

None.

Restrictions

None.

Example

To display the LED admin state:

```
DGS-3000-28XMP:admin#show led
Command: show led

 Port LED State: Disabled

DGS-3000-28XMP:admin#
```

Chapter 68 PPPoE Circuit ID Insertions Command List

config pppoe circuit_id_insertion state [enable | disable]
config pppoe circuit_id_insertion ports <portlist> {state [enable | disable] | circuit_id [mac | ip | udf <string 32>]}(1)
show pppoe circuit_id_insertion
show pppoe circuit_id_insertion ports {<portlist>}

68-1 config pppoe circuit_id_insertion state

Description

This command is used to enable or disable PPPoE circuit ID insertion function. When both port and global state are 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 insert circuit ID contains the following information: Client MAC address, Device ID and Port number. By default, Switch IP address is used as the device ID to encode the circuit ID option.

Format

config pppoe circuit_id_insertion state [enable | disable]

Parameters

enable - Specifies to enable the PPPoE circuit ID insertion on the Switch.
disable - Specifies to disable the PPPoE circuit ID insertion on the Switch. This is the default.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable the PPPoE circuit insertion state:

```
DGS-3000-28XMP:admin# config pppoe circuit_id_insertion state enable
Command: config pppoe circuit_id_insertion state enable

Success.

DGS-3000-28XMP:admin#
```

68-2 config pppoe circuit_id_insertion ports

Description

This command is used to configure port's PPPoE Circuit ID insertion function. When the port's state and the global state are enabled, the system will insert the Circuit ID TAG to the received PPPoE discovery initiation and request

packet if the TAG is absent, and remove the Circuit ID TAG from the received PPPoE offer and session confirmation packet.

Format

config pppoe circuit_id_insertion ports <portlist> {state [enable | disable] | circuit_id [mac | ip | udf <string 32>]}(1)

Parameters

<portlist> - Specifies a list of ports to be configured.
state - Specifies to enable or disable port's PPPoE circuit ID insertion function. The default setting is enable. **enable** - Specifies to enable port's PPPoE circuit ID insertion function. **disable** - Specifies to disable port's PPPoE circuit ID insertion function.
circuit_id - Specifies to configure the device ID part for encoding of the circuit ID option. **mac** - Specifies to use the MAC address of the Switch to encode the circuit ID option. **ip** - Specifies to use the Switch's IP address will be used to encode the circuit ID option. This is the default. **udf** - Specifies a user-defined string to be used to encode the circuit ID option. **<string 32>** - Enter a string with the maximum length of 32.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable port 5 PPPoE circuit ID insertion function:

```
DGS-3000-28XMP:admin# config pppoe circuit_id_insertion ports 5 state enable
Command: config pppoe circuit_id_insertion ports 5 state enable

Success.

DGS-3000-28XMP:admin#
```

68-3 show pppoe circuit_id_insertion

Description

This command is used to display PPPoE circuit ID insertion status.

Format

show pppoe circuit_id_insertion

Parameters

None.

Restrictions

None.

Example

To display PPPoE circuit ID insertion status:

```
DGS-3000-28XMP:admin# show pppoe circuit_id_insertion
Command: show pppoe circuit_id_insertion

Global PPPoE State: Enabled


DGS-3000-28XMP:admin#
```

68-4 show pppoe circuit_id_insertion ports

Description

This command is used to display Switch's port PPPoE Circuit ID insertion configuration.

Format

show pppoe circuit_id_insertion ports {<portlist>}

Parameters

<portlist> - (Optional) Specifies a list of ports to be displayed.

Restrictions

None.

Example

To display port 2-5 PPPoE circuit ID insertion configuration:

```
DGS-3000-28XMP:admin# show pppoe circuit_id_insertion ports  2-5
Command: show pppoe circuit_id_insertion ports 2-5

Port State    Circuit ID
---- -------- -------------------------------------------
2    Enabled  Switch IP
3    Enabled  Switch IP
4    Enabled  Switch IP
5    Enabled  Switch IP


DGS-3000-28XMP:admin#
```

Chapter 69 Protocol VLAN Command List

create dot1v_protocol_group group_id <id> {group_name <name 32>}
config dot1v_protocol_group [group_id <id> | group_name <name 32>] [add protocol [ethernet_2 | ieee802.3_snap | ieee802.3_llc] <protocol_value> | delete protocol [ethernet_2 | ieee802.3_snap | ieee802.3_llc] <protocol_value>]
delete dot1v_protocol_group [group_id <id> | group_name <name 32> | all]
show dot1v_protocol_group {[group_id <id> | group_name <name 32>]}
config port dot1v ports [<portlist> | all] [add protocol_group [group_id <id> | group_name <name 32>] [vlan <vlan_name 32> | vlanid <id>] {priority <value 0-7>} | delete protocol_group [group_id <id> | all]]
show port dot1v {ports <portlist>}

69-1 create dot1v_protocol_group group_id

Description

This command is used to create a protocol group for protocol VLAN function.

Format

create dot1v_protocol_group group_id < id> {group_name <name 32>}

Parameters

<id> - Enter the group ID for protocol VLAN here.
group_name - (Optional) Specifies the name of the protocol group. The maximum length is 32 chars. **<name 32>** - Enter the group name here. This name can be up to 32 characters long.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To create a protocol group:

```
DGS-3000-28XMP:admin# create dot1v_protocol_group group_id 10 group_name General_Group
Command: create dot1v_protocol_group group_id 10 group_name General_Group

Success.

DGS-3000-28XMP:admin#
```

69-2 config dot1v_protocol_group

Description

This command is used to add a protocol to a protocol group. The selection of a protocol can be a pre-defined protocol type or a user-defined protocol.

Format

config dot1v_protocol_group [group_id <id> | group_name <name 32>] [add protocol [ethernet_2 | ieee802.3_snap | ieee802.3_llc] <protocol_value> | delete protocol [ethernet_2 | ieee802.3_snap | ieee802.3_llc] <protocol_value>]

Parameters

group_id - Specifies the ID of the protocol group which is used to identify a set of protocols.
- **<id>** - Enter the group ID used here.

group_name - Specifies the name of the protocol group.
- **<name 32>** - Enter the group name here. This name can be up to 32 characters long.

add - Specifies that the protocol will be added to the specified group.

delete - Specifies that the protocol will be removed from the specified group.

protocol - Specifies the protocol value is used to identify a protocol of the frame type specified.
- **ethernet_2** - Specifies that the Ethernet 2 protocol will be used.
- **ieee802.3_snap** - Specifies that the IEEE 802.3 Snap protocol will be used.
- **ieee802.3_llc** - Specifies that the IEEE 802.3 LLC protocol will be used.
  - **<protocol_value>** - Enter the protocol value here.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To add a protocol ipv6 to protocol group 10:

```
DGS-3000-28XMP:admin# config dot1v_protocol_group group_id 10 add protocol ethernet_2 86dd
Command: config dot1v_protocol_group group_id 10 add protocol ethernet_2 86DD

Success.

DGS-3000-28XMP:admin#
```

69-3 delete dot1v_protocol_group

Description

This command is used to delete a protocol group.

Format

delete dot1v_protocol_group [group_id <id> | group_name <name 32> | all]

Parameters

group_id - Specifies the group ID to be deleted.
- **<id>** - Enter the group ID used here.

group_name - Specifies the name of the group to be deleted.

<name 32> - Enter the group name here. This name can be up to 32 characters long.
all - Specifies that all the protocol group will be deleted.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete protocol group 100:

```
DGS-3000-28XMP:admin# delete dot1v_protocol_group group_id 100
Command: delete dot1v_protocol_group group_id 100

Success.

DGS-3000-28XMP:admin#
```

69-4 show dot1v_protocol_group

Description

This command is used to display the protocols defined in a protocol group.

Format

show dot1v_protocol_group {[group_id <id> | group_name <name 32>]}

Parameters

group_id - (Optional) Specifies the ID of the group to be displayed. **<id>** - Enter the group ID used here.
group_name - (Optional) Specifies the name of the protocol group to be displayed. **<name 32>** - Enter the group name here. This name can be up to 32 characters long.
If no parameter is specified, all the configured protocol groups will be displayed.

Restrictions

None.

Example

To display the protocol group ID 10:

```
DGS-3000-28XMP:admin# show dot1v_protocol_group group_id 10
Command: show dot1v_protocol_group group_id 10

Protocol Group ID Protocol Group Name              Frame Type     Protocol Value
----------------- -------------------------------- -------------- --------------
10                General_Group                    EthernetII     86DD

Total Entries: 1

DGS-3000-28XMP:admin#
```

69-5 config port dot1v

Description

This command is used to assign the VLAN for untagged packets ingress from the port list based on the protocol group configured. This assignment can be removed by using the **delete protocol_group** parameter.

When priority is not specified in the command, the port default priority will be the priority for those untagged packets classified by the protocol VLAN.

Format

config port dot1v ports [<portlist> | all] [add protocol_group [group_id <id> | group_name <name 32>] [vlan <vlan_name 32> | vlanid <id>] {priority <value 0-7>} | delete protocol_group [group_id <id> | all]]

Parameters

<portlist> - Enter a list of ports used for the configuration here.
all - Specifies that all the ports will be used for this configuration.
add - Specifies that the group specified will be added.
protocol_group - Specifies that parameters for the group will follow.
group_id - Specifies the group ID of the protocol group. **<id>** - Enter the group ID used here.
group_name - Specifies the name of the protocol group. **<name 32>** - Enter the name of the group used here. This name can be up to 32 characters long.
vlan - The VLAN that is to be associated with this protocol group on this port. **<vlan_name 32>** - Enter the name of the VLAN here. This name can be up to 32 characters long.
vlanid - Specifies the VLAN ID. **<id>** - Enter the VLAN ID used here.
priority - (Optional) Specifies the priority to be associated with the packet which has been classified to the specified VLAN by the protocol. **<value 0-7>** - Enter the priority value here. This value must be between 0 and 7.
delete - Specifies that the group specified will be deleted.
protocol_group - Specifies that parameters for the group will follow.
group_id - Specifies the group ID of the protocol group. **<id>** - Enter the group ID used here. **all** - Specifies that all the groups will be deleted.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the group ID 10 on port 3 to be associated with VLAN marketing-1:

```
DGS-3000-28XMP:admin# config port dot1v ports 3 add protocol_group group_id 10 vlan
marketing-1
Command: config port dot1v ports 3 add protocol_group group_id 10 vlan marketing-1

Success.

DGS-3000-28XMP:admin#
```

69-6 show port dot1v

Description

This command is used to display the VLAN to be associated with ingress untagged packets on a port based on the protocol group.

Format

show port dot1v {ports <portlist>}

Parameters

ports - (Optional) Specifies a range of ports to be displayed. **<portlist>** - Enter a list of ports used for the configuration here.
If no parameter is specified, information for all ports will be displayed.

Restrictions

None.

Example

The example display the protocol VLAN information for ports 1:

```
DGS-3000-28XMP:admin# show port dot1v ports 1
Command: show port dot1v ports 1

Port: 1
 Protocol Group ID     VLAN Name                          Protocol Priority
 -------------------   --------------------------------   -----------------
 1                     default                            -
 2                     VLAN2                              -
 3                     VLAN3                              -
 4                     VLAN4                              -

Success.

DGS-3000-28XMP:admin#
```

Chapter 70 QinQ Command List

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

70-1 enable qinq

Description

This command is used to enable QinQ. When QinQ is enabled, all network port roles will be NNI ports and outer TPID will be set to 0x88A8; all existing static VLANs will run as S-VLAN; all dynamic learned L2 address will be cleared; all dynamic registered VLAN entries will be cleared; and GVRP will be disabled.

To run GVRP on the Switch, the administrator should enable GVRP manually. In QinQ mode, GVRP protocol will employ reserve address 01-80-C2-00-00-0D.

Format

enable qinq

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable QinQ:

```
DGS-3000-28XMP:admin# enable qinq
Command: enable qinq

Success.

DGS-3000-28XMP:admin#
```

70-2 disable qinq

Description

This command is used to disable the QinQ. When QinQ is disabled, all dynamic learned L2 addresses will be cleared, all dynamic registered VLAN entries will be cleared, and GVRP will be disabled.

To run GVRP on the Switch, the administrator should enable GVRP manually.

Format

disable qinq

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To disable QinQ:

```
DGS-3000-28XMP:admin# disable qinq
Command: disable qinq

Success.

DGS-3000-28XMP:admin#
```

70-3 config qinq inner_tpid

Description

This command is used to configure the inner TPID of the system. The inner TPID is used to decide if the ingress packet is c-tagged. Inner tag TPID is per system configurable.

Format

config qinq inner_tpid <hex 0x1-0xffff>

Parameters

<hex 0x1-0xffff> - Enter the inner-TPID of the system here.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the inner TPID in the system to 0x9100:

```
DGS-3000-28XMP:admin# config qinq inner_tpid 0x9100
Command: config qinq inner_tpid 0x9100

Success.

DGS-3000-28XMP:admin#
```

70-4 config qinq ports

Description

This command is used to configure the QinQ port's parameters.

Format

config qinq ports [<portlist> | all] {role [uni | nni] | missdrop [enable | disable] | outer_tpid <hex 0x1-0xffff> | add_inner_tag [<hex 0x1-0xffff> | disable]}(1)

Parameters

<portlist> - Enter the list of ports to be configured here.
all - Specifies that all the ports will be used for the configuration.
role - Specifies the port role in QinQ mode. **uni** - Specifies that the port is connecting to the customer network. **nni** - Specifies that the port is connecting to the service provider network.
missdrop - Specifies the state of the miss drop of ports option. **enable** - Specifies that the miss drop of ports option will be enabled. **disable** - Specifies that the miss drop of ports option will be disabled.
outer_tpid - Specifies the outer-TPID of a port. **<hex 0x1-0xffff>** - Enter the outer-TPID value used here.
add_inner_tag - Specifies to add an inner tag for ingress untagged packets. If set, the inner tag will be added for the ingress untagged packets and therefore the packets that egress to the NNI port will be double tagged. If disable, only the s-tag will be added for ingress untagged packets. **<hex 0x1-0xffff>** - Enter the inner tag value used here. **disable** - Specifies that the add inner tag option will be disabled.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure port list 1-4 as NNI port and set the TPID to 0x88A8:

```
DGS-3000-28XMP:admin# config qinq ports 1-4 role nni outer_tpid 0x88A8
Command: config qinq ports 1-4 role nni outer_tpid 0x88A8

Success.

DGS-3000-28XMP:admin#
```

70-5 show qinq

Description

This command is used to display the global QinQ status.

Format

show qinq

Parameters

None.

Restrictions

None.

Example

To display the global QinQ status:

```
DGS-3000-28XMP:admin# show qinq
Command: show qinq

 QinQ Status : Enabled

DGS-3000-28XMP:admin#
```

70-6 show qinq inner_tpid

Description

This command is used to display the inner-TPID of a system.

Format

show qinq inner_tpid

Parameters

None.

Restrictions

None.

Example

To display the inner-TPID of a system:

```
DGS-3000-28XMP:admin# show qinq inner_tpid
Command: show qinq inner_tpid

 Inner TPID: 0x9100


DGS-3000-28XMP:admin#
```

70-7 show qinq ports

Description

This command is used to display the QinQ configuration of the ports.

Format

show qinq ports {<portlist>}

Parameters

<portlist> - (Optional) Enter the list of ports to be displayed here.

Restrictions

None.

Example

To show the QinQ mode for ports 1-2:

```
DGS-3000-28XMP:admin# show qinq ports 1-2
Command: show qinq ports 1-2


Port ID:    1
------------------------------------------------------------
  Role:                     NNI
  Miss Drop:                Disabled
  Outer Tpid:               0x8100
  Add Inner Tag:            Disabled

Port ID:    2
------------------------------------------------------------
  Role:                     NNI
  Miss Drop:                Disabled
  Outer Tpid:               0x8100
  Add Inner Tag:            Disabled

DGS-3000-28XMP:admin#
```

70-8 create vlan_translation ports

Description

This command is used to create a VLAN translation rule. This setting will not be effective when the QinQ mode is disabled.

This configuration is only effective for a UNI port. At UNI port, the ingress C-VLAN tagged packets will be translated to S-VLAN tagged packets by adding or replacing according the configured rule. The S-VLAN Tag of egress packets at this port will be recovered to C-VLAN Tag or stripped.

Format

create vlan_translation ports [<portlist> | all] [add cvid <vidlist> | replace cvid <vlanid 1-4094>] svid <vlanid 1-4094> {priority <priority 0-7>}

Parameters

<portlist> - Enter the list of ports to be configured here.
all - Specifies that all the ports will be used for the configuration.
add - Specifies to add an S-Tag to the packet. **cvid** - Specifies the customer VLAN ID used. **<vidlist>** - Enter the customer VLAN ID used here.
replace - Specifies to replace the C-Tag with the S-Tag. **cvid** - Specifies the customer VLAN ID used. **<vlanid 1-4094>** - Enter the customer VLAN ID used here.
svid - Specifies the service provider VLAN ID used. **<vlanid 1-4094>** - Enter the service provider VLAN ID used here.
priority - (Optional) Specifies to assign an 802.1p priority to the S-Tag. If the priority is not specified, the priority of the ports will be set to S-TAG by default. **<priority 0-7>** - Enter the 802.1p S-Tag priority value here. This value must be between 0 and 7.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To replace the C-Tag in which the CVID is 20, with the S-Tag and the S-VID is 200 at UNI Port 1:

```
DGS-3000-28XMP:admin# create vlan_translation ports 1 replace cvid 20 svid 200
Command: create vlan_translation ports 1 replace cvid 20 svid 200

Success.

DGS-3000-28XMP:admin#
```

To add S-Tag, when the S-VID is 300, to a packet in which the CVID is 30 at UNI Port 1:

```
DGS-3000-28XMP:admin# create vlan_translation ports 1 add cvid 30 svid 300
Command: create vlan_translation ports 1 add cvid 30 svid 300

Success.

DGS-3000-28XMP:admin#
```

70-9 delete vlan_translation ports

Description

This command is used to delete translation relationships between the C-VLAN and the S-VLAN.

Format

delete vlan_translation ports [<portlist> | all] {cvid <vidlist>}

Parameters

<portlist> - Enter the list of ports to be configured here.
all - Specifies that all the ports will be used for the configuration.
cvid - (Optional) Specifies the rules for the specified CVIDs. If the CVID is not specified, all rules configured for the port will be deleted. **<vidlist>** - Enter the CVID value here.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete a VLAN translation rule on ports 1-4:

```
DGS-3000-28XMP:admin# delete vlan_translation ports 1-4
Command: delete vlan_translation ports 1-4

Success.

DGS-3000-28XMP:admin#
```

70-10 show vlan_translation

Description

This command is used to display the existing C-VLAN-based VLAN translation rules.

Format

show vlan_translation {[ports <portlist> | cvid <vidlist>]}

Parameters

ports – (Optional) Specifies a list of ports to be displayed. **<portlist>** - Enter the list of ports to be displayed here.
cvid - (Optional) Specifies the rules for the specified CVIDs. **<vidlist>** - Enter the CVID value used here.

Restrictions

None.

Example

To show C-VLANs based on VLAN translation rules in the system:

```
DGS-3000-28XMP:admin# show vlan_translation
Command: show vlan_translation

Port    CVID       SPVID      Action    Priority
-----   --------   --------   -------   ---------
1       20         200        Replace   -
1       30         300        Add       -

 Total Entries: 2

DGS-3000-28XMP:admin#
```

Chapter 71 Quality of Service (QoS) Command List

config bandwidth_control [<portlist> | all] {rx_rate [no_limit | <value 64-10240000>] | tx_rate [no_limit | <value 64-10240000>]}
show bandwidth_control {<portlist>}
config per_queue bandwidth_control {ports [<portlist> | all]} <cos_id_list 0-7> {{min_rate [no_limit | <value 64-10240000>]} max_rate [no_limit | <value 64-10240000>]}(1)
show per_queue bandwidth_control {<portlist>}
config scheduling {ports [<portlist> | all]} <class_id 0-7> [strict | weight <value 1-127>]
config scheduling_mechanism {ports [<portlist> | all]} [strict | wrr | wdrr]
show scheduling {<portlist>}
show scheduling_mechanism {<portlist>}
config 802.1p user_priority <priority 0-7> <class_id 0-7>
show 802.1p user_priority
config 802.1p default_priority [<portlist> | all] <priority 0-7>
show 802.1p default_priority {<portlist>}
enable hol_prevention
disable hol_prevention
show hol_prevention
config 802.1p map {[<portlist> | all]} 1p_color <priority_list> to [green | red | yellow]
show 802.1p map 1p_color {<portlist>}
config dscp trust [<portlist> | all] state [enable | disable]
show dscp trust {<portlist>}
config dscp map {[<portlist> | all]} [dscp_priority <dscp_list> to <priority 0-7> | dscp_dscp <dscp_list> to <dscp 0-63> | dscp_color <dscp_list> to [green | red | yellow]]
show dscp map {<portlist>} [dscp_priority | dscp_dscp | dscp_color] {dscp <dscp_list>}

71-1 config bandwidth_control

Description

This command is used to configure the port bandwidth limit control.

Format

config bandwidth_control [<portlist> | all] {rx_rate [no_limit | <value 64-10240000>] | tx_rate [no_limit | <value 64-10240000>]}

Parameters

<portlist> - Enter a range of ports to be configured.
all - Specifies that all the ports will be used for this configuration.

rx_rate - (Optional) Specifies the limitation applied to receive data rate.

- **no_limit** - Specifies that there is no limit on receiving bandwidth of the configured ports. The actual bandwidth will be an adjusted value based on the user specified bandwidth. The actual limit may be equal to the user specified limit, but will not exceed it. The actual limit recognized by the device, will be displayed when the command is executed.
- **<value 64-10240000>** - Enter the receiving data rate here. This value must be between 64 and 10240000 Kbps.

tx_rate - (Optional) Specifies the limitation applied to transmit data rate.

- **no_limit** - Specifies that there is no limit on port TX bandwidth. The actual bandwidth will be an adjusted value based on the user specified bandwidth. The actual limit may be equal to the user specified limit, but will not exceed it. The actual limit recognized by the device, will be displayed when the command is executed.
- **<value 64-10240000>** - Enter the transmitting data rate here. This value must be between 64 and 10240000 Kbps.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the port bandwidth:

```
DGS-3000-28XMP:admin#config bandwidth_control 1-10 rx_rate 100
Command: config bandwidth_control 1-10 rx_rate 100

 Granularity: RX: 64, TX: 64. Actual Rate: RX: 64.

Success.

DGS-3000-28XMP:admin#
```

71-2 show bandwidth_control

Description

This command is used to display the port bandwidth configurations.

The bandwidth can also be assigned by the RADIUS server through the authentication process. If RADIUS server has assigned the bandwidth, then the RADIUS-assigned bandwidth will be the effective bandwidth. The authentication with the RADIUS sever can be per port or per user. For per-user authentication, there may be multiple bandwidth control values assigned when there are multiple users attached to this specific port. In this case, the largest assigned bandwidth value will be applied to the effective bandwidth for this specific port.

NOTE: Only devices that support MAC-based VLAN can provide per user authentication.

Format

show bandwidth_control {<portlist>}

Parameters

<portlist> - (Optional) Specifies a range of ports to be displayed.
If no parameter is specified, system will display all ports bandwidth configurations.

Restrictions

None.

Example

To display port bandwidth control table:

```
DGS-3000-28XMP:admin# show bandwidth_control 1-10
Command: show bandwidth_control 1-10

Bandwidth Control Table

 Port   RX Rate       TX Rate       Effective RX       Effective TX
        (Kbit/sec)    (Kbit/sec)    (Kbit/sec)         (Kbit/sec)
 -----  ----------    ----------    ----------------   ----------------
 1      No Limit      64            No Limit           64
 2      No Limit      64            No Limit           64
 3      No Limit      64            No Limit           64
 4      No Limit      64            No Limit           64
 5      No Limit      64            No Limit           64
 6      No Limit      64            No Limit           64
 7      No Limit      64            No Limit           64
 8      No Limit      64            No Limit           64
 9      No Limit      64            No Limit           64
 10     No Limit      64            No Limit           64


DGS-3000-28XMP:admin#
```

71-3 config per_queue bandwidth_control

Description

This command is used to configure per-port CoS bandwidth control.

Format

config per_queue bandwidth_control {ports [<portlist> | all]} <cos_id_list 0-7> {{min_rate [no_limit | <value 64-10240000>]} max_rate [no_limit | <value 64-10240000>]}(1)

Parameters

ports - (Optional) Specifies a range of ports to be configured. If not specified, all ports will be configured. **<portlist>** - Enter the list of ports used for this configuration here. **all** - Specifies that all the ports will be used for this configuration.
<cos_id_list 0-7> - Specifies a list of priority queues. The priority queue number is ranged from 0 to 7.
min_rate - (Optional) Specifies the minimum rate at which the above specified class will be allowed to receive

packets.

no_limit - Specifies that there will be no limit on the rate of packets received by the above specified class.

<value 64-10240000> - Specifies the packet limit, in Kbps, that the above ports will be allowed to receive. If the specified rate is not a multiple of the minimum granularity, the rate will be adjusted.

max_rate - Specifies the maximum rate at which the above specified class will be allowed to transmit packets.

no_limit - Specifies that there will be no limit on the rate of packets received by the above specified class.

<value 64-10240000> - Specifies the packet limit, in Kbps, that the above ports will be allowed to receive. If the specified rate is not a multiple of the minimum granularity, the rate will be adjusted.

Restrictions

Only Administrators can issue this command.

Example

To configure the ports 1-10 CoS bandwidth queue 1 min rate to 130 and max rate to 100000:

```
DGS-3000-28XMP:admin# config per_queue bandwidth_control ports 1-10 1 min_rate 130 max_rate
1000
Command: config per_queue bandwidth_control ports 1-10 1 min_rate 130 max_rate 1000

 Granularity: TX: 64. Actual Rate: MIN: 128, MAX: 960.

Success.
```

71-4 show per_queue bandwidth_control

Description

This command is used to display per-port CoS bandwidth control settings.

Format

show per_queue bandwidth_control {<portlist>}

Parameters

<portlist> - (Optional) Specifies a range of ports to be displayed.

If no parameter is specified, system will display all ports CoS bandwidth configurations.

Restrictions

None.

Example

Display per-port CoS bandwidth control table:

```
DGS-3000-28XMP:admin# show per_queue bandwidth_control 10
Command: show per_queue bandwidth_control 10

Queue Bandwidth Control Table On Port: 10

Queue     Min Rate(Kbit/sec)     Max Rate(Kbit/sec)
0         640                    No Limit
1         640                    No Limit
2         640                    No Limit
3         640                    No Limit
4         No Limit               No Limit
5         No Limit               No Limit
6         No Limit               No Limit
7         No Limit               No Limit

DGS-3000-28XMP:admin#
```

71-5 config scheduling

Description

This command is used to configure the traffic scheduling mechanism for each CoS queue.

Format

config scheduling {ports [<portlist> | all]} <class_id 0-7> [strict | weight <value 1-127>]

Parameters

ports - (Optional) Specifies a range of ports to be configured. If not specified, all ports will be configured. **<portlist>** - Enter the list of ports used for this configuration here. **all** - Specifies that all the ports will be used for this configuration.
<class_id 0-7> - Enter the 8 hardware priority queues. The 8 hardware priority queues are identified by number from 0 to 7 with the 0 queue being the lowest priority.
strict - Specifies that the queue will operate in strict mode.
weight - Specifies the weights for weighted round robin. **<value 1-127>** - Enter the weights for weighted round robin value here. This value must be between 1 and 127.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the traffic scheduling CoS queue 1 to weight 25 on port 10:

```
DGS-3000-28XMP:admin# config scheduling ports 10 1 weight 25
Command: config scheduling ports 10 1 weight 25

Success.

DGS-3000-28XMP:admin#
```

71-6 config scheduling_mechanism

Description

This command is used to configure the traffic scheduling mechanism for each CoS queue.

Format

config scheduling_mechanism {ports [<portlist> | all]} [strict | wrr | wdrr]

Parameters

ports - (Optional) Specifies a range of ports to be configured. If not specified, all ports will be configured. **<portlist>** - Enter the list of ports used for this configuration here. **all** - Specifies that all the ports will be used for this configuration.
strict - Specifies that all queues operate in strict mode. The highest class of service is the first to process traffic. That is, the highest class of service will finish before other queues empty.
wrr - Specifies to use the weighted round-robin algorithm to handle packets in an even distribution in priority classes of service..
wdrr - Specifies to use the weighted deficit round-robin algorithm to handle packets in an even distribution in priority classes of service.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the traffic scheduling mechanism for each CoS queue:

```
DGS-3000-28XMP:admin# config scheduling_mechanism strict
Command: config scheduling_mechanism strict

Success.

DGS-3000-28XMP:admin#
```

To configure the traffic scheduling mechanism for CoS queue on port 1:

```
DGS-3000-28XMP:admin# config scheduling_mechanism ports 1 strict
Command: config scheduling_mechanism ports 1 strict

Success.

DGS-3000-28XMP:admin#
```

71-7 show scheduling

Description

This command is used to display the current traffic scheduling parameters.

Format

show scheduling {<portlist>}

Parameters

<portlist> - (Optional) Specifies a range of ports to be displayed.
If no parameter is specified, the scheduling configuration of all ports will be displayed.

Restrictions

None.

Example

To display the traffic scheduling parameters for each CoS queue on port 1(take eight hardware priority queues for example):

```
DGS-3000-28XMP:admin# show scheduling 1
Command: show scheduling 1


QOS Output Scheduling On Port: 1
Class ID  Weight
--------  ------
Class-0   1
Class-1   2
Class-2   3
Class-3   4
Class-4   5
Class-5   6
Class-6   7
Class-7   8


DGS-3000-28XMP:admin#
```

71-8 show scheduling_mechanism

Description

This command is used to show the traffic scheduling mechanism.

Format

show scheduling_mechanism {<portlist>}

Parameters

<portlist> - (Optional) Specifies a range of ports to be displayed.
If no parameter is specified, the scheduling mechanism configuration of all ports will be displayed.

Restrictions

None.

Example

To show scheduling mechanism:

```
DGS-3000-28XMP:admin# show scheduling_mechanism
Command: show scheduling_mechanism

Port    Mode
-----   ------
1       Strict
2       Strict
3       Strict
4       Strict
5       Strict
6       Strict
7       Strict
8       Strict
9       Strict
10      Strict
11      Strict
12      Strict
13      Strict
14      Strict
15      Strict
16      Strict
17      Strict
18      Strict
19      Strict
20      Strict
21      Strict
22      Strict
23      Strict
24      Strict
25      Strict
26      Strict
27      Strict
28      Strict


DGS-3000-28XMP:admin#
```

71-9 config 802.1p user_priority

Description

This command is used to map the 802.1p user priority of an incoming packet to one of the eight hardware queues available on the Switch.

Format

config 802.1p user_priority <priority 0-7> <class_id 0-7>

Parameters

<priority 0-7> - Enter the 802.1p user priority you want to associate with the **<class_id 0-7>** queue.
<class_id 0-7> - Enter the number of the Switch's hardware priority queue. The switch has 8 hardware priority queues available. They are numbered between 0 (the lowest priority) and 7 (the highest priority).

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the 802.1p user priority:

```
DGS-3000-28XMP:admin# config 802.1p user_priority 1 3
Command: config 802.1p user_priority 1 3

Success.

DGS-3000-28XMP:admin#
```

71-10 show 802.1p user_priority

Description

This command is used to display 802.1p user priority for ports.

Format

show 802.1p user_priority

Parameters

None.

Restrictions

None.

Example

To display the 802.1p user priority:

```
DGS-3000-28XMP:admin# show 802.1p user_priority
Command: show 802.1p user_priority

QOS Class of Traffic:
Priority-0  ->  <Class-2>
Priority-1  ->  <Class-0>
Priority-2  ->  <Class-1>
Priority-3  ->  <Class-3>
Priority-4  ->  <Class-4>
Priority-5  ->  <Class-5>
Priority-6  ->  <Class-6>
Priority-7  ->  <Class-7>

DGS-3000-28XMP:admin#
```

71-11 config 802.1p default_priority

Description

This command is used to configure the 802.1p default priority settings on the Switch. If an untagged packet is received by the Switch, the priority configured with this command will be written to the packet's priority field.

Format

config 802.1p default_priority [<portlist> | all] <priority 0-7>

Parameters

<portlist> - Enter a range of ports for which the default priority is to be configured. That is, a range of ports for which all untagged packets received will be assigned the priority specified below. The port list is specified by listing the beginning port number on the Switch, separated by a colon. Then highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash.
all - Specifies that the command apply to all ports on the Switch.
<priority 0-7> - Enter the priority value (0 to 7) assigned to untagged packets received by the Switch or a range of ports on the Switch.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the 802.1p default priority settings on the Switch:

```
DGS-3000-28XMP:admin# config 802.1p default_priority all 5
Command: config 802.1p default_priority all 5

Success.

DGS-3000-28XMP:admin#
```

71-12 show 802.1p default_priority

Description

This command is used to display the current configured default priority settings on the Switch.

The default priority can also be assigned by the RADIUS server through the authentication process. The authentication with the RADIUS sever can be per port or port user. For per port authentication, the priority assigned by RADIUS server will be the effective port default priority. For per user authentication, the priority assigned by RADIUS will not be the effective port default priority whereas it will become the priority associated with MAC address.

NOTE: Only devices supporting MAC-based VLAN can provide per user authentication.

Format

show 802.1p default_priority {<portlist>}

Parameters

<portlist> - (Optional) Specifies a range of ports to be displayed.
If no parameter is specified, all ports for 802.1p default priority will be displayed.

Restrictions

None.

Example

To display 802.1p default priority:

```
DGS-3000-28XMP:admin# show 802.1p default_priority  1-10
Command: show 802.1p default_priority 1-10

Port       Priority      Effective Priority
----       -----------   ------------------
1          5             5
2          5             5
3          5             5
4          5             5
5          5             5
6          5             5
7          5             5
8          5             5
9          5             5
10         5             5

DGS-3000-28XMP:admin#
```

71-13 enable hol_prevention

Description

This command is used to enable head of line prevention on the Switch.

Format

enable hol_prevention

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable HOL prevention on the Switch:

```
DGS-3000-28XMP:admin#enable hol_prevention
Command: enable hol_prevention

Success.

DGS-3000-28XMP:admin#
```

71-14 disable hol_prevention

Description

This command is used to disable head of line prevention on the Switch.

Format

disable hol_prevention

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To disable HOL prevention on the Switch:

```
DGS-3000-28XMP:admin#disable hol_prevention
Command: disable hol_prevention

Success.

DGS-3000-28XMP:admin#
```

71-15 show hol_prevention

Description

This command is used to display head of line prevention state on the Switch.

Format

show hol_prevention

Parameters

None.

Restrictions

None.

Example

To display HOL prevention state on the Switch.

```
DGS-3000-28XMP:admin#show hol_prevention
Command: show hol_prevention

Device HOL Prevention State: Enabled


DGS-3000-28XMP:admin#
```

71-16 config 802.1p map

Description

This command is used to configure the mapping of 802.1p to the packet's initial color. The mapping of 802.1p to a color is used to determine the initial color of the packet when the policing function of the packet is color aware and the packet is 1p-trusted.

Format

config 802.1p map {[<portlist> | all]} 1p_color <priority_list> to [green | red | yellow]

Parameters

<portlist> - (Optional) Enter the list of ports used for this configuration.
all - (Optional) Specifies that the command apply to all ports on the Switch.
1p_color - Specifies the list of source priority for incoming packets. **<priority_list>** - Enter the list of source priority for incoming packets.
to - Specifies the mapped color for a packet. **green** - Specifies green as the mapped color. **red** - Specifies red as the mapped color. **yellow** - Specifies yellow as the mapped color.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

If a product supports per-port 802.1p mapping configuration, configure the mapping of 802.1p priority 1 to red on ports 1-8.

```
DGS-3000-28XMP:admin# config 802.1p map 1-8 1p_color 1 to red
Command: config 802.1p map 1-8 1p_color 1 to red

Success.

DGS-3000-28XMP:admin#
```

71-17 show 802.1p map 1p_color

Description

This command is used to display the 802.1p to color mapping.

Format

show 802.1p map 1p_color {<portlist>}

Parameters

<portlist> - (Optional) Specifies a list of ports.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To show the 802.1p color mapping on port 1:

```
DGS-3000-28XMP:admin# show 802.1p map 1p_color 1
Command: show 802.1p map 1p_color 1

802.1p to Color Mapping:
-------------------------------------------------------------
Port 0      1      2      3      4      5      6      7
---- ------ ------ ------ ------ ------ ------ ------ ------
1    Green  Green  Green  Green  Green  Green  Green  Green

DGS-3000-28XMP:admin#
```

71-18 config dscp trust

Description

This command is used to configure the state of DSCP trust per port. When DSCP is not trusted, 802.1p is trusted instead.

Format

config dscp trust [<portlist> | all] state [enable | disable]

Parameters

<portlist> - Enter a list of ports used for this configuration.
all - Specifies that the command apply to all ports on the Switch.
state - Specifies to enable or disable trusting of DSCP. **enable** - Specifies that the DSCP trust state will be enabled. **disable** - Specifies that the DSCP trust state will be disabled. This is the default.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

Enable DSCP trust on ports 1-8.

```
DGS-3000-28XMP:admin# config dscp trust 1-8 state enable
Command: config dscp trust 1-8 state enable

Success.

DGS-3000-28XMP:admin#
```

71-19 show dscp trust

Description

This command is used to display DSCP trust state for the specified ports on the Switch.

Format

show dscp trust {<portlist>}

Parameters

<portlist> - (Optional) Specifies a range of ports to display.
If no parameter is specified, all ports for DSCP trust status on the Switch will be displayed.

Restrictions

None.

Example

Display DSCP trust status on ports 1-8.

```
DGS-3000-28XMP:admin# show dscp trust 1-8
Command: show dscp trust 1-8

Port DSCP-Trust
---- ----------
1    Disabled
2    Disabled
3    Disabled
4    Disabled
5    Disabled
6    Disabled
7    Disabled
8    Disabled

DGS-3000-28XMP:admin#
```

71-20 config dscp map

Description

This command is used to configure DSCP mapping. The mapping of DSCP to priority will be used to determine the priority of the packet (which will be then used to determine the scheduling queue) when the port is in DSCP trust state.

The mapping of DSCP to color will be used to determine the initial color of the packet when the policing function of the packet is color aware and the packet is DSCP-trusted.

The DSCP-to-DSCP mapping is used in the swap of DSCP of the packet when the packet is ingresses to the port. The remaining processing of the packet will base on the new DSCP. By default, the DSCP is mapped to the same DSCP.

These DSCP mapping will take effect at the same time when IP packet ingress from a DSCP-trusted port.

Format

config dscp map {[<portlist> | all]} [dscp_priority <dscp_list> to <priority 0-7> | dscp_dscp <dscp_list> to <dscp 0-63> | dscp_color <dscp_list> to [green | red | yellow]]

Parameters

<portlist> - Enter the list of ports used for this configuration here.

all - Specifies that all the ports will be included in this configuration.

dscp_priority - Specifies a list of DSCP values to be mapped to a specific priority.
- **<dscp_list>** - Enter the DSCP priority list here.
- **to** - Specifies that the above or following parameter will be mapped to the previously mentioned parameter.
  - **<priority 0-7>** - Enter the result priority of mapping.

dscp_dscp - Specifies a list of DSCP values to be mapped to a specific DSCP.
- **<dscp_list>** - Enter the DSCP to DSCP list here.
- **to** - Specifies that the above or following parameter will be mapped to the previously mentioned parameter.
  - **<dscp 0-63>** - Enter the result DSCP of mapping.

dscp_color - Specifies a list of DSCP values to be mapped to a specific color.
- **<dscp_list>** - Enter the DSCP to color list here.
- **to** - Specifies that the above or following parameter will be mapped to the previously mentioned parameter.
  - **green** - Specifies the result color of mapping to be green.

red - Specifies the result color of mapping to be red.

yellow - Specifies the result color of mapping to be yellow.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the mapping of the DSCP priority to priority 1:

```
DGS-3000-28XMP:admin# config dscp map 1-8 dscp_priority 1 to 1
Command: config dscp map 1-8 dscp_priority 1 to 1

Success.

DGS-3000-28XMP:admin#
```

To configure the global mapping of the DSCP priority to priority 1:

```
DGS-3000-28XMP:admin# config dscp map dscp_priority 1 to 1
Command: config dscp map dscp_priority 1 to 1

Success.

DGS-3000-28XMP:admin#
```

71-21 show dscp map

Description

This command is used to show DSCP trusted port list, and mapped color, priority and DSCP values.

Format

show dscp map {<portlist>} [dscp_priority | dscp_dscp | dscp_color] {dscp <dscp_list>}

Parameters

<portlist> - (Optional) Enter a range of ports to show. If no parameter is specified, all ports' DSCP mapping will be displayed.

dscp_priority - Specifies a list of DSCP values to be mapped to a specific priority.

dscp_dscp - Specifies a list of DSCP values to be mapped to a specific DSCP.

dscp_color - Specifies a list of DSCP values to be mapped to a specific color.

dscp - (Optional) Specifies the DSCP value that will be mapped.

<dscp_list> - Enter the DSCP list here.

Restrictions

None.

Example

To show DSCP map configuration on port 1:

```
DGS-3000-28XMP:admin# show dscp map 1 dscp_dscp
Command: show dscp map 1 dscp_dscp

DSCP to DSCP Mapping:
-------------------------------------------------------------
Port 1     |   0    1    2    3    4    5    6    7    8    9
-----------+-------------------------------------------------
         0 |   0    1    2    3    4    5    6    7    8    9
         1 |  10   11   12   13   14   15   16   17   18   19
         2 |  20   21   22   23   24   25   26   27   28   29
         3 |  30   31   32   33   34   35   36   37   38   39
         4 |  40   41   42   43   44   45   46   47   48   49
         5 |  50   51   52   53   54   55   56   57   58   59
         6 |  60   61   62   63
-------------------------------------------------------------

DGS-3000-28XMP:admin#
```

Chapter 72 RADIUS Client Command List

config radius add <server_index 1-3> [<server_ip> | <ipv6addr>] [key <password 32>] [default | {auth_port <udp_port_number 1-65535> | acct_port <udp_port_number 1-65535> | timeout <sec 1-255> | retransmit <int 1-20>}(1)]
config radius delete <server_index 1-3>
config radius <server_index 1-3> {ipaddress [<server_ip> | <ipv6addr>] | [key <password 32>] | auth_port [<udp_port_number 1-65535> | default] | acct_port [<udp_port_number 1-65535> | default] | timeout [<sec 1-255> | default] | retransmit [<int 1-20> | default]}(1)
show radius
show auth_statistics {ports <portlist>}
show auth_diagnostics {ports <portlist>}
show auth_session_statistics {ports <portlist>}
show auth_client
show acct_client

72-1 config radius add

Description

This command is used to add a new RADIUS server. The server with lower index has higher authentication priority.

Format

config radius add <server_index 1-3> [<server_ip> | <ipv6addr>] [key <password 32>] [default | {auth_port <udp_port_number 1-65535> | acct_port <udp_port_number 1-65535> | timeout <sec 1-255> | retransmit <int 1-20>}(1)]

Parameters

<server_index 1-3> - Enter the RADIUS server index. This value must be between 1 and 3.
<server_ip> - Enter the IP address of the RADIUS server here.
<ipv6addr> - Enter the IPv6 address of the RADIUS server here.
key - Specifies the key pre-negotiated between switch and the RADIUS server. It is used to encrypt user's authentication data before being transmitted over internet. **<password 32>** - Enter the password here. The password can be up to 32 characters long.
default - Specifies to set the authentication UDP port number to 1812 accounting UDP port number to 1813, timeout to 5 seconds and retransmit to 2.
auth_port - Specifies the UDP port number which is used to transmit RADIUS authentication data between the Switch and the RADIUS server. **<udp_port_number 1-65535>** - Enter the authentication port number here. This value must be between 1 and 65535.
acct_port - Specifies the UDP port number which is used to transmit RADIUS accounting statistics between the Switch and the RADIUS server. **<udp_port_number 1-65535>** - Enter the accounting port number here. This value must be between 1 and 65535.
timeout - Specifies the time in second for waiting server reply. The default value is 5 seconds.

<sec 1-255> - Enter the timeout value here. This value must be between 1 and 255 seconds.

retransmit - Specifies the count for re-transmitting. The default value is 2.

<int 1-20> - Enter the re-transmit value here. This value must be between 1 and 20.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To add a new RADIUS server:

```
DGS-3000-28XMP:admin# config radius add 1 10.48.74.121 key dlink default
Command: config radius add 1 10.48.74.121 key dlink default

Success.

DGS-3000-28XMP:admin#
```

72-2 config radius delete

Description

This command is used to delete a RADIUS server.

Format

config radius delete <server_index 1-3>

Parameters

<server_index 1-3> - Enter the RADIUS server index to be deleted.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete a RADIUS server:

```
DGS-3000-28XMP:admin# config radius delete 1
Command: config radius delete 1

Success.

DGS-3000-28XMP:admin#
```

72-3 config radius

Description

This command is used to configure a RADIUS server.

Format

config radius <server_index 1-3> {ipaddress [<server_ip> | <ipv6addr>] | [key <password 32>] | auth_port [<udp_port_number 1-65535> | default] | acct_port [<udp_port_number 1-65535> | default] | timeout [<sec 1-255> | default] | retransmit [<int 1-20> | default]}(1)

Parameters

<server_index 1-3> - Enter the RADIUS server index here. This value must be between 1 and 3.

ipaddress - Specifies the IP address of the RADIUS server.

- **<server_ip>** - Enter the RADIUS server IP address here.
- **<ipv6addr>** - Enter the RADIUS server IPv6 address here.

key - Specifies the key pre-negotiated between switch and RADIUS server. It is used to encrypt user's authentication data before being transmitted over internet.

- **<password 32>** - Enter the key here. The key can be up to 32 characters long.

auth_port - Specifies the UDP port number which is used to transmit RADIUS authentication data between the Switch and the RADIUS server. The default value is 1812.

- **<udp_port_number 1-65535>** - Enter the authentication port number here. This value must be between 1 and 65535.
- **default** - Specifies that the default port number will be used.

acct_port - Specifies the UDP port number which is used to transmit RADIUS accounting statistics between the Switch and the RADIUS server. The default value is 1813.

- **<udp_port_number 1-65535>** - Enter the accounting port number here. This value must be between 1 and 65535.
- **default** - Specifies that the default port number will be used.

timeout - Specifies the time in second for waiting server reply. The default value is 5 seconds.

- **<sec 1-255>** - Enter the timeout value here. This value must be between 1 and 255 seconds.
- **default** - Specifies that the default timeout value will be used.

retransmit - Specifies the count for re-transmitting. The default value is 2.

- **<int 1-20>** - Enter the re-transmit value here. This value must be between 1 and 20.
- **default** - Specifies that the default re-transmit value will be used.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure a RADIUS server:

```
DGS-3000-28XMP:admin# config radius 1 auth_port 60
Command: config radius 1 auth_port 60

Success.

DGS-3000-28XMP:admin#
```

72-4 show radius

Description

This command is used to display the RADIUS server configuration.

Format

show radius

Parameters

None.

Restrictions

None.

Example

To display RADIUS server configurations:

```
DGS-3000-28XMP:admin# show radius
Command: show radius

Index  IP Address      Auth-Port Acct-Port Timeout Retransmit Key
                                           (sec)
-----  --------------- --------- --------- ------- ---------- ----------------
1      10.48.74.121    60        1813      5       2          dlink


Total Entries : 1

DGS-3000-28XMP:admin#
```

72-5 show auth_statistics

Description

This command is used to display information of authenticator statistics.

Format

show auth_statistics {ports <portlist>}

Parameters

ports - (Optional) Specifies a range of ports to be displayed. **<portlist>** - Enter the list of ports that will be displayed here.

Restrictions

None.

Example

To display authenticator statistics information for port 1:

```
DGS-3000-28XMP:admin# show auth_statistics ports 1
Command: show auth_statistics ports 1


 Port Number : 1

 EapolFramesRx                      0
 EapolFramesTx                      9
 EapolStartFramesRx                 0
 EapolReqIdFramesTx                 6
 EapolLogoffFramesRx                0
 EapolReqFramesTx                   0
 EapolRespIdFramesRx                0
 EapolRespFramesRx                  0
 InvalidEapolFramesRx               0
 EapLengthErrorFramesRx             0
 LastEapolFrameVersion              0
 LastEapolFrameSource               00-00-00-00-00-00




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

72-6 show auth_diagnostics

Description

This command is used to display information of authenticator diagnostics.

Format

show auth_diagnostics {ports <portlist>}

Parameters

ports - (Optional) Specifies a range of ports to be displayed. **<portlist>** - Enter the list of ports that will be displayed here.

Restrictions

None.

Example

To display authenticator diagnostics information for port 1:

```
DGS-3000-28XMP:admin# show auth_diagnostics ports 1
Command: show auth_diagnostics ports 1


 Port Number : 1

 EntersConnecting                    11
 EapLogoffsWhileConnecting           0
 EntersAuthenticating                0
 SuccessWhileAuthenticating          0
 TimeoutsWhileAuthenticating         0
 FailWhileAuthenticating             0
 ReauthsWhileAuthenticating          0
 EapStartsWhileAuthenticating        0
 EapLogoffWhileAuthenticating        0
 ReauthsWhileAuthenticated           0
 EapStartsWhileAuthenticated         0
 EapLogoffWhileAuthenticated         0
 BackendResponses                    0
 BackendAccessChallenges             0
 BackendOtherRequestsToSupplicant    0
 BackendNonNakResponsesFromSupplicant 0
 BackendAuthSuccesses                0
 BackendAuthFails                    0

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

72-7 show auth_session_statistics

Description

This command is used to display authenticator session statistics.

Format

show auth_session_statistics {ports <portlist>}

Parameters

ports - (Optional) Specifies a range of ports to be displayed.
<portlist> - Enter the list of ports that will be displayed here.

Restrictions

None.

Example

To display authenticator session statistics information on port 1:

```
DGS-3000-28XMP:admin# show auth_session_statistics ports 1
Command: show auth_session_statistics ports 1

Port Number : 1

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

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

72-8 show auth_client

Description

This command is used to display authentication information of the RADIUS client.

Format

show auth_client

Parameters

None.

Restrictions

None.

Example

To display authentication information of the RADIUS client information:

```
DGS-3000-28XMP:admin# show auth_client
Command: show auth_client

radiusAuthClient ==>
 radiusAuthClientInvalidServerAddresses   0
 radiusAuthClientIdentifier

 radiusAuthServerEntry ==>
 radiusAuthServerIndex :1

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

DGS-3000-28XMP:admin#
```

72-9 show acct_client

Description

This command is used to display accounting information of the RADIUS client.

Format

show acct_client

Parameters

None.

Restrictions

None.

Example

To display accounting information of the RADIUS client:

```
DGS-3000-28XMP:admin# show acct_client
Command: show acct_client

radiusAcctClient ==>
 radiusAcctClientInvalidServerAddresses   0
 radiusAcctClientIdentifier

 radiusAuthServerEntry ==>
 radiusAccServerIndex : 1

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

DGS-3000-28XMP:admin#
```

Chapter 73 RSPAN Command List

enable rspan
disable rspan
create rspan vlan [vlan_name <vlan_name> | vlan_id <vlanid 1-4094>]
delete rspan vlan [vlan_name <vlan_name> | vlan_id <vlanid 1-4094>]
config rspan vlan [vlan_name <vlan_name> | vlan_id <vlanid 1-4094>] [redirect [add | delete] ports <portlist> | source {[add | delete] ports <portlist> [rx | tx | both]]}]
show rspan {[vlan_name <vlan_name> | vlan_id <vlanid 1-4094>]}

73-1 enable rspan

Description

This command is used to enable all previously entered RSPAN configurations.

Format

enable rspan

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable all previously entered RSPAN configurations:

```
DGS-3000-28XMP:admin#enable rspan
Command: enable rspan

Success.

DGS-3000-28XMP:admin#
```

73-2 disable rspan

Description

This command is used to disable all previously entered RSPAN configurations.

Format

disable rspan

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To disable all previously entered RSPAN configurations:

```
DGS-3000-28XMP:admin#disable rspan
Command: disable rspan

Success.

DGS-3000-28XMP:admin#
```

73-3 create rspan vlan

Description

This command is used to create an RSPAN VLAN. Up to 16 RSPAN VLANs can be created.

Format

create rspan vlan [vlan_name <vlan_name> | vlan_id <vlanid 1-4094>]

Parameters

vlan_name - Create the RSPAN VLAN by VLAN name. **<vlan_name>** - Enter the VLAN name.	
vlan_id - Create the RSPAN VLAN by VLAN ID. **<vlanid 1-4094>** - Enter the VLAN ID between 1 and 4094.	

Restrictions

Only Administrators and Operators can issue this command.

Example

To create an RSPAN VLAN entry by VLAN name “v2”:

```
DGS-3000-28XMP:admin#create rspan vlan vlan_name v2
Command: create rspan vlan vlan_name v2

Success.

DGS-3000-28XMP:admin#
```

To create an RSPAN VLAN entry by VLAN ID “3”:

```
DGS-3000-28XMP:admin#create rspan vlan vlan_id 3
Command: create rspan vlan vlan_id 3

Success.

DGS-3000-28XMP:admin#
```

73-4 delete rspan vlan

Description

This command is used to delete RSPAN VLANs.

Format

delete rspan vlan [vlan_name <vlan_name> | vlan_id <vlanid 1-4094>]

Parameters

vlan_name - Specifies the RSPAN VLAN by VLAN name. **<vlan_name>** - Enter the VLAN name.
vlan_id - Specifies the RSPAN VLAN by VLAN ID. **<vlanid 1-4094>** - Enter the VLAN ID between 1 and 4094.

Restrictions

Only Administrators and Operators can issue this command.

Example

To delete an RSPAN VLAN entry by VLAN name “v2”:

```
DGS-3000-28XMP:admin#delete rspan vlan vlan_name v2
Command: delete rspan vlan vlan_name v2

Success.

DGS-3000-28XMP:admin#
```

To delete an RSPAN VLAN entry by VLAN ID “3”:

```
DGS-3000-28XMP:admin#delete rspan vlan vlan_id 3
Command: delete rspan vlan vlan_id 3

Success.

DGS-3000-28XMP:admin#
```

73-5 config rspan vlan

Description

This command is used to configure the RSPAN VLAN settings.

The **source** parameter is used by the source switch to configure the source setting for the RSPAN VLAN.

The **redirect** parameter is used by the intermediate or last switch to configure the output port of the RSPAN VLAN packets and makes sure that the RSPAN VLAN packets can egress to the redirect ports.

In addition, the VLAN setting must be correctly configured to make the RSPAN VLAN work correctly. That is, for the intermediate switch, the redirect port must be a tagged member port of the RSPAN VLAN. For the last switch, the redirect port must be either a tagged member port or an untagged member port of the RSPAN VLAN based on the users' requirements. If untagged membership is specified, the RSPAN VLAN tag will be removed. The redirect function will only work when RSPAN is enabled. Multiple RSPAN VLANs can be configured with the redirect setting at the same time.

A RSPAN VLAN can be configured with the source setting and the redirect setting at the same time.

Format

config rspan vlan [vlan_name <vlan_name> | vlan_id <vlanid 1-4094>] [redirect [add | delete] ports <portlist> | source {[add | delete] ports <portlist> [rx | tx | both]]}]

Parameters

vlan_name - Specifies the RSPAN VLAN by VLAN name.
- **<vlan_name>** - Enter the VLAN name.

vlan_id - Specifies the RSPAN VLAN by VLAN ID.
- **<vlanid 1-4094>** - Enter the VLAN ID between 1 and 4094.

redirect - Specifies output port list for the RSPAN VLAN packets. If the redirect port is a Link Aggregation port, the Link Aggregation behavior will apply to the RSPAN packets.
- **add** - Specifies to add the redirect port.
- **delete** - Specifies to delete the redirect port.
  - **ports** - Specifies the output port list to add to or delete from the RSPAN packets.
    - **<portlist>** - Enter a range of ports to be configured.

source - If the ports are not specified by this command, the source of RSPAN will come from the source specified by the mirror command or the flow-based source specified by an ACL. If no parameter is specified for source, it deletes the configured source parameters.
- **add** - (Optional) Specifies to add source ports.
- **delete** - (Optional) Specifies to delete source ports.
  - **ports** - Specifies source port list to add to or delete from the RSPAN source.
    - **<portlist>** - Enter a range of ports to be configured.
  - **rx** - Specifies to only monitor ingress packets.
  - **tx** - Specifies to only monitor egress packets.
  - **both** - Specifies to monitor both ingress and egress packets.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure an RSPAN source entry without source target port:

```
DGS-3000-28XMP:admin#config rspan vlan vlan_name v2 source add ports 2-5 rx
Command: config rspan vlan vlan_name v2 source add ports 2-5 rx

Success.

DGS-3000-28XMP:admin#
```

To configure an RSPAN source entry for per flow RSPAN, without any source ports:

```
DGS-3000-28XMP:admin#config rspan vlan vlan_id 3 source
Command: config rspan vlan vlan_id 3 source

Success.

DGS-3000-28XMP:admin#
```

To configure RSPAN redirect for “VLAN 2” to ports 18 and 19:

```
DGS-3000-28XMP:admin#config rspan vlan vlan_name VLAN2 redirect add port 18-19
Command: config rspan vlan vlan_name VLAN2 redirect add ports 18-19

Success.

DGS-3000-28XMP:admin#
```

73-6 show rspan

Description

This command is used to display RSPAN configuration.

Format

show rspan {[vlan_name <vlan_name> | vlan_id <vlanid 1-4094>]}

Parameters

vlan_name - (Optional) Specifies the RSPAN VLAN by VLAN name. **<vlan_name>** - Enter the VLAN name.
vlan_id - (Optional) Specifies the RSPAN VLAN by VLAN ID. **<vlanid 1-4094>** - Enter the VLAN ID between 1 and 4094.

Restrictions

None.

Example

To display specific RSPAN VLAN settings:

```
DGS-3000-28XMP:admin#show rspan vlan_id 3
Command: show rspan vlan_id 3

RSPAN   : Enabled

RSPAN VLAN ID  : 3
--------------------
  Source Port
      RX           : 2-5
      TX           :



DGS-3000-28XMP:admin#
```

To display all RSPAN VLAN settings:

```
DGS-3000-28XMP:admin#show rspan
Command: show rspan

RSPAN   : Enabled

RSPAN VLAN ID  : 3
--------------------
  Source Port
      RX           : 2-5
      TX           :

RSPAN VLAN ID  : 4
--------------------
  Redirect Ports   : 6-10


Total RSPAN VLAN :2


DGS-3000-28XMP:admin#
```

Chapter 74 Safeguard Engine Command List

config safeguard_engine {state [enable | disable] | utilization {rising <20-100> | falling <20-100>} | trap_log [enable | disable] | mode [strict | fuzzy]}
show safeguard_engine

74-1 config safeguard_engine

Description

This command is used to configure the CPU protection control for the system.

Format

config safeguard_engine {state [enable | disable] | utilization {rising <20-100> | falling <20-100>} | trap_log [enable | disable] | mode [strict | fuzzy]}

Parameters

state - (Optional) Specifies to configure CPU protection state to enable or disable.

- **enable** - Specifies that CPU protection will be enabled.
- **disable** - Specifies that CPU protection will be enabled.

utilization - (Optional) Specifies the CPU protection threshold.

- **rising** - Specifies utilization rising threshold, the range is between 20-100%, if the CPU utilization is over the rising threshold, the Switch enters exhausted mode.
  - **<20-100>** - Enter the utilization rising value here. This value must be between 20 and 100.
- **falling** - Specifies utilization falling threshold , the range is between 20-100 , if the CPU utilization is lower than the falling threshold, the Switch enters normal mode.
  - **<20-100>** - Enter the utilization falling value here. This value must be between 20 and 100.

trap_log - (Optional) Specifies the state of CPU protection related trap/log mechanism to be enabled or disabled.

- **enable** - Specifies that the CPU protection trap or log mechanism will be enabled. When enabled, trap and log events will be created when the CPU protection mode changes.
- **disable** - Specifies that the CPU protection trap or log mechanism will be disabled. When disabled, the CPU protection mode change will not trigger trap and log events.

mode - (Optional) Specifies to determine the controlling method of broadcast traffic. Here are two modes (strict and fuzzy).

- **strict** - Specifies to use the strict mode. The Switch will stop receiving all 'IP broadcast' packets, packets from the untrusted IP address and reduce the bandwidth of 'ARP not to me' packets (the protocol address of the target in ARP packet is the Switch itself) to the Switch. That means that no matter what the reasons are that cause high CPU utilization (may not be caused by an ARP storm), the Switch processes the specified traffic, as mentioned previously in the Exhausted mode.
- **fuzzy** - Specifies to use the fuzzy mode. The Switch will adjust the bandwidth dynamically depending on some reasonable algorithm.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure CPU protection:

```
DGS-3000-28XMP:admin# config safeguard_engine state enable utilization rising 50 falling 30
trap_log enable
Command: config safeguard_engine state enable utilization rising 50 falling 30 trap_log
enable

Success.

DGS-3000-28XMP:admin#
```

74-2 show safeguard_engine

Description

This command is used to show safeguard engine information.

Format

show safeguard_engine

Parameters

None.

Restrictions

None.

Example

To show safeguard engine information:

```
DGS-3000-28XMP:admin# show safeguard_engine
Command: show safeguard_engine


Safeguard Engine State          :  Disabled
Safeguard Engine Current Status :  Normal Mode
=====================================================
CPU Utilization Information:
Rising Threshold  :  30%
Falling Threshold :  20%
Trap/Log State    :  Disabled
Mode              :  Fuzzy

DGS-3000-28XMP:admin#
```

NOTE: Safeguard engine current status has two modes: exhausted and normal mode.

Chapter 75 Secure Shell (SSH) Command List

config ssh algorithm [3DES | AES128 | AES192 | AES256 | arcfour | blowfish | cast128 | twofish128 | twofish192 | twofish256 | MD5| SHA1 | RSA | DSA] [enable | disable]
show ssh algorithm
config ssh authmode [password | publickey | hostbased] [enable | disable]
show ssh authmode
config ssh user <username 15> authmode [hostbased [hostname <domain_name 32> | hostname_IP <domain_name 32> [<ipaddr> | <ipv6addr>]] | password | publickey]
show ssh user authmode
config ssh server {maxsession <int 1-8> | contimeout <sec 120-600> | authfail <int 2-20> | rekey [10min | 30min | 60min | never] | port <tcp_port_number 1-65535>}
enable ssh
disable ssh
show ssh server

75-1 config ssh algorithm

Description

This command is used to configure SSH service algorithm.

Format

config ssh algorithm [3DES | AES128 | AES192 | AES256 | arcfour | blowfish | cast128 | twofish128 | twofish192 | twofish256 | MD5| SHA1 | RSA | DSA] [enable | disable]

Parameters

3DES - Specifies the three-key triple-DES (encrypt-decrypt-encrypt), where the first 8 bytes of the key are used for the first encryption, the next 8 bytes for the decryption, and the following 8 bytes for the final encryption.
AES (128, 192, 256) - Specifies Advanced Encryption Standard as the SSH algorithm.
arcfour - Specifies as RC4. RC4 (also known as ARC4 or ARCFOUR meaning Alleged RC4) is the most widely-used software stream cipher.
blowfish - Specifies Blowfish as the SSH algorithm. Blowfish is a keyed, symmetric block cipher.
cast128 - Specifies CAST-128 as the SSH algorithm. CAST-128 is a 12- or 16-round Feistel network with a 64-bit block size and a key size of between 40 to 128 bits.
twofish (128, 192, 256) - Specifies Twofish as the SSH algorithm. Twofish has a 128-bit block size, a key size ranging from 128 to 256 bits.
MD5 - Specifies Message-Digest Algorithm 5 as the SSH algorithm.
SHA1 - Specifies Secure Hash Algorithm as the SSH algorithm.
RSA - Specifies RSA as the SSH algorithm.RSA encryption algorithm is a non-symmetric encryption algorithm.
DSS - Specifies Digital Signature Standard as the SSH algorithm.
enable - Specifies to enable the algorithm.
disable - Specifies to disable the algorithm.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable SSH server public key algorithm:

```
DGS-3000-28XMP:admin# config ssh algorithm DSA enable
Command: config ssh algorithm DSA enable

Success.

DGS-3000-28XMP:admin#
```

75-2 show ssh algorithm

Description

This command is used to show the SSH service algorithm.

Format

show ssh algorithm

Parameters

None.

Restrictions

None.

Example

To show server algorithm:

```
DGS-3000-28XMP:admin# show ssh algorithm
Command: show ssh algorithm

Encryption Algorithm
--------------------------
3DES       : Enabled
AES128     : Enabled
AES192     : Enabled
AES256     : Enabled
Arcfour    : Enabled
Blowfish   : Enabled
Cast128    : Enabled
Twofish128 : Enabled
Twofish192 : Enabled
Twofish256 : Enabled

Data Integrity Algorithm
--------------------------
MD5        : Enabled
SHA1       : Enabled

Public Key Algorithm
--------------------------
RSA        : Enabled
DSA        : Enabled

DGS-3000-28XMP:admin#
```

75-3 config ssh authmode

Description

This command is used to configure user authentication method for SSH.

Format

config ssh authmode [password | publickey | hostbased] [enable | disable]

Parameters

password - Specifies the user authentication method as password.
publickey - Specifies the user authentication method as public key.
hostbased - Specifies the user authentication method as host-based.
enable - Specifies to enable the selected user authentication method.
disable - Specifies to disable the selected user authentication method.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure user authentication method:

```
DGS-3000-28XMP:admin# config ssh authmode publickey enable
Command: config ssh authmode publickey enable

Success.

DGS-3000-28XMP:admin#
```

75-4 show ssh authmode

Description

This command is used to show the user authentication method.

Format

show ssh authmode

Parameters

None.

Restrictions

None.

Example

To show user authentication method:

```
DGS-3000-28XMP:admin# show ssh authmode
Command: show ssh authmode

The SSH Authentication Method:
Password    : Enabled
Public Key  : Enabled
Host-based  : Enabled


DGS-3000-28XMP:admin#
```

75-5 config ssh user

Description

This command is used to update user information for SSH configuration.

Format

config ssh user <username 15> authmode [hostbased [hostname <domain_name 32> | hostname_IP <domain_name 32> <ipaddr>] | password | publickey]

config ssh user <username 15> authmode [hostbased [hostname <domain_name 32> | hostname_IP <domain_name 32> [<ipaddr> | <ipv6addr>]] | password | publickey]

Parameters

<username 15> - Enter the user name used here. This name can be up to 15 characters long.
automode - Specifies the user authentication method. **hostbased** - Specifies to use the host-based method. **hostname** - Specifies the host domain name. **<domain_name 32>** - Enter the domain name here. This name can be up to 32 characters long. **hostname_IP** - Specifies the host domain name and IP address. **<domain_name 32>** - Enter the host name if configuring the host-based method. **<ipaddr>** - Enter the host IP address. **<ipv6addr>** - Enter the host IPv6 address. **password** - Specifies to use password as the user authentication method. **publickey** - Specifies to use public key as the user authentication method.

Restrictions

Only Administrators can issue this command.

Example

To update user “test” authentication method:

```
DGS-3000-28XMP:admin# config ssh user test authmode publickey
Command: config ssh user test authmode publickey

Success.

DGS-3000-28XMP:admin#
```

75-6 show ssh user

Description

This command is used to show the SSH user information.

Format

show ssh user authmode

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To show user information about SSH configuration:

```
DGS-3000-28XMP:admin# show ssh user authmode
Command: show ssh user authmode

Current Accounts
Username          AuthMode             HostName            HostIP
------------  -------------        ------------      -------------
test              Public Key
alpha             Host-based           alpha-local        172.18.61.180
beta              Host-based           beta-local          3000::105
Total Entries : 3

DGS-3000-28XMP:admin#
```

75-7 config ssh server

Description

This command is used to configure the SSH server general information.

Format

config ssh server {maxsession <int 1-8> | contimeout <sec 120-600> | authfail <int 2-20> | rekey [10min | 30min | 60min | never] | port <tcp_port_number 1-65535>}

Parameters

maxsession - (Optional) Specifies SSH server maximum simultaneous sessions.

<int 1-8> - Enter the maximum number of simultaneous sessions value here. This value must be between 1 and 8.

contimeout - (Optional) Specifies SSH server connection time-out, in the unit of second.

<sec 120-600> - Enter the connection time-out value here. This value must be between 120 and 600 seconds.

authfail - (Optional) Specifies the maximum number of failed login attempts.

<int 2-20> - Enter the maximum fail attempts value here. This value must be between 2 and 20.

rekey - (Optional) Specifies time to re-generate session key. There are 10 minutes, 30 minutes, 60 minutes and never for the selection.

10min - Specifies that the re-generate session key time will be 10 minutes.

30min - Specifies that the re-generate session key time will be 30 minutes.

60min - Specifies that the re-generate session key time will be 60 minutes.

never - Specifies that the re-generate session key time will be set to never.

port - (Optional) Specifies the TCP port used to communication between SSH client and server. The default value is 22.

<tcp_port_number 1-65535> - Enter the TCP port number here. This value must be between 1 and 65535.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure SSH server maximum session number is 3:

```
DGS-3000-28XMP:admin# config ssh server maxsession 3
Command: config ssh server maxsession 3

Success.

DGS-3000-28XMP:admin#
```

75-8 enable ssh

Description

This command is used to enable SSH server services.

Format

enable ssh

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable SSH server:

```
DGS-3000-28XMP:admin# enable ssh
Command: enable ssh

Success.

DGS-3000-28XMP:admin#
```

75-9 disable ssh

Description

This command is used to disable SSH server services.

Format

disable ssh

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To disable the SSH server services:

```
DGS-3000-28XMP:admin# disable ssh
Command: disable ssh

Success.

DGS-3000-28XMP:admin#
```

75-10 show ssh server

Description

This command is used to show the SSH server general information.

Format

show ssh server

Parameters

None.

Restrictions

None.

Example

To show SSH server:

```
DGS-3000-28XMP:admin# show ssh server
Command: show ssh server

The SSH Server Configuration
Maximum Session              : 8
Connection Timeout           : 120
Authentication Fail Attempts : 2
Rekey Timeout                : Never
TCP Port Number              : 22


DGS-3000-28XMP:admin#
```

Chapter 76 Secure Sockets Layer (SSL) Command List

download ssl certificate {<ipaddr> certfilename <path_filename 64> keyfilename <path_filename 64>}
enable ssl {version [all | {ssl3.0 | tls1.0 | tls1.1 | tls1.2}] | ciphersuite {RSA_with_RC4_128_MD5 | RSA_with_3DES_EDE_CBC_SHA | DHE_DSS_with_3DES_EDE_CBC_SHA | RSA_EXPORT_with_RC4_40_MD5 | RSA_with_AES_128_CBC_SHA | RSA_with_AES_128_CBC_SHA256 | RSA_with_AES_256_CBC_SHA | RSA_with_AES_256_CBC_SHA256 | DHE_DSS_with_AES_256_CBC_SHA | DHE_RSA_with_AES_256_CBC_SHA}}
disable ssl {version [all | {ssl3.0 | tls1.0 | tls1.1 | tls1.2}(1)] | ciphersuite {RSA_with_RC4_128_MD5 | RSA_with_3DES_EDE_CBC_SHA | DHE_DSS_with_3DES_EDE_CBC_SHA | RSA_EXPORT_with_RC4_40_MD5 | RSA_with_AES_128_CBC_SHA | RSA_with_AES_128_CBC_SHA256 | RSA_with_AES_256_CBC_SHA | RSA_with_AES_256_CBC_SHA256 | DHE_DSS_with_AES_256_CBC_SHA | DHE_RSA_with_AES_256_CBC_SHA}(1)}
config ssl cachetimeout <value 60-86400>
show ssl {certificate}
show ssl cachetimeout

76-1 download ssl certificate

Description

This command is used to download the certificate to the device according to the certificate level. The user can download the specified certificate to the device which must, according to desired key exchange algorithm. For RSA key exchange, the user must download RSA type certificate and for DHS_DSS is using the DSA certificate for key exchange.

Format

download ssl certificate {<ipaddr> certfilename <path_filename 64> keyfilename <path_filename 64>}

Parameters

<ipaddr> - (Optional) Enter the TFTP server IP address used for this configuration here.
certfilename - (Optional) Specifies the desired certificate file name. **<path_filename 64>** - Specifies certificate file path respect to TFTP server root path, and input a maximum of 64 octets.
keyfilename - (Optional) Specifies the private key file name which accompany with the certificate. **<path_filename 64>** - Enter the private key file path respect to TFTP server root path, and input a maximum of 64 octets.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To download certificate from TFTP server:

```
DGS-3000-28XMP:admin# download ssl certificate 10.55.47.1 certfilename cert.der keyfilename
pkey.der
Command: download ssl certificate 10.55.47.1 certfilename cert.der keyfilename pkey.der

Success.

DGS-3000-28XMP:admin#
```

76-2 enable ssl

Description

This command is used to enable the SSL global state, SSL and TLS version, and cipher suites.

NOTE: HTTP will be disabled when SSL is enabled.

Format

enable ssl {version [all | {ssl3.0 | tls1.0 | tls1.1 | tls1.2}(1)] | ciphersuite {RSA_with_RC4_128_MD5 | RSA_with_3DES_EDE_CBC_SHA | DHE_DSS_with_3DES_EDE_CBC_SHA | RSA_EXPORT_with_RC4_40_MD5 | RSA_with_AES_128_CBC_SHA | RSA_with_AES_128_CBC_SHA256 | RSA_with_AES_256_CBC_SHA | RSA_with_AES_256_CBC_SHA256 | DHE_DSS_with_AES_256_CBC_SHA | DHE_RSA_with_AES_256_CBC_SHA}(1)}

Parameters

version - (Optional) Specifies the SSL/TLS version.

- **all** - Specifies that the appliance accepts SSL 3.0, TLS 1.0, TLS 1.1, and TLS 1.2.
- **ssl3.0** - Specifies that the appliance accepts SSL 3.0.
- **tls1.0** - Specifies that the appliance accepts TLS 1.0.
- **tls1.1** - Specifies that the appliance accepts TLS 1.1.
- **tls1.2** - Specifies that the appliance accepts TLS 1.2.

ciphersuite - (Optional) Specifies the cipher suite combination used for this configuration.

- **RSA_with_RC4_128_MD5** - Specifies an RSA key exchange with RC4 128 bits encryption and MD5 hash.
- **RSA_with_3DES_EDE_CBC_SHA** - Specifies an RSA key exchange with 3DES_EDE_CBC encryption and SHA hash.
- **DHE_DSS_with_3DES_EDE_CBC_SHA** - Specifies a DH key exchange with 3DES_EDE_CBC encryption and SHA hash.
- **RSA_EXPORT_with_RC4_40_MD5** - Specifies an RSA_EXPORT key exchange with RC4 40 bits encryption and MD5 hash.
- **RSA_with_AES_128_CBC_SHA** - Specifies an RSA key exchange with AES 128 bits encryption and SHA hash.
- **RSA_with_AES_128_CBC_SHA256** - Specifies an RSA key exchange with AES 128 bits encryption and SHA256 hash.
- **RSA_with_AES_256_CBC_SHA** - Specifies an RSA key exchange with AES 256 bits encryption and SHA hash.
- **RSA_with_AES_256_CBC_SHA256** - Specifies an RSA key exchange with AES 256 bits encryption and SHA256 hash.
- **DHE_DSS_with_AES_256_CBC_SHA** - Specifies a DHE-DSS key exchange with AES 256 bits encryption

and SHA hash.

DHE_RSA_with_AES_256_CBC_SHA - Specifies a DHE-RSA key exchange with AES 256 bits encryption and SHA hash.

If no parameter is specified, the SSL global state is enabled.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable the SSL ciphersuite for RSA_with_RC4_128_MD5:

```
DGS-3000-28XMP:admin# enable ssl ciphersuite RSA_with_RC4_128_MD5
Command: enable ssl ciphersuite RSA_with_RC4_128_MD5

Success.

DGS-3000-28XMP:admin#
```

To enable SSL:

```
DGS-3000-28XMP:admin#enable ssl
Command: enable ssl

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

DGS-3000-28XMP:admin#
```

76-3 disable ssl

Description

This command is used to disable the SSL global state, SSL and TLS version, and cipher suites.

Format

disable ssl {version [all | {ssl3.0 | tls1.0 | tls1.1 | tls1.2}(1)] | ciphersuite {RSA_with_RC4_128_MD5 | RSA_with_3DES_EDE_CBC_SHA | DHE_DSS_with_3DES_EDE_CBC_SHA | RSA_EXPORT_with_RC4_40_MD5 | RSA_with_AES_128_CBC_SHA | RSA_with_AES_128_CBC_SHA256 | RSA_with_AES_256_CBC_SHA | RSA_with_AES_256_CBC_SHA256 | DHE_DSS_with_AES_256_CBC_SHA | DHE_RSA_with_AES_256_CBC_SHA}(1)}

Parameters

version - (Optional) Specifies the SSL/TLS version.

all - Specifies that the appliance accepts SSL 3.0, TLS 1.0, TLS 1.1, and TLS 1.2.

ssl3.0 - Specifies that the appliance accepts SSL 3.0.

tls1.0 - Specifies that the appliance accepts TLS 1.0.

tls1.1 - Specifies that the appliance accepts TLS 1.1.

tls1.2 - Specifies that the appliance accepts TLS 1.2.

ciphersuite - (Optional) Specifies the cipher suite combination used for this configuration.

- **RSA_with_RC4_128_MD5** - Specifies an RSA key exchange with RC4 128 bits encryption and MD5 hash.
- **RSA_with_3DES_EDE_CBC_SHA** - Specifies an RSA key exchange with 3DES_EDE_CBC encryption and SHA hash.
- **DHE_DSS_with_3DES_EDE_CBC_SHA** - Specifies a DH key exchange with 3DES_EDE_CBC encryption and SHA hash.
- **RSA_EXPORT_with_RC4_40_MD5** - Specifies an RSA_EXPORT key exchange with RC4 40 bits encryption and MD5 hash.
- **RSA_with_AES_128_CBC_SHA** - Specifies an RSA key exchange with AES 128 bits encryption and SHA hash.
- **RSA_with_AES_128_CBC_SHA256** - Specifies an RSA key exchange with AES 128 bits encryption and SHA256 hash.
- **RSA_with_AES_256_CBC_SHA** - Specifies an RSA key exchange with AES 256 bits encryption and SHA hash.
- **RSA_with_AES_256_CBC_SHA256** - Specifies an RSA key exchange with AES 256 bits encryption and SHA256 hash.
- **DHE_DSS_with_AES_256_CBC_SHA** - Specifies a DHE-DSS key exchange with AES 256 bits encryption and SHA hash.
- **DHE_RSA_with_AES_256_CBC_SHA** - Specifies a DHE-RSA key exchange with AES 256 bits encryption and SHA hash.

If no parameter is specified, the SSL global state is disabled.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To disable SSL ciphersuite for RSA_with_RC4_128_MD5:

```
DGS-3000-28XMP:admin# disable ssl ciphersuite RSA_with_RC4_128_MD5
Command: disable ssl ciphersuite RSA_with_RC4_128_MD5

Success.

DGS-3000-28XMP:admin#
```

To disable SSL:

```
DGS-3000-28XMP:admin# disable ssl
Command: disable ssl

Success.

DGS-3000-28XMP:admin#
```

76-4 config ssl cachetimeout

Description

This command is used to configure the cache timeout value which is designed for dlktimer library to remove the session ID after expired. In order to support the resume session feature, the SSL library keep the session ID in web server, and invoking the dlktimer library to remove this session ID by cache timeout value. The unit of

argument's value is second and it's boundary is between 60 (1 minute) and 86400 (24 hours). Default value is 600 seconds.

Format

config ssl cachetimeout <value 60-86400>

Parameters

<value 60-86400> - Enter the SSL cache timeout value here. This value must be between 60 and 86400.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the SSL cache timeout value to 60:

```
DGS-3000-28XMP:admin# config ssl cachetimeout 60
Commands: config ssl cachetimeout 60

Success.

DGS-3000-28XMP:admin#
```

76-5 show ssl

Description

This command is used to display the certificate status. User must download specified certificate type according to desired key exchange algorithm. The options may be no certificate, RSA type or DSA type certificate

Format

show ssl {certificate}

Parameters

certificate – (Optional) Specifies that the SSL certificate will be displayed.

Restrictions

None.

Example

To show SSL:

```
DGS-3000-28XMP:admin#show ssl
Command: show ssl

 SSL Status                                    Disabled
 SSL 3.0                                       Disabled
 TLS 1.0                                       Enabled
 TLS 1.1                                       Enabled
 TLS 1.2                                       Enabled

 Cipher Suites:
 RSA_WITH_RC4_128_MD5                  0x0004  Disabled
 RSA_WITH_3DES_EDE_CBC_SHA             0x000A  Enabled
 DHE_DSS_WITH_3DES_EDE_CBC_SHA         0x0013  Enabled
 RSA_EXPORT_WITH_RC4_40_MD5            0x0003  Disabled
 RSA_WITH_AES_128_CBC_SHA              0x002F  Enabled
 RSA_WITH_AES_256_CBC_SHA              0x0035  Enabled
 RSA_WITH_AES_128_CBC_SHA256           0x003C  Enabled
 RSA_WITH_AES_256_CBC_SHA256           0x003D  Enabled
 DHE_DSS_WITH_AES_256_CBC_SHA          0x0038  Enabled
 DHE_RSA_WITH_AES_256_CBC_SHA          0x0039  Enabled

DGS-3000-28XMP:admin#
```

To show certificate:

```
DGS-3000-28XMP:admin# show ssl certificate
Command: show ssl certificate

Loaded with RSA Certificate!

DGS-3000-28XMP:admin#
```

76-6 show ssl cachetimeout

Description

This command is used to show the cache timeout value which is designed for dlktimer library to remove the session ID after expired. In order to support the resume session feature, the SSL library keep the session ID in web server, and invoking the dlktimer library to remove this session ID by cache timeout value.

Format

show ssl cachetimeout

Parameters

None.

Restrictions

None.

Example

To show SSL cache timeout:

```
DGS-3000-28XMP:admin# show ssl cachetimeout
Commands: show ssl cachetimeout

Cache timeout is 600 second(s)

DGS-3000-28XMP:admin#
```

Chapter 77 sFlow Command List

enable sflow
disable sflow
create sflow analyzer_server <value 1-4> owner <name 16> {timeout [<sec 1-2000000> | infinite] | collectoraddress [<ipaddr> | <ipv6addr>] | collectorport <udp_port_number 1-65535> | maxdatagramsize <value 300-1400>}
create sflow counter_poller ports [<portlist> | all] analyzer_server_id <value 1-4> {interval [disable | <sec 20-120>]}
create sflow flow_sampler ports [<portlist> | all] analyzer_server_id <value 1-4> { rate <value 0-65535> | tx_rate <value 0-65535> | maxheadersize <value 18-256>}
delete sflow analyzer_server <value 1-4>
delete sflow counter_poller ports [<portlist> | all]
delete sflow flow_sampler ports [<portlist> | all]
config sflow analyzer_server <value 1-4> {timeout [<sec 1-2000000> | infinite] | collectoraddress [<ipaddr> | <ipv6addr>] | collectorport <udp_port_number 1-65535> | maxdatagramsize <value 300-1400>}(1)
config sflow counter_poller ports [<portlist> | all] interval [disable | <sec 20-120>]
config sflow flow_sampler ports [<portlist> | all] {rate <value 0-65535> | tx_rate <value 0-65535> | maxheadersize <value 18-256>}(1)
show sflow
show sflow analyzer_server
show sflow counter_poller
show sflow flow_sampler

77-1 enable sflow

Description

This command is used to enable the sFlow function on the Switch.

Format

enable sflow

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable the sFlow function globally:

```
DGS-3000-28XMP:admin#enable sflow
Command: enable sflow

Success.

DGS-3000-28XMP:admin#
```

77-2 disable sflow

Description

This command is used to disable the sFlow function on the Switch.

Format

disable sflow

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

Disable the sFlow globally:

```
DGS-3000-28XMP:admin#disable sflow
Command: disable sflow

Success.

DGS-3000-28XMP:admin#
```

77-3 create sflow analyzer_server

Description

This command is used to create the analyzer server. You can specify more than one analyzer server with the same IP address but with different UDP port numbers. You can have up to four unique combinations of IP address and UDP port number.

Format

create sflow analyzer_server <value 1-4> owner <name 16> {timeout [<sec 1-2000000> | infinite] | collectoraddress [<ipaddr> | <ipv6addr>] | collectorport <udp_port_number 1-65535> | maxdatagramsize <value 300-1400>}

Parameters

<value 1-4> - Enter the analyzer server ID here.
owner - The entity making use of this sFlow analyzer server. When owner is set or modified, the timeout value will

become 400 automatically.

<name 16> - Enter the owner name here. This name can be up to 16 characters long.

timeout - (Optional) The seconds to wait before the server is timed out. When the analyzer server times out, all of the flow samplers and counter pollers associated with this analyzer server will be deleted. The default value is 400 seconds.

<sec 1-2000000> - Enter the time-out value here. This value must be between 1 and 2000000 seconds.

infinite - Indicates the analyzer server never timeout.

collectoraddress - (Optional) The IP address of the analyzer server. If this is set to 0 or not specified, the IP address is 0 and the entry is not active.

<ipaddr> - Enter the IP address used for the configuration here.

<ipv6addr> - Enter the IPv6 address used for the configuration here.

collectorport - (Optional) The destination UDP port for sending the sFlow datagram. If not specified, the default value is 6364. The specified UDP port number can not conflict with other applications.

<udp_port_number 1-65535> - Enter the destination UDP port number here. This value must be between 1 and 65535.

maxdatagramsize - (Optional) The maximum number of data bytes that can be packed in a single sample datagram. If not specified, the default value is 1400 bytes.

<value 300-1400> - Enter the maximum datagram size here. This value must be between 300 and 1400.

Restrictions

Only Administrators and Operators can issue this command.

Example

To create the analyzer server:

```
DGS-3000-28XMP:admin#create sflow analyzer_server 2 owner monitor timeout inf
inite collectoraddress 10.0.0.1 collectorport 65524 maxdatagramsize 300
Command: create sflow analyzer_server 2 owner monitor timeout infinite collectoraddress 10
.0.0.1 collectorport 65524 maxdatagramsize 300

Success.

DGS-3000-28XMP:admin#
```

77-4 create sflow counter_poller ports

Description

This command is used to create the sFlow counter poller. The poller function instructs the Switch to forward port statistics counter information.

Format

create sflow counter_poller ports [<portlist> | all] analyzer_server_id <value 1-4> {interval [disable | <sec 20-120>]}

Parameters

<portlist> - Enter the list of ports that will be used for this configuration here.

all - Specifies all ports on the Switch.

analyzer_server_id - Specifies the analyzer server ID.

<value 1-4> - Enter the analyzer server here. This value must be between 1 and 4.

interval - (Optional) The maximum number of seconds between successive statistic counters information updates.

disable - This new sFlow counter will not export counters until the interval is set to an appropriate value. If interval is not specified, its default value is disabled.

<sec 20-120> - Enter the maximum number of seconds between successive statistics counter information updates here. This value must be between 20 and 120 seconds.

Restrictions

Only Administrators and Operators can issue this command.

Example

Create sFlow counter poller, which sample port 1 to analyzer server 1:

```
DGS-3000-28XMP:admin#create sflow counter_poller ports 1 analyzer_server_id 1

Command: create sflow counter_poller ports 1 analyzer_server_id 1

Success.

DGS-3000-28XMP:admin#
```

77-5 create sflow flow_sampler ports

Description

This command is used to create the sFlow flow sampler on ports. By configuring the sampling function, a sample packet received by this port will be encapsulated and forwarded to the analyzer server at specified intervals.

Format

create sflow flow_sampler ports [<portlist> | all] analyzer_server_id <value 1-4> {rate <value 0-65535> | tx_rate <value 0-65535> | maxheadersize <value 18-256>}

Parameters

<portlist> - Enter the list of ports that will be used for this configuration here.

all - Specifies all ports on the Switch.

analyzer_server_id - Specifies the ID of a server analyzer that the packet will be forwarded to.

<value 1-4> - Enter the analyzer server ID here. This value must be between 1 and 4.

rate - (Optional) Specifies the RX sampling rate for packet sampling. The default value is 256. If set to 0, the sampler is disabled. If the rate is not specified, its default value is 0.

<value 0-65535> - Enter the RX sampling rate value here. This value must be between 0 and 65535.

tx_rate - (Optional) Specifies the TX sampling rate for packet sampling. The default value is 256. If set to 0, the sampler is disabled. If the rate is not specified, its default value is 0.

<value 0-65535> - Enter the TX sampling rate value here. This value must be between 0 and 65535.

maxheadersize - (Optional) The maximum number of leading bytes in the packet which has been sampled that will be encapsulated and forwarded to the server. If not specified, the default value is 128.

<value 18-256> - Enter the maximum header size here. This value must be between 18 and 256.

Restrictions

Only Administrators and Operators can issue this command.

Example

Create sFlow flow sampler:

```
DGS-3000-28XMP:admin#create sflow flow_sampler ports 1 analyzer_server_id 1 rate 1
maxheadersize 18
Command: create sflow flow_sampler ports 1 analyzer_server_id 1 rate 1 maxheadersize 18

Success.

DGS-3000-28XMP:admin#
```

77-6 delete sflow_analyzer_server

Description

This command is used to delete a specified analyzer server.

Format

delete sflow analyzer_server <value 1-4>

Parameters

<value 1-4> - Enter the analyzer server ID value here. This value must be between 1 and 4.

Restrictions

Only Administrators and Operators can issue this command.

Example

To delete an analyzer server:

```
DGS-3000-28XMP:admin#delete sflow analyzer_server 1
Command: delete sflow analyzer_server 1

Success.

DGS-3000-28XMP:admin#
```

77-7 delete sflow counter_poller

Description

This command is used to delete the sFlow counter poller from the specified port.

Format

delete sflow counter_poller ports [<portlist> | all]

Parameters

<portlist> - Enter the list of ports to be deleted.
all - Specifies all ports on the Switch.

Restrictions

Only Administrators and Operators can issue this command.

Example

To delete an sFlow counter poller on port 1:

```
DGS-3000-28XMP:admin#delete sflow counter_poller ports 1
Command: delete sflow counter_poller ports 1

Success.

DGS-3000-28XMP:admin#
```

77-8 delete sflow flow_sampler ports

Description

This command is used to delete the sFlow flow sampler.

Format

delete sflow flow_sampler ports [<portlist> | all]

Parameters

<portlist> - Enter the list of ports to be deleted.
all - Specifies all ports on the Switch.

Restrictions

Only Administrators and Operators can issue this command.

Example

To delete the sFlow sampler port 1:

```
DGS-3000-28XMP:admin#delete sflow flow_sampler ports 1
Command: delete sflow flow_sampler ports 1

Success.

DGS-3000-28XMP:admin#
```

77-9 config sflow analyzer_server

Description

This command is used to configure the receiver information. You can specify more than one collector with the same IP address if the UDP port numbers are unique.

Format

config sflow analyzer_server <value 1-4> {timeout [<sec 1-2000000> | infinite] | collectoraddress [<ipaddr> | <ipv6addr>] | collectorport <udp_port_number 1-65535> | maxdatagramsize < value 300-1400>}(1)

Parameters

<value 1-4> - Enter the analyzer server ID here. This value must be between 1 and 4.

timeout - The time (in seconds) remaining before the sample is released and stops sampling. When the analyzer server times out, all of the flow samplers and counter pollers associated with this analyzer server will be deleted.

<sec 1-2000000> - Enter the time-out value here. This value must be between 1 and 2000000 seconds.

infinite - Indicates the analyzer server will never time out.

collectoraddress - The IP address of the server. If the address is not specified or configured as 0.0.0.0, sFlow packets will not be sent to this server.

<ipaddr> - Enter the IP address used for the configuration here.

<ipv6addr> - Enter the IPv6 address used for the configuration here.

collectorport - The destination UDP port for sending the sFlow datagram. If not specified, the default value is 6364.

<udp_port_number 1-65535> - Enter the destination port number here. This value must be between 1 and 65535.

maxdatagramsize - The maximum number of data bytes that can be packed in a single sample datagram. If not specified, the default value is 1400 bytes.

<value 300-1400> - Enter the maximum datagram size here. This value must be between 300 and 1400.

Restrictions

Only Administrators and Operators can issue this command.

Example

Configure the host 10.90.90.90 to be the sFlow analyzer server with the ID 1:

```
DGS-3000-28XMP:admin#config sflow analyzer_server 1 collectoraddress 10.90.90.90
Command: config sflow analyzer_server 1 collectoraddress 10.90.90.90

Success.

DGS-3000-28XMP:admin#
```

77-10 config sflow counter_poller ports

Description

This command is used to configure the sFlow counter poller parameters. In order to change the analyzer server ID, delete the flow sampler first and create a new one.

Format

config sflow counter_poller ports [<portlist> | all] interval [disable | <sec 20-120>]

Parameters

<portlist> - Enter the list of ports that will be used for this configuration here.
all - Specifies all ports on the Switch.
interval - The maximum number of seconds between successive samples of the counters. **disable** - Stop exporting counter. **<sec 20-120>** - Enter the maximum number of seconds between successive samples of the counters here. This value must be between 20 and 120.

Restrictions

Only Administrators and Operators can issue this command.

Example

Configure the interval of sFlow counter poller port 1 to be 0:

```
DGS-3000-28XMP:admin#config sflow counter_poller ports 1 interval disable
Command: config sflow counter_poller ports 1 interval disable

Success.

DGS-3000-28XMP:admin#
```

77-11 config sflow flow_sampler ports

Description

This command is used to configure the sFlow flow sampler parameters. In order to change the analyzer server ID, delete the flow sampler first and create a new one.

Format

config sflow flow_sampler ports [<portlist> | all] {rate <value 0-65535> | tx_rate <value 0-65535> | maxheadersize <value 18-256>}(1)

Parameters

<portlist> - Enter the list of ports that will be used for this configuration here.
all - Specifies all ports on the Switch.
rate - Specifes the RX sampling rate for packet sampling. If set to 0, the sampler is disabled. If the rate is not specified, the default value is 0. **<value 0-65535>** - Enter the RX sampling rate value here. This value must be between 0 and 65535.
tx_rate - Specifies the TX sampling rate for packet sampling. If set to 0, the sampler is disabled. If the rate is not specified, the default value is 0. **<value 0-65535>** - Enter the product dependent variables between 0 to 65535 here.
maxheadersize - The maximum number of leading bytes in the packet which has been sampled that will be encapsulated and forwarded to the server. The default value is 128. **<value 18-256>** - Enter the maximum header size value here. This value must be between 18 and 256.

Restrictions

Only Administrators and Operators can issue this command.

Example

Configure the sFlow sampler the rate of port 1 to be 0:

```
DGS-3000-28XMP:admin#config sflow flow_sampler ports 1 rate 0 maxheadersize 18
Command: config sflow flow_sampler ports 1 rate 0 maxheadersize 18

Success.

DGS-3000-28XMP:admin#
```

77-12 show sflow

Description

This command is used to show the sFlow information.

Format

show sflow

Parameters

None.

Restrictions

None.

Example

To show the sFlow information:

```
DGS-3000-28XMP:admin#show sflow
Command: show sflow

 sFlow Version  : V5
 sFlow Address  : 10.90.90.90
 sFlow AddressV6: FE80::F27D:68FF:FE15:1000
 sFlow State    : Enabled

DGS-3000-28XMP:admin#
```

77-13 show sflow analyzer_server

Description

This command is used to show the sFlow analyzer server information. The Timeout field specifies the timeout configured by user. The Current Countdown Time is the current time remaining before the server timeout.

Format

show sflow analyzer_server

Parameters

None.

Restrictions

None.

Example

To show the sFlow flow sampler information of ports which have been created:

```
DGS-3000-28XMP:admin#show sflow analyzer_server
Command: show sflow analyzer_server

 sFlow Analyzer_server Information
 ------------------------------
 Server ID             : 1
 Owner                 : sflow
 Timeout               : 10000
 Current Countdown Time: 9526
 Collector Address     : 10.90.90.5
 Collector Port        : 6343
 Max Datagram Size     : 1400

 Server ID             : 2
 Owner                 : monitor
 Timeout               : Infinite
 Current Countdown Time: Infinite
 Collector Address     : 10.0.0.1
 Collector Port        : 65524
 Max Datagram Size     : 300

Total Entries: 2

DGS-3000-28XMP:admin#
```

77-14 show sflow counter_poller

Description

This command is used to display the sFlow counter pollers which have been configured for the port.

Format

show sflow counter_poller

Parameters

None.

Restrictions

None.

Example

To show the sFlow counter poller information of ports which have been created:

```
DGS-3000-28XMP:admin#show sflow counter_poller
Command: show sflow counter_poller

 Port   Analyzer Server ID   Polling Interval (sec)
 ----   ------------------   ----------------------
 1      1                    Disable
 2      1                    Disable
 3      1                    Disable

Total Entries: 3

DGS-3000-28XMP:admin#
```

77-15 show sflow flow_sampler

Description

This command is used to show the sFlow flow sampler configured for ports. The actual value rate is 256 times the displayed rate value. There are two types of rates: the Configured Rate and the Active Rate. The Configured Rate is configured by the user. In order to limit the number of packets sent to the CPU when the rate of traffic to the CPU is high, the sampling rate will be decreased. This is specified as the Active Rate.

Format

show sflow flow_sampler

Parameters

None.

Restrictions

None.

Example

To show the sFlow flow sampler information of ports which have been created:

```
DGS-3000-28XMP:admin#show sflow flow_sampler
Command: show sflow flow_sampler

 Port    Analyzer   Configured  Configured  Active   Active   Max Header
         Server ID  Rx Rate     Tx Rate     Rx Rate  Tx Rate  Size
 ------  ---------  ----------  ----------  -------  -------  -----------
 1       1          0           0           0        0        18

Total Entries: 1

DGS-3000-28XMP:admin#
```

Chapter 78 Show Technical Support Command List

show tech_support
upload tech_support_toTFTP {<ipaddr> <path_filename 64>}

78-1 show tech_support

Description

This command is used by technical support personnel to dump the device operation information.

- Basic System information
- System log
- Running configuration
- Layer 1 information
- Layer 2 information
- Layer 3 information
- Application
- OS status
- Controller's status

This command can be interrupted by CTRL+C or ESC when it is executing.

Format

show tech_support

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To show the information of technical support:

```
DGS-3000-28XMP:admin# show tech_support
Command: show tech_support

 #------------------------------------------------------------------------------
 #                    DGS-3000-28XMP Gigabit Ethernet Switch
 #                         Technical Support Information
 #
 #                           Firmware: Build 4.00.010
 #          Copyright(C) 2018  D-Link Corporation. All rights reserved.
 #------------------------------------------------------------------------------


 ********************   Basic System Information   ********************

 [SYS 2017-12-20 10:34:38]

 Boot Time           : 20 Dec 2017  08:09:53
 RTC Time            : 2017/12/20 10:34:38
 Boot PROM Version   : Build 4.00.001
 Firmware Version    : Build 4.00.010
 Hardware Version    : B1
 Serial number       : DGS-3000-28XMP
 MAC Address         : F0-7D-68-15-10-00
 [ERROR_LOG 2017-12-20 10:34:38]

  Error log is empty.

 ********************   System Log   ********************
```

78-2 upload tech_support_toTFTP

Description

This command is used to upload the technical support information to a TFTP server.

- Basic System information
- System log
- Running configuration
- Layer 1 information
- Layer 2 information
- Layer 3 information
- Application
- OS status
- Controller’s status

This command can be interrupted by CTRL+C or ESC when it is executing.

Format

upload tech_support_toTFTP {<ipaddr> <path_filename 64>}

Parameters

<ipaddr> - (Optional) Enter the IP address of the TFTP server.

<path_filename 64> - Enter the file name to store the technical support information on the TFTP server. The maximum filename length is 64 characters.

Restrictions

Only Administrators and Operators can issue this command.

Example

To upload the information of technical support:

```
DGS-3000-28XMP:admin# upload tech_support_toTFTP 10.0.0.66 tech_report.txt
Command: upload tech_support_toTFTP 10.0.0.66 tech_report.txt

 Connecting to server.................. Done.
 Upload techsupport file............... Done.

 Success.

DGS-3000-28XMP:admin#
```

Chapter 79 Simple Mail Transfer Protocol (SMTP) Command List

enable smtp
disable smtp
config smtp {server <ipaddr> | server_port <tcp_port_number 1-65535> | self_mail_addr <mail_addr 64> | [add mail_receiver <mail_addr 64> | delete mail_receiver <index 1-8>]}(1)
show smtp
smtp send_testmsg

79-1 enable smtp

Description

This command is used to enable the SMTP status.

Format

enable smtp

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To enable SMTP status:

```
DGS-3000-28XMP:admin# enable smtp
Command: enable smtp

Success.

DGS-3000-28XMP:admin#
```

79-2 disable smtp

Description

This command is used to disable SMTP status.

Format

disable smtp

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To disable SMTP status:

```
DGS-3000-28XMP:admin# disable smtp
Command: disable smtp

Success.

DGS-3000-28XMP:admin#
```

79-3 config smtp

Description

This command is used to configure SMTP settings.

Format

config smtp {server <ipaddr> | server_port <tcp_port_number 1-65535> | self_mail_addr <mail_addr 64> | [add mail_receiver <mail_addr 64> | delete mail_receiver <index 1-8>]}(1)

Parameters

server - Specifies the SMTP server IP address. **<ipaddr>** - Enter the SMTP server IP address
server_port - Specifies the SMTP server port. **<tcp_port_number 1-65535>** - Enter the port number between 1 and 65535.
self_mail_addr - Specifies the sender's mail address. **<mail_addr 64>** - Enter the mail address with maximum of 64 characters.
add mail_receiver – Specifies to add mail receiver's address. **<mail_addr 64>** - Enter the mail address with maximum of 64 characters.
delete mail_receiver – Specifies to delete mail receiver's address. **<index 1-8>** - Enter the index number.

Restrictions

Only Administrators can issue this command.

Example

To configure an SMTP server IP address:

```
DGS-3000-28XMP:admin# config smtp server 172.18.208.9
Command: config smtp server 172.18.208.9

Success.

DGS-3000-28XMP:admin#
```

To configure an SMTP server port:

```
DGS-3000-28XMP:admin# config smtp server_port 25
Command: config smtp server_port 25

Success.

DGS-3000-28XMP:admin#
```

To configure a mail source address:

```
DGS-3000-28XMP:admin# config smtp self_mail_addr mail@dlink.com
Command: config smtp self_mail_addr mail@dlink.com

Success.

DGS-3000-28XMP:admin#
```

To add a mail destination address:

```
DGS-3000-28XMP:admin# config smtp add mail_receiver receiver@dlink.com
Command: config smtp add mail_receiver receiver@dlink.com

Success.

DGS-3000-28XMP:admin#
```

To delete a mail destination address:

```
DGS-3000-28XMP:admin# config smtp delete mail_receiver 1
Command: config smtp delete mail_receiver 1

Success.

DGS-3000-28XMP:admin#
```

79-4 show smtp

Description

This command is display the current SMTP information.

Format

show smtp

Parameters

None.

Restrictions

None.

Example

To display the current SMTP information:

```
DGS-3000-28XMP:admin# show smtp
Command: show smtp

SMTP Status             : Disabled
SMTP Server Address     : 172.18.208.9
SMTP Server Port        : 25
Self Mail Address       : mail@dlink.com

Index    Mail Receiver Address
-----    ------------------------------------------------------------------------
1        receiver@dlink.com
2
3
4
5
6
7
8


DGS-3000-28XMP:admin#
```

79-5 smtp send_testmsg

Description

This command is used to test whether the SMTP server can be reached.

Format

smtp send_testmsg

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To test whether the SMTP server can be reached:

```
DGS-3000-28XMP:admin# smtp send_testmsg
Command: smtp send_testmsg

Subject:e-mail heading
Content:e-mail content

Sending mail, please wait...

Success.

DGS-3000-28XMP:admin#
```

Chapter 80 Simple Network Management Protocol (SNMP) Command List

create snmp community <community_string 32> view <view_name 32> [read_only | read_write]
delete snmp community <community_string 32>
show snmp community {<community_string 32>}
create snmp user <user_name 32> <groupname 32> {encrypted [by_password auth [md5 <auth_password 8-16> | sha <auth_password 8-20>] priv [none | des <priv_password 8-16>] | by_key auth [md5 <auth_key 32-32> | sha <auth_key 40-40>] priv [none | des <priv_key 32-32>]]}
delete snmp user <username 32>
show snmp user
create snmp group <groupname 32> [v1 | v2c | v3 [noauth_nopriv | auth_nopriv | auth_priv]] {read_view <view_name 32> | write_view <view_name 32> | notify_view <view_name 32>}
delete snmp group <groupname 32>
show snmp groups
create snmp view <view_name 32> <oid> view_type [included | excluded]
delete snmp view <view_name 32> [all | <oid>]
show snmp view {<view_name 32>}
create snmp [host <ipaddr> | v6host <ipv6addr>] [v1 | v2c | v3 [noauth_nopriv | auth_nopriv | auth_priv]] <auth_string 32>
delete snmp [host <ipaddr> | v6host <ipv6addr>]
show snmp host {<ipaddr>}
show snmp v6host {<ipv6addr>}
config snmp engineID <snmp_engineID 10-64>
show snmp engineID
enable snmp
disable snmp
config snmp system_name {<sw_name>}
config snmp system_location {<sw_location>}
config snmp system_contact {<sw_contact>}
enable snmp traps
disable snmp traps
enable snmp authenticate_traps
disable snmp authenticate_traps
enable snmp linkchange_traps
disable snmp linkchange_traps
config snmp linkchange_traps ports [all | <portlist>] [enable | disable]
config snmp coldstart_traps [enable | disable]
config snmp warmstart_traps [enable | disable]
show snmp traps {linkchange_traps {ports <portlist>}}

config rmon trap {rising_alarm [enable | disable] | falling_alarm [enable | disable]}(1)
show rmon

80-1 create snmp community

Description

This command is used to create an SNMP community string.

Use an SNMP community string to define the relationship between the SNMP manager and the agent. The community string acts like a password to permit access to the agent on the Switch. You can specify one or more of the following characteristics associated with the string:

An access list of IP addresses of the SNMP managers that are permitted to use the community string to gain access to the agent.

A MIB view, which defines the subset of all MIB objects accessible to the given community.

Read and write or read-only permission for the MIB objects accessible to the community.

Format

create snmp community <community_string 32> view <view_name 32> [read_only | read_write]

Parameters

<community_string> - Enter an alphanumeric string of up to 32 characters used to authenticate of users wanting access to the Switch's SNMP agent.
view_name - Specifies to view a MIB name. **<view_name 32>** - Enter the MIB view name here. This name can be up to 32 characters long.
read_only - Specifies to allow the user using the above community string to have read only access to the Switch's SNMP agent.
read_write - Specifies to allow the user using the above community string to have read and write access to the Switch's SNMP agent. The default read only community string is public. The default read write community string is private.

Restrictions

Only Administrators can issue this command.

Example

To create a read-only level SNMP community "System" with a "CommunityView" view:

```
DGS-3000-28XMP:admin# create snmp community System view CommunityView read_only
Command: create snmp community System view CommunityView read_only

Success.

DGS-3000-28XMP:admin#
```

80-2 delete snmp community

Description

This command is used to delete an SNMP community string.

Format

delete snmp community <community_string 32>

Parameters

<community_string 32> - Enter the community string value to be deleted. This value can be up to 32 characters long.

Restrictions

Only Administrators can issue this command.

Example

To delete a SNMP community “System”:

```
DGS-3000-28XMP:admin# delete snmp community System
Command: delete snmp community System

Success.

DGS-3000-28XMP:admin#
```

80-3 show snmp community

Description

This command is used to display the community string configuration.

Format

show snmp community {<community_string 32>}

Parameters

<community_string 32> - (Optional) Enter the Community string.
If no parameter is specified, all community string information will be displayed.

Restrictions

Only Administrators can issue this command.

Example

To display SNMP community:

```
DGS-3000-28XMP:admin# show snmp community
Command: show snmp community

SNMP Community Table
Community Name                          View Name           Access Right
------------------------------  ----------------------  ------------
private                                  CommunityView      read_write
public                                   CommunityView      read_only

Total Entries : 2

DGS-3000-28XMP:admin#
```

80-4 create snmp user

Description

This command is used to create a new user to an SNMP group originated by this command.

Format

create snmp user <user_name 32> <groupname 32> {encrypted [by_password auth [md5 <auth_password 8-16> | sha <auth_password 8-20>] priv [none | des <priv_password 8-16>] | by_key auth [md5 <auth_key 32-32> | sha <auth_key 40-40>] priv [none | des <priv_key 32-32>]]}

Parameters

<user_name 32> - Enter the name of the user on the host that connects to the agent. The range is 1 to 32.

<groupname 32> - Enter the name of the group to which the user is associated. The range is 1 to 32.

encrypted - (Optional) Specifies whether the password appears in encrypted format.

- **by_password** - Specifies to indicate input password for authentication and privacy.
  - **auth** - Specifies an authentication level setting session. The options are md5 and sha.
    - **md5** - Specifies the HMAC-MD5-96 authentication level.
      - **<auth_password 8-16>** - Enter the MD5 authentication password here. This value must be between 8 and 16 characters.
    - **sha** - Specifies the HMAC-SHA-96 authentication level.
      - **<auth_password 8-20>** - Enter the SHA authentication password here. This value must be between 8 and 20 characters.
  - **priv** - Specifies a privacy key used by DES, it is hex string type.
    - **none** - Specifies that no encryption will be used for the privacy key.
    - **des** - Specifies that the DES encryption will be used for the privacy key.
      - **<priv_password 8-16>** - Enter the DES password value here. This value must be between 8 and 16 characters long.
- **by_key** - Specifies to indicate input key for authentication and privacy.
  - **auth** - Specifies an authentication string used by MD5 or SHA1.
    - **md5** - Specifies an authentication key used by MD5, it is hex string type.
      - **<auth_key 32-32>** - Enter the MD5 authentication key here. This value must be 32 characters long.
    - **sha** - Specifies an authentication key used by SHA1, it is hex string type.
      - **<auth_key 40-40>** - Enter the SHA authentication key here. This value must be 32 characters long.
  - **priv** - Specifies a privacy key used by DES, it is hex string type.
    - **none** - Specifies that no encryption will be used for the privacy key.

des - Specifies that the DES encryption will be used for the privacy key.
<priv_key 32-32> - Enter the DES privacy key here. This value must be 32 characters long.

Restrictions

Only Administrators can issue this command.

Example

To create a SNMP user “user123” with group “group123”:

```
DGS-3000-28XMP:admin# create snmp user user123 group123 encrypted by_password auth md5
12345678 priv des 12345678
Command: create snmp user user123 group123 encrypted by_password auth md5 12345678 priv des
12345678

Success.

DGS-3000-28XMP:admin#
```

80-5 delete snmp user

Description

This command is used to remove a user from an SNMP group and delete the associated group in SNMP group.

Format

delete snmp user <username 32>

Parameters

<username 32> - Enter the name of the user on the host that connects to the agent. The range is 1 to 32.

Restrictions

Only Administrators can issue this command.

Example

To delete a SNMP user “user123”:

```
DGS-3000-28XMP:admin# delete snmp user user123
Command: delete snmp user user123

Success.

DGS-3000-28XMP:admin#
```

80-6 show snmp user

Description

This command is used to display information on each SNMP username in the group username table.

Format

show snmp user

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To show SNMP user:

```
DGS-3000-28XMP:admin# show snmp user
Command: show snmp user

Username                          Group Name             VerAuthPriv
--------------------------------  -------------------------  -----------
initial                           initial                V3 NoneNone
user123                           group123               V3 MD5 DES

Total Entries : 2

DGS-3000-28XMP:admin#
```

80-7 create snmp group

Description

This command is used to create a new SNMP group, or a table that maps SNMP users to SNMP views.

Format

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>}

Parameters

<groupname 32> - Enter the group name here. This name can be up to 32 characters long.
v1 - Specifies the least secure of the possible security models.
v2c - Specifies the second least secure of the possible security models.
v3 - Specifies the most secure of the possible. **noauth_nopriv** - Specifies to support neither packet authentication nor encryption. **auth_nopriv** - Specifies to support packet authentication.

auth_priv - Specifies to support packet authentication and encryption.
read_view - (Optional) Specifies that the view name would be read. **<view_name 32>** - Enter the read view name here. This name can be up to 32 characters long.
write_view - (Optional) Specifies that the view name would be write. **<view_name 32>** - Enter the write view name here. This name can be up to 32 characters long.
notify_view - (Optional) Specifies that the view name would be notify. **<view_name 32>** - Enter the notify view name here. This name can be up to 32 characters long.

Restrictions

Only Administrators can issue this command.

Example

To create SNMP group “group123”:

```
DGS-3000-28XMP:admin# create snmp group group123 v3 auth_priv read_view CommunityView
write_view CommunityView notify_view CommunityView
Command: create snmp group group123 v3 auth_priv read_view CommunityView write_view
CommunityView notify_view CommunityView

Success.

DGS-3000-28XMP:admin#
```

80-8 delete snmp group

Description

This command is used to remove a SNMP group.

Format

delete snmp group <groupname 32>

Parameters

<groupname 32> - Enter the name of the group to be deleted.

Restrictions

Only Administrators can issue this command.

Example

To delete SNMP group “group123”:

```
DGS-3000-28XMP:admin# delete snmp group group123
Command: delete snmp group group123

Success.

DGS-3000-28XMP:admin#
```

80-9 show snmp groups

Description

This command is used to display the names of groups on the Switch and the security model, level, the status of the different views.

Format

show snmp groups

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To show SNMP groups:

```
DGS-3000-28XMP:admin# show snmp groups
Command: show snmp groups

Vacm Access Table Settings

Group    Name      : public
ReadView Name     : CommunityView
WriteView Name    :
Notify View Name : CommunityView
Securiy Model     : SNMPv1
Securiy Level     : NoAuthNoPriv

Group    Name      : public
ReadView Name     : CommunityView
WriteView Name    :
Notify View Name : CommunityView
Securiy Model     : SNMPv2
Securiy Level     : NoAuthNoPriv

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

Group    Name      : WriteGroup
ReadView Name     : CommunityView
WriteView Name    : CommunityView
Notify View Name : CommunityView
Securiy Model     : SNMPv2
Securiy Level     : NoAuthNoPriv

Total Entries: 10

DGS-3000-28XMP:admin#
```

80-10 create snmp view

Description

This command is used to assign views to community strings to limit which MIB objects an SNMP manager can access.

Format

create snmp view <view_name 32> <oid> view_type [included | excluded]

Parameters

<view_name 32> - Enter the view name here. The name can be up to 32 characters long.
<oid> - Enter Object-Identified tree, MIB tree.

view_type - Specifies the access type of the MIB tree in this view.
included - Specifies to include for this view.
excluded - Specifies to exclude for this view.

Restrictions

Only Administrators can issue this command.

Example

To create SNMP view “view123”:

```
DGS-3000-28XMP:admin# create snmp view view123 1.3.6 view_type included
Command: create snmp view view123 1.3.6 view_type included

Success.

DGS-3000-28XMP:admin#
```

80-11 delete snmp view

Description

This command is used to remove a view record.

Format

delete snmp view <view_name 32> [all | <oid>]

Parameters

<view_name 32> - Enter the view name here. The name can be up to 32 characters long.

all - Specifies that all view records will be removed.

<oid> - Specifies Object-Identified tree, MIB tree.

Restrictions

Only Administrators can issue this command.

Example

To delete SNMP view “view123”:

```
DGS-3000-28XMP:admin# delete snmp view view123 all
Command: delete snmp view view123 all

Success.

DGS-3000-28XMP:admin#
```

80-12 show snmp view

Description

This command is used to display the SNMP view record.

Format

show snmp view {<view_name 32>}

Parameters

<view_name 32> - (Optional) Enter the view name here. The name can be up to 32 characters long.

Restrictions

Only Administrators can issue this command.

Example

To show SNMP view:

```
DGS-3000-28XMP:admin# show snmp view
Command: show snmp view

Vacm View Table Settings
View Name              Subtree                   View Type
---------------------  ------------------------  ----------
view123                1.3.6                     Included
restricted             1.3.6.1.2.1.1             Included
restricted             1.3.6.1.2.1.11            Included
restricted             1.3.6.1.6.3.10.2.1        Included
restricted             1.3.6.1.6.3.11.2.1        Included
restricted             1.3.6.1.6.3.15.1.1        Included
CommunityView          1                         Included
CommunityView          1.3.6.1.6.3               Excluded
CommunityView          1.3.6.1.6.3.1             Included

Total Entries: 9

DGS-3000-28XMP:admin#
```

80-13 create snmp

Description

This command is used to create a recipient of an SNMP trap operation.

Format

create snmp [host <ipaddr> | v6host <ipv6addr>] [v1 | v2c | v3 [noauth_nopriv | auth_nopriv | auth_priv]] <auth_string 32>

Parameters

host - Specifies the recipient for which the traps are targeted. **<ipaddr>** - Enter the IP address of the recipient for which the traps are targeted.
v6host - Specifies the IPv6 host address to which the trap packet will be sent. **<ipv6addr>** - Enter the IPv6 address of the recipient for which the traps are targeted.
v1 - Specifies that SNMPv1 will be used. The is the least secure of the possible security models.
v2c - Specifies that SNMPv2c will be used. This is the second least secure of the possible security models.
v3 - Specifies that SNMPv3 will be used. This is the most secure of the possible security models. **noauth_nopriv** - Neither supports packet authentication nor encryption. **auth_nopriv** - Supports packet authentication. **auth_priv** - Supports packet authentication and encryption.
<auth_string 32> - Enter the authentication string. If the v1 or v2 is specified, the auth_string presents the community string, and it must be one of the entries in the community table. If the v3 is specified, the auth_string presents the user name, and it must be one of the entries in the user table.

Restrictions

Only Administrators can issue this command.

Example

To create SNMP host “10.0.0.1” with community string “public”:

```
DGS-3000-28XMP:admin# create snmp host 10.0.0.1 v1 public
Command: create snmp host 10.0.0.1 v1 public

Success.

DGS-3000-28XMP:admin#
```

80-14 delete snmp

Description

This command is used to delete a recipient of an SNMP trap operation.

Format

delete snmp [host <ipaddr> | v6host <ipv6addr>]

Parameters

host - The IP address of the recipient for which the traps are targeted. **<ipaddr>** - Enter the IP address used for the configuration here.
v6host - The IPv6 address of the recipient for which the traps are targeted. **<ipv6addr>** - Enter the IPv6 address used for the configuration here.

Restrictions

Only Administrators can issue this command.

Example

To delete SNMP host “10.0.0.1”:

```
DGS-3000-28XMP:admin# delete snmp host 10.0.0.1
Command: delete snmp host 10.0.0.1

Success.

DGS-3000-28XMP:admin#
```

80-15 show snmp host

Description

This command is used to display the recipient for which the traps are targeted.

Format

show snmp host {<ipaddr>}

Parameters

<ipaddr> - (Optional) Enter the IP address used for the configuration here.
If no parameter is specified, all SNMP hosts will be displayed.

Restrictions

Only Administrators can issue this command.

Example

To show SNMP host:

```
DGS-3000-28XMP:admin# show snmp host
Command: show snmp host

SNMP Host Table
Host IP Address  SNMP Version     Community Name / SNMPv3 User Name
---------------  ---------------  ---------------------------------
10.90.90.3        V3 noauthnopriv  initial
10.90.90.2        V2c                private
10.90.90.1        V1                 public
10.90.90.4        V3 authnopriv    user123
10.90.90.5        V3 authpriv      user234

Total Entries : 5

DGS-3000-28XMP:admin#
```

80-16 show snmp v6host

Description

This command is used to display the SNMP version 6 hosts.

Format

show snmp v6host {<ipv6addr>}

Parameters

<ipv6addr> - (Optional) Enter the IPv6 host address to be displayed.
If no parameter is specified, all SNMP version 6 hosts will be displayed.

Restrictions

Only Administrators can issue this command.

Example

To show SNMP v6 host:

```
DGS-3000-28XMP:admin# show snmp v6host
Command: show snmp v6host

SNMP Host Table
----------------------------------------------------------------
Host IPv6 Address : 3FFE::3
SNMP Version      : V3 na/np
Community Name/SNMPv3 User Name : initial

Host IPv6 Address : 3FFE::2
SNMP Version      : V2c
Community Name/SNMPv3 User Name : private

Host IPv6 Address : 3FFE::1
SNMP Version      : V1
Community Name/SNMPv3 User Name : public

Host IPv6 Address : 3FFE::3
SNMP Version      : V3  a/np
Community Name/SNMPv3 User Name : user123

Host IPv6 Address : 3FFE::3
SNMP Version      : V3  a/ p
Community Name/SNMPv3 User Name : user234

Total Entries: 5

DGS-3000-28XMP:admin#
```

80-17 config snmp engineID

Description

This command is used to configure an identifier for the SNMP engine on the Switch.

Format

config snmp engineID <snmp_engineID 10-64>

Parameters

<snmp_engineID 10-64> - Enter the SNMP engine ID here. It is octet string type. It accepts the hex number directly. This value must be between 10 and 64.

Restrictions

Only Administrators can issue this command.

Example

To configure SNMP engine ID to “1023457890”:

```
DGS-3000-28XMP:admin# config snmp engineID 1023457890
Command: config snmp engineID 1023457890

Success.

DGS-3000-28XMP:admin#
```

80-18 show snmp engineID

Description

This command is used to display the identification of the SNMP engine on the Switch. The default value is suggested in RFC2271. The very first bit is 1, and the first four octets are set to the binary equivalent of the agent’s SNMP management private enterprise number as assigned by IANA, D-Link is 171. The fifth octet is 03 to indicates the rest is the MAC address of this device. The 6th –11th octets is MAC address.

Format

show snmp engineID

Parameters

None.

Restrictions

None.

Example

To show SNMP engine ID:

```
DGS-3000-28XMP:admin#show snmp engineID
Command: show snmp engineID

SNMP Engine ID : 800000ab03000102e30400

DGS-3000-28XMP:admin#
```

80-19 enable snmp

Description

This command is used to enable the SNMP function.

Format

enable snmp

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable SNMP:

```
DGS-3000-28XMP:admin# enable snmp
Command: enable snmp

Success.

DGS-3000-28XMP:admin#
```

80-20 disable snmp

Description

This command is used to disable the SNMP function.

Format

disable snmp

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To disable SNMP:

```
DGS-3000-28XMP:admin# disable snmp
Command: disable snmp

Success.

DGS-3000-28XMP:admin#
```

80-21 config snmp system_name

Description

This command is used to configure the name for the Switch.

Format

config snmp system_name {<sw_name>}

Parameters

<sw_name> - (Optional) Enter the system name with a maximum of 128 characters here.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the Switch name for “DGS-3000 Switch”:

```
DGS-3000-28XMP:admin# config snmp system_name DGS-3000 Switch
Command: config snmp system_name DGS-3000 Switch

Success.

DGS-3000-28XMP:admin#
```

80-22 config snmp system_location

Description

This command is used to enter a description of the location of the Switch.

Format

config snmp system_location {<sw_location>}

Parameters

<sw_location> - (Optional) Enter the system location string with a maximum of 128 characters here.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the Switch location for “HQ 5F”:

```
DGS-3000-28XMP:admin# config snmp system_location HQ 5F
Command: config snmp system_location HQ 5F

Success.

DGS-3000-28XMP:admin#
```

80-23 config snmp system_contact

Description

This command is used to enter the name of a contact person who is responsible for the Switch.

Format

config snmp system_contact {<sw_contact>}

Parameters

<sw_contact> - (Optional) Enter the system contact string with a maximum of 128 characters here.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the Switch contact to “MIS Department II”:

```
DGS-3000-28XMP:admin# config snmp system_contact "MIS Department II"
Command: config snmp system_contact "MIS Department II"

Success.

DGS-3000-28XMP:admin#
```

80-24 enable snmp traps

Description

This command is used to enable SNMP trap support.

Format

enable snmp traps

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable SNMP trap support:

```
DGS-3000-28XMP:admin# enable snmp traps
Command: enable snmp traps

Success.

DGS-3000-28XMP:admin#
```

80-25 disable snmp traps

Description

This command is used to disable SNMP trap support on the Switch.

Format

disable snmp traps

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To prevent SNMP traps from being sent from the Switch:

```
DGS-3000-28XMP:admin# disable snmp traps
Command: disable snmp traps

Success.

DGS-3000-28XMP:admin#
```

80-26 enable snmp authenticate_traps

Description

This command is used to enable SNMP authentication failure trap support.

Format

enable snmp authenticate_traps

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable SNMP authentication trap support:

```
DGS-3000-28XMP:admin# enable snmp authenticate_traps
Command: enable snmp authenticate_traps

Success.

DGS-3000-28XMP:admin#
```

80-27 disable snmp authenticate_traps

Description

This command is used to disable SNMP authentication failure trap support.

Format

disable snmp authenticate_traps

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To disable SNMP authentication trap support:

```
DGS-3000-28XMP:admin# disable snmp authenticate_traps
Command: disable snmp authenticate_traps

Success.

DGS-3000-28XMP:admin#
```

80-28 enable snmp linkchange_traps

Description

This command is used to configure the sending of linkchange traps.

Format

enable snmp linkchange_traps

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable the sending of linkchange traps:

```
DGS-3000-28XMP:admin# enable snmp linkchange_traps
Command: enable snmp linkchange_traps

Success.

DGS-3000-28XMP:admin#
```

80-29 disable snmp linkchange_traps

Description

This command is used to configure the sending of linkchange traps.

Format

disable snmp linkchange_traps

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To disable the sending of linkchange traps:

```
DGS-3000-28XMP:admin# disable snmp linkchange_traps
Command: disable snmp linkchange_traps

Success.

DGS-3000-28XMP:admin#
```

80-30 config snmp linkchange_traps ports

Description

This command is used to enable or disable the sending of linkChange traps through the specified port(s).

Format

config snmp linkchange_traps ports [all | <portlist>] [enable | disable]

Parameters

all - Specifies to configure all ports.
<portlist> - Enter a range of ports to be configured.
enable - Specifies to enable sending of the link change trap for this port.
disable - Specifies to disable sending of the link change trap for this port.

Restrictions

Only Administrators can issue this command.

Example

To configure the sending of linkchange traps:

```
DGS-3000-28XMP:admin# config snmp linkchange_traps ports 1-4 enable
Command: config snmp linkchange_traps ports 1-4 enable

Success.

DGS-3000-28XMP:admin#
```

80-31 config snmp coldstart_traps

Description

This command is used to configure the trap for coldstart event.

Format

config snmp coldstart_traps [enable | disable]

Parameters

enable - Specifies to enable the trap of the coldstart event. This is the default option.
disable - Specifies to disable the trap of the coldstart event.

Restrictions

Only Administrators can issue this command.

Example

To configure the trap for coldstart event:

```
DGS-3000-28XMP:admin# config snmp coldstart_traps enable
Command: config snmp coldstart_traps enable

Success.

DGS-3000-28XMP:admin#
```

80-32 config snmp warmstart_traps

Description

This command is used to configure the trap state for warmstart event.

Format

config snmp warmstart_traps [enable | disable]

Parameters

enable - Specifies to enable the trap of the warmstart event. This is the default option.
disable - Specifies to disable the trap of the warmstart event.

Restrictions

Only Administrators can issue this command.

Example

To configure the trap state for warmstart event:

```
DGS-3000-28XMP:admin# config snmp warmstart_traps enable
Command: config snmp warmstart_traps enable

Success.

DGS-3000-28XMP:admin#
```

80-33 show snmp traps

Description

This command is used to display the SNMP trap sending status.

Format

show snmp traps {linkchange_traps {ports <portlist>}}

Parameters

linkchange_traps - (Optional) Specifies to display the SNMP trap sending status.
ports - (Optional) Specifies the ports to be displayed. **<portlist>** - Enter the list of ports used here.

Restrictions

None.

Example

To display SNMP trap sending status:

```
DGS-3000-28XMP:admin# show snmp traps
Command: show snmp traps

SNMP Traps         : Enabled
Authenticate Trap  : Enabled
Linkchange Traps   : Enabled
Coldstart Traps    : Enabled
Warmstart Traps    : Enabled

DGS-3000-28XMP:admin#
```

80-34 config rmon trap

Description

This command is used to configure the trap state for RMON events.

Format

config rmon trap {rising_alarm [enable | disable] | falling_alarm [enable | disable]}(1)

Parameters

rising_alarm - Specifies the trap state for rising alarm. The default state is enabled. **enable** - Specifies that the rising alarm function will be enabled. **disable** - Specifies that the rising alarm function will be disabled.
falling_alarm - Specifies the trap state for falling alarm. The default state is enabled. **enable** - Specifies that the falling alarm function will be enabled. **disable** - Specifies that the falling alarm function will be disabled.

Restrictions

Only Administrators can issue this command.

Example

To configure the trap state for RMON events:

```
DGS-3000-28XMP:admin# config rmon trap rising_alarm disable
Command: config rmon trap rising_alarm disable

Success.

DGS-3000-28XMP:admin#
```

80-35 show rmon

Description

This command is used to display the RMON related setting.

Format

show rmon

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To display the RMON related setting:

```
DGS-3000-28XMP:admin# show rmon
Command: show rmon

RMON Rising Alarm Trap      : Enabled
RMON Falling Alarm Trap     : Enabled

DGS-3000-28XMP:admin#
```

Chapter 81 Single IP Management Command List

enable sim
disable sim
show sim {[candidates {<candidate_id 1-100>} | members {<member_id 1-32>} | group {commander_mac <macaddr>} | neighbor]}
reconfig {member_id <value 1-32> | exit}
config sim_group [add <candidate_id 1-100> {<password>} | delete <member_id 1-32>]
config sim [{[commander {group_name <groupname 64>} | candidate] | dp_interval <sec 30-90> | hold_time <sec 100-255>}]
download sim_ms [firmware_from_tftp | configuration_from_tftp] {[<ipaddr> | <ipv6addr>] <path_filename> {[members <mslist 1-32> | all]}}
upload sim_ms [configuration_to_tftp | log_to_tftp] {[<ipaddr> | <ipv6addr>] <path_filename> {[members <mslist> | all]}}
config sim trap [enable | disable]

81-1 enable sim

Description

This command is used to configure the single IP management on the Switch as enabled.

Format

enable sim

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable SIM:

```
DGS-3000-28XMP:admin# enable sim
Command: enable sim

Success.

DGS-3000-28XMP:admin#
```

81-2 disable sim

Description

This command is used to disable single IP management on the Switch.

Format

disable sim

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To disable SIM:

```
DGS-3000-28XMP:admin# disable sim
Command: disable sim

Success.

DGS-3000-28XMP:admin#
```

81-3 show sim

Description

This command is used to display the current information of the specific sort of devices.

Format

show sim {[candidates {<candidate_id 1-100>} | members {<member_id 1-32>} | group {commander_mac <macaddr>} | neighbor]}

Parameters

candidates - (Optional) Specifies the candidate devices. **<candidate_id 1-100>** - (Optional) Enter the candidate device ID here. This value must be between 1 and 100.
members - (Optional) Specifies the member devices. **<member_id 1-32>** - (Optional) Enter the member device ID here. This value must be between 1 and 32.
group - (Optional) Specifies other group devices. **commander_mac** - (Optional) Specifies the commander MAC address used. **<macaddr>** - Enter the commander MAC address used here.
neighbor - (Optional) Specifies other neighbor devices.

Restrictions

None.

Example

To display general SIM information:

```
DGS-3000-28XMP:admin#show sim
Command: show sim

SIM Version        : VER-1.61
Firmware Version   : 4.00.010
Device Name        :
MAC Address        : F0-7D-68-15-10-00
Capabilities       : L2
Platform           : DGS-3000-28XMP L2 Switch
SIM State          : Disabled
Role State         : Candidate
Discovery Interval : 30 sec
Hold Time          : 100 sec

DGS-3000-28XMP:admin#
```

To show the candidate information in summary, if user specify candidate ID, it would show information in detail:

```
DGS-3000-28LP:admin#show sim candidates
Command: show sim candidates

ID  MAC Address       Platform /              Hold  Firmware  Device Name
                      Capability              Time  Version
--- ----------------- ----------------------- ----- --------- ----------------
1  00-01-02-03-E4-00  DGS-3000-52L          94    1.00.010  default:03-E4-00
                      L2 Switch
2  00-01-02-03-D4-00  DGS-3000-28XS         86    1.00.010  default:03-D4-00
                      L2 Switch
3  00-01-02-03-A4-00  DGS-3000-28X          90    1.00.010  default:03-A4-00
                      L2 Switch
4  00-01-02-03-B4-00  DGS-3000-52X          99    1.00.010  default:03-B4-00
                      L2 Switch

Total Entries: 4

DGS-3000-28LP:admin#
```

To show the member information in summary, if user specify member id, it will show information in detail:

```
DGS-3000-28LP:admin#show sim members
Command: show sim members

ID  MAC Address       Platform /              Hold  Firmware  Device Name
                      Capability              Time  Version
--- ----------------- ----------------------- ----- --------- ----------------
1  00-01-02-03-A4-00  DGS-3000-28X          93    1.00.010
                      L2 Switch
2  00-01-02-03-E4-00  DGS-3000-52L          97    1.00.010
                      L2 Switch
3  00-01-02-03-D4-00  DGS-3000-28XS         91    1.00.010
                      L2 Switch

Total Entries: 3

DGS-3000-28LP:admin#
```

To show other groups information in summary, if user specify group name, it will show information in detail:

```
DGS-3000-28LP:admin#show sim group
Command: show sim group

SIM Group Name   : Group_2

ID  MAC Address       Platform /              Hold  Firmware  Device Name
                      Capability              Time  Version
--- ----------------- ----------------------- ----- --------- ----------------
*1  00-01-02-03-A4-00 DGS-3000-28X          82    1.00.010
                      L2 Switch

SIM Group Name   : Group_1

ID  MAC Address       Platform /              Hold  Firmware  Device Name
                      Capability              Time  Version
--- ----------------- ----------------------- ----- --------- ----------------
*1  00-01-02-03-B4-00 DGS-3000-52X          91    1.00.010
                      L2 Switch


Total Entries: 2

DGS-3000-28LP:admin#
```

To show neighbor table of SIM:

```
DGS-3000-28LP:admin#show sim neighbor
Command: show sim neighbor

Neighbor Info Table

Port   MAC Address        Role
------ ------------------ ---------
19     00-01-02-03-B4-00  Commander
23     00-01-02-03-E4-00  Candidate

Total Entries: 4

DGS-3000-28LP:admin#
```

81-4 reconfig

Description

This command is used reconnect to a SIM member using Telnet by specifying the member ID.

Format

reconfig {member_id <value 1-32> | exit}

Parameters

member_id - (Optional) Specifies the serial number of the member. **<value 1-32>** - Enter the serial number of the member here.
exit - (Optional) Specifies to exit from the telnet session.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To reconnect to the SIM member ID 1 using Telnet:

```
DGS-3000-28XMP:admin# reconfig member_id 1
Command: reconfig member_id 1

DGS-3000-28XMP:admin#
Login:
```

81-5 config sim_group

Description

This command is used to configure group information.

Format

config sim_group [add <candidate_id 1-100> {<password>} | delete <member_id 1-32>]

Parameters

add - Specifies to add a specific candidate to the group.

<candidate_id 1-100> - Enter the candidate ID to be added to the group here. This value must be between 1 and 100.

<password> - (Optional) Enter the password of candidate if necessary.

delete - Specifies to delete a member from the group.

<member_id 1-32> - Enter the member ID of the member to be removed from the group here. This value must be between 1 and 32.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To add a member:

```
DGS-3000-28XMP:admin# config sim_group add 2
Command: config sim_group add 2

Please wait for ACK !!!
SIM Configure Success !!!

Success.

DGS-3000-28XMP:admin#
```

To delete a member:

```
DGS-3000-28XMP:admin# config sim_group delete 1
Command: config sim_group delete 1

Please wait for ACK !!!
SIM Configure Success !!!

Success.

DGS-3000-28XMP:admin#
```

81-6 config sim

Description

This command is used to configure the role state and the parameters of the discovery protocol on the Switch.

Format

config sim [{[commander {group_name <groupname 64>} | candidate] | dp_interval <sec 30-90> | hold_time <sec 100-255>}]

Parameters

commander - (Optional) Specifies to transfer the role to the commander. **group_name** - (Optional) Specifies that if the user is the commander, the user can update the name of group. **<groupname 64>** - Enter the group name here. This name can be up to 64 characters long.
candidate - (Optional) Specifies to transfer the role to the candidate.
dp_interval - (Optional) Specifies the time in seconds between discoveries. **<sec 30-90>** - Enter the discovery time here in seconds. This value must be between 30 and 90 seconds.
hold_time - (Optional) Specifies the time in seconds the device holds the discovery result. **<sec 100-255>** - Enter the hold time here in seconds. This value must be between 100 and 255.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To transfer to commander:

```
DGS-3000-28XMP:admin# config sim commander
Command: config sim commander

Success.

DGS-3000-28XMP:admin#
```

To transfer to candidate:

```
DGS-3000-28XMP:admin# config sim candidate
Command: config sim candidate

Success.

DGS-3000-28XMP:admin#
```

To update name of group:

```
DGS-3000-28XMP:admin# config sim commander group_name mygroup
Command: config sim commander group_name mygroup

Success.

DGS-3000-28XMP:admin#
```

To change the time interval of the discovery protocol:

```
DGS-3000-28XMP:admin# config sim dp_interval 30
Command: config sim dp_interval 30

Success.

DGS-3000-28XMP:admin#
```

To change the hold time of discovery protocol:

```
DGS-3000-28XMP:admin# config sim hold_time 200
Command: config sim hold_time 200

Success.

DGS-3000-28XMP:admin#
```

81-7 download sim_ms

Description

This command is used to download firmware or configuration to the specified device.

Format

download sim_ms [firmware_from_tftp | configuration_from_tftp] {[<ipaddr> | <ipv6addr>] <path_filename> {[members <mslist 1-32> | all]}}

Parameters

firmware_from_tftp - Specifies that the firmware will be downloaded from the TFTP server.
configuration_from_tftp - Specifies that the configuration will be downloaded from the TFTP server.
<ipaddr> - (Optional) Enter the IP address of the TFTP server.
<ipv6addr> - (Optional) Enter the IPv6 address of TFTP server. If the IPv6 address is a link-local address, the IP interface name needs to be specified in the following format: IPv6Address%Interface-ID.
<path_filename> - Enter the file path of the firmware or configuration in the TFTP server.
members - (Optional) Specifies a range of members who can download this firmware or configuration.
<mslist 1-32> - Enter the member list used here. This value must be between 1 and 32.
all - (Optional) Specifies that all members will be used.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To download configuration:

```
DGS-3000-28XMP:admin# download sim_ms configuration_from_tftp 10.55.47.1 D:\dwl600x.tfp
members 1
Commands: download sim_ms configuration_from_tftp 10.55.47.1 D:\dwl600x.tfp members 1

This device is updating configuration.  Please wait several minutes ...

Download Status :

ID   MAC Address        Result
---  -----------------  ----------------
1   00-01-02-03-04-00  Success

DGS-3000-28XMP:admin#
```

To download firmware:

```
DGS-3000-28XMP:admin# download sim_ms firmware_from_tftp 10.55.47.1 D:\test.txt members 1
Commands: download sim_ms firmware_from_tftp 10.55.47.1 D:\test.txt members 1

This device is updating firmware.  Please wait several minutes ...

Download Status :

ID   MAC Address        Result
---  -----------------  ----------------
1   00-01-02-03-04-00  Success

DGS-3000-28XMP:admin#
```

To download configuration via IPv6:

```
DGS-3000-28XMP:admin# download sim_ms configuratin_from_tftp 2001::1234 D:\config.cfg 1
Commands: download sim_ms configuratin_from_tftp 2001::1234 D:\config.cfg 1

This device is updating configuration.  Please wait several minutes ...

Download Status :

ID   MAC Address        Result
---  -----------------  ----------------
1   00-01-02-03-04-00  Success
2   00-07-06-05-04-03  Fail

DGS-3000-28XMP:admin#
```

81-8 upload sim_ms

Description

This command is used to upload the configuration to a TFTP server.

Format

upload sim_ms [configuration_to_tftp | log_to_tftp] {[<ipaddr> | <ipv6addr>] <path_filename> {[members <mslist> | all]}}

Parameters

configuration_to_tftp - Specifies that the configuration will be uploaded to the TFTP server.

log_to_tftp - Specifies that the log file will be uploaded to the TFTP server.

<ipaddr> - (Optional) Enter the IP address of the TFTP server.

<ipv6addr> - (Optional) Enter the IPv6 address of TFTP server. If the IPv6 address is a link-local address, the IP interface name needs to be specified in the following format: IPv6Address%Interface-ID.

<path_filename> - Enter the file path to store the configuration in the TFTP server.

members - (Optional) Specifies a range of members who can upload this configuration.

<mslist> - Enter the member list used here.

all - (Optional) Specifies that all members will be used.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To upload configuration:

```
DGS-3000-28XMP:admin# upload sim_ms configuration_to_tftp 10.55.47.1 D:\configuration.txt
members 1
Command: upload sim_ms configuration_to_tftp 10.55.47.1 D:\configuration.txt members 1

This device is uploading configuration.  Please wait several minutes ...

Upload Status :

ID   MAC Address       Result
---  ----------------- ----------------
1   00-1A-2D-00-12-12 Success

DGS-3000-28XMP:admin#
```

To upload log via IPv6:

```
DGS-3000-28XMP:admin# upload sim_ms log_to_tftp 2001::1234 D:\log.txt members 1
Command: upload sim_ms log_to_tftp 2001::1234 D:\log.txt members 1

This device is uploading log. Please wait several minutes ...

Upload Status :

ID   MAC Address       Result
---  ----------------- ----------------
00-01-02-03-04-00 Success

DGS-3000-28XMP:admin#
```

81-9 config sim trap

Description

This command is used to control sending of traps issued from the member switch.

NOTE: This command is only for the commander switch.

Format

config sim trap [enable | disable]

Parameters

enable - Specifies to enable the trap state.
disable - Specifies to disable the trap state.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable sim trap:

```
DGS-3000-28XMP:admin# config sim trap enable
Command: config sim trap enable

Success.

DGS-3000-28XMP:admin#
```

Chapter 82 Static Route Command List

create iproute [default | <network_address>] <ipaddr> {<metric 1-65535>} {[primary | backup]}
delete iproute [default | <network_address>] <ipaddr>
show iproute {<network_address> | <ipaddr>} {static}
create ipv6route [default | <ipv6networkaddr>] [<ipif_name 12> <ipv6addr> | <ipv6addr>] {<metric 1-65535>} {[primary | backup]}
delete ipv6route [[default | <ipv6networkaddr>] [<ipif_name 12> <ipv6addr> | <ipv6addr>] | all]
show ipv6route {[<ipv6networkaddr> | <ipv6addr>]} {static}

82-1 create iproute

Description

This command is used to create an IP static route entry in the IP routing table of 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 and not set this route to be a multipath route.

Format

create iproute [default | <network_address>] <ipaddr> {<metric 1-65535>} {[primary | backup]}

Parameters

default - Specifies to create an IP default route (0.0.0.0/0).
network_address - Specifies the IP address and net mask of the destination route. The address and the mask can be set using the traditional format (for example, 10.1.2.3/255.0.0.0) or in CIDR format (for example,10.1.2.3/16).
<ipaddr> - Enter the IP address for the IP route.
<metric 1-65535> - (Optional) Enter the routing protocol metric entry representing the number of routers between the Switch and the IP address above. The default setting is 1.
primary - (Optional) Specifies the route as the primary route to the destination
backup - (Optional) Specifies the route as the backup route to the destination.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To add an IP static route entry:

```
DGS-3000-28XMP:admin#create iproute 10.48.74.121/255.0.0.0 10.1.1.254 primary
Command: create iproute 10.48.74.121/8 10.1.1.254 primary

Success.

DGS-3000-28XMP:admin#
```

82-2 delete iproute

Description

This command is used to delete an IP route entry from the Switch's IP routing table.

Format

delete iproute [default | <network_address>] <ipaddr>

Parameters

default - Specifies to delete an IP default route (0.0.0.0/0).
<network_address> - Enter the destination IP address and net mask route. The address and the mask can be set by the traditional format (for example, 10.1.2.3/255.0.0.0 or in CIDR format, 10.1.2.3/16).
<ipaddr> - Enter the next hop IP address route that needs to be deleted.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete an IP route entry:

```
DGS-3000-28XMP:admin#delete iproute 10.48.74.121/255.0.0.0 10.1.1.254
Command: delete iproute 10.48.74.121/8 10.1.1.254

Success.

DGS-3000-28XMP:admin#
```

82-3 show iproute

Description

This command is used to display current IP routing table of the Switch.

Format

show iproute {<network_address> | <ipaddr>} {static}

Parameters

<network_address> - (Optional) Enter the destination network address of the route to be displayed.
<ipaddr> - (Optional) Enter the destination IP address of the route to be displayed. The longest prefix matched route will be displayed.
static - (Optional) Specifies to display only static routes. One static route may be active or inactive.

Restrictions

None.

Example

To display the contents of the IP routing table:

```
DGS-3000-28XMP:admin#show iproute
Command: show iproute


Routing Table

IP Address/Netmask  Gateway          Interface     Metric    Protocol
------------------  ---------------  ------------  --------  --------
10.0.0.0/8          0.0.0.0          System        1         Local

Total Entries: 1


DGS-3000-28XMP:admin#
```

To display the contents of the static IP routing table:

```
DGS-3000-28XMP:admin#show iproute static
Command: show iproute static


Routing Table

IP Address/Netmask  Gateway          Metric   Protocol  Backup    Status
------------------  ---------------  -------  --------  --------  --------
10.0.0.0/8          10.1.1.254       1        Static    Primary   Inactive

Total Entries: 1


DGS-3000-28XMP:admin#
```

82-4 create ipv6route

Description

This command is used to create an IPv6 static route. The next hop can be an IPv6 router. The primary route has higher priority than backup. When primary route is inactive, the backup route will be used. One static route will be primary route by default if there is no primary route to this destination yet.

Format

create ipv6route [default | <ipv6networkaddr>] [<ipif_name 12> <ipv6addr> | <ipv6addr>] {<metric 1-65535>} {[primary | backup]}

Parameters

default - Specifies an IPv6 default route.
<ipv6networkaddr> - Enter the IPv6 address and prefix of the destination of the route.
<ipif_name 12> - Enter the interface name to specify the IP interface for this route from an existing interface. Enter the IPv6 route name using a maximum of 12 characters. **<ipv6addr>** - Enter the next hop address of the route.
<ipv6addr> - Specifies the next ipv6 address hop of the route.
<metric 1-65535> - (Optional) Enter the metric value here. The default value is 1.
primary - (Optional) Specifies the route as the primary route to the destination.
backup - (Optional) Specifies the route as the backup route to the destination

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To create an IPv6 static route with outgoing interface System:

```
DGS-3000-28XMP:admin#create ipv6route 5000::/64 System FE80::1
Command: create ipv6route 5000::/64 System FE80::1

Success.

DGS-3000-28XMP:admin#
```

82-5 delete ipv6route

Description

This command is used to delete an IPv6 static route. If the next hop is a global address, it is not needed to indicate the interface name. If the next hop is a link local address, then the interface name must be specified.

Format

delete ipv6route [[default | <ipv6networkaddr>] [<ipif_name 12> <ipv6addr> | <ipv6addr>] | all]

Parameters

default - Specifies the default route.
<ipv6networkaddr> - Enter the destination network route.
<ipif_name 12> - Enter the IP interface name used here. This name can be up to 12 characters long. **<ipv6addr>** - Enter the next hop address for the route.

<ipv6addr> - Enter the next hop address for the route.
all - Specifies to delete all created static routes.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete an IPv6 static route:

```
DGS-3000-28XMP:admin#delete ipv6route 5000::/64 System FE80::1
Command: delete ipv6route 5000::/64 System FE80::1

Success.

DGS-3000-28XMP:admin#
```

82-6 show ipv6route

Description

This command is used to display IPv6 routes.

Format

show ipv6route {[<ipv6networkaddr> | <ipv6addr>]} {static}

Parameters

<ipv6networkaddr> - (Optional) Enter the destination network address of the route to be displayed.
<ipv6addr> - (Optional) Enter the destination IPv6 address of the route to be displayed. The longest prefix matched route will be displayed
static - (Optional) Specifies to display only static routes. One static route may be active or inactive.

Restrictions

None.

Example

To display all the IPv6 routes:

```
DGS-3000-28XMP:admin#show ipv6route
Command: show ipv6route

IPv6 Prefix: 3710::/64                        Protocol: Local  Metric: 1
Next Hop   : ::                               IPIF    : System


Total Entries: 1


DGS-3000-28XMP:admin#
```

Chapter 83 Syslog and Trap Source-interface Command List

config syslog source_ipif [<ipif_name 12> {<ipaddr> | <ipv6addr>} | none]
show syslog source_ipif
config trap source_ipif [<ipif_name 12> {<ipaddr> | <ipv6addr>} | none]
show trap source_ipif

83-1 config syslog source_ipif

Description

This command is used to configure syslog source IP interface.

Format

config syslog source_ipif [<ipif_name 12> {<ipaddr> | <ipv6addr>} | none]

Parameters

<ipif_name 12> - Enter the IP interface name here. This name can be up to 12 characters long. The lowest IPv4/IPv6 address associated with the interface will be used as the source IPv4/IPv6 address if the IP address is not specified. **<ipaddr>** - (Optional) Enter the IP address used for the configuration here. **<ipv6addr>** - (Optional) Enter the IPv6 address used for the configuration here.
none - Specifies to clear the configured source IP interface.

Restrictions

Only Administrators and Operators can issue this command.

Example

Configure syslog source IP interface:

```
DGS-3000-28XMP:admin# config syslog source_ipif ipif3 14.0.0.5
Command: config syslog source_ipif ipif3 14.0.0.5

Success

DGS-3000-28XMP:admin#
```

To clear the configured source IP interface for syslog:

```
DGS-3000-28XMP:admin# config syslog source_ipif none
Command: config syslog source_ipif none

Success

DGS-3000-28XMP:admin#
```

83-2 show syslog source_ipif

Description

This command is used to display the syslog source IP interface.

Format

show syslog source_ipif

Parameters

None.

Restrictions

None.

Example

Show syslog source IP interface:

```
DGS-3000-28XMP:admin#show syslog source_ipif
Command: show syslog source_ipif

 Syslog Source IP Interface Configuration:

 IP Interface           : ipif3
 IPv4 Address           : 192.168.0.1
 IPv6 Address           : None

DGS-3000-28XMP:admin#
```

83-3 config trap source_ipif

Description

This command is used to configure trap source IP interface.

Format

config trap source_ipif [<ipif_name 12> {<ipaddr> | <ipv6addr>} | none]

Parameters

<ipif_name 12> - Enter the IP interface name here. This name can be up to 12 characters long. The lowest

IPv4/IPv6 address associated with the interface will be used as the source IPv4/IPv6 address if the IP address is not specified.

<ipaddr> - (Optional) Enter the IP address used for the configuration here.

<ipv6addr> - (Optional) Enter the IPv6 address used for the configuration here.

none - Specifies to clear the configured source IP interface.

Restrictions

Only Administrators and Operators can issue this command.

Example

Configure trap source IP interface:

```
DGS-3000-28XMP:admin# config trap source_ipif System
Command: config trap source_ipif System

Success

DGS-3000-28XMP:admin#
```

To clear the configured trap source IP interface:

```
DGS-3000-28XMP:admin# config trap source_ipif none
Command: config trap source_ipif none

Success

DGS-3000-28XMP:admin#
```

83-4 show trap source_ipif

Description

This command is used to display the trap source IP interface.

Format

show trap source_ipif

Parameters

None.

Restrictions

None.

Example

Show trap source IP interface:

```
DGS-3000-28XMP:admin#show trap source_ipif
Command: show trap source_ipif

 Trap Source IP Interface Configuration:

 IP Interface           : System
 IPv4 Address           : None
 IPv6 Address           : None

DGS-3000-28XMP:admin#
```

Chapter 84 System Log Command List

enable syslog
disable syslog
create syslog host <index 1-4> ipaddress [<ipaddr> | <ipv6addr>] {severity [emergency | alert | critical | error | warning | notice | informational | debug | <level 0-7>] | facility [local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7] | udp_port <udp_port_number> | state [enable | disable]}
config syslog host [<index> | all] {severity [emergency | alert | critical | error | warning | notice | informational | debug | <level 0-7>] | facility [local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7] | udp_port <udp_port_number> | ipaddress [<ipaddr> |<ipv6addr>] | state [enable | disable]}
config log_save_timing [time_interval <min 1-65535> | on_demand | log_trigger]
delete syslog host [<index 1-4> | all]
clear log
clear attack_log
show log {[index <value_list> | severity {module <module_list>} {emergency | alert | critical | error | warning | notice | informational | debug | <level_list 0-7>} | module<module_list>]}
show log_software_module
show syslog
show syslog host {<index 1-4>}
show log_save_timing
show attack_log {index <value_list>}
create log_discriminator <name 15> {facility [drops <module_list> | includes <module_list>] | severity [drops <level_list 0-7> | includes <level_list 0-7>]}(1)
delete log_discriminator <name 15>
show log_discriminator
enable log_monitor
disable log_monitor
config log_monitor severity [emergency | alert | critical | error | warning | notice | informational | debug | <level 0-7>]
config log_monitor discriminator {<name 15>}
show log_monitor
enable log_console
disable log_console
config log_console severity [emergency | alert | critical | error | warning | notice | informational | debug | <level 0-7>]
config log_console discriminator {<name 15>}
show log_console

84-1 enable syslog

Description

This command is used to enable the sending of syslog messages.

Format

enable syslog

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable the sending of syslog messages:

```
DGS-3000-28XMP:admin# enable syslog
Command: enable syslog

Success.

DGS-3000-28XMP:admin#
```

84-2 disable syslog

Description

This command is used to disable the sending of syslog messages.

Format

disable syslog

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To disable the sending of syslog messages:

```
DGS-3000-28XMP:admin# disable syslog
Command: disable syslog

Success.

DGS-3000-28XMP:admin#
```

84-3 create syslog host

Description

This command is used to create a new syslog host. The user can choose and report specific levels of messages to a specific host. When the user chooses a specific level for a specific host, messages which are at that severity level or higher will be reported to that host.

Format

create syslog host <index 1-4> ipaddress [<ipaddr> | <ipv6addr>] {severity [emergency | alert | critical | error | warning | notice | informational | debug | <level 0-7>] | facility [local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7] | udp_port <udp_port_number> | state [enable | disable]}

Parameters

<index 1-4> - Enter the host index value here.

ipaddress - Specifies the IP address for the host.

- **<ipaddr>** - Enter the IP address for the host.
- **<ipv6addr>** - Enter the IPv6 address for the host.

severity - (Optional) Specifies the severity level.

- **emergency** - Severity level 0.
- **alert** - Severity level 1.
- **critical** - Severity level 2.
- **error** - Severity level 3.
- **warning** - Severity level 4.
- **notice** - Severity level 5.
- **informational** - Severity level 6.
- **debug** - Severity level 7.
- **<level 0-7>** - Enter the severity level value here. This value must be between 0 and 7.

facility - (Optional) Some of the operating system daemons and processes have been assigned Facility values. Processes and daemons that have not been explicitly assigned a Facility may use any of the "local use" facilities or they may use the "user-level" Facility. Those Facilities that have been designated are shown below. This facility setting will be put in the syslog packet when it is sent to a specific syslog server.

- **local0** - Specifies that the user-defined facility will be set to local 0.
- **local1** - Specifies that the user-defined facility will be set to local 1.
- **local2** - Specifies that the user-defined facility will be set to local 2.
- **local3** - Specifies that the user-defined facility will be set to local 3.
- **local4** - Specifies that the user-defined facility will be set to local 4.
- **local5** - Specifies that the user-defined facility will be set to local 5.
- **local6** - Specifies that the user-defined facility will be set to local 6.
- **local7** - Specifies that the user-defined facility will be set to local 7.

udp_port - (Optional) Specifies the UDP port number.

- **<udp_port_number>** - Enter the UDP port number used here.

state - (Optional) Specifies the syslog protocol is used for the transmission of event notification messages across networks to a host. The option enables or disables the host to receive such messages.

- **enable** - Specifies that the host to receive such messages will be enabled.
- **disable** - Specifies that the host to receive such messages will be disabled.

Restrictions

Only Administrators and Operators can issue this command.

Example

Adds a new syslog host:

```
DGS-3000-28XMP:admin# create syslog host 1 ipaddress 10.90.90.1 severity debug facility
local0
Command: create syslog host 1 ipaddress 10.90.90.1 severity debug facility local0

Success.

DGS-3000-28XMP:admin#
```

84-4 config syslog host

Description

This command is used to configure the syslog host configurations. The user can choose and report a specific level of messages to a specific host. When the user chooses a specific level for a specific host, messages which are at that severity level or higher will be reported to the specified host.

Format

config syslog host [<index> | all] {severity [emergency | alert | critical | error | warning | notice | informational | debug | <level 0-7>] | facility [local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7] | udp_port <udp_port_number> | ipaddress [<ipaddr> |<ipv6addr>] | state [enable | disable]}

Parameters

<index> - Enter the host index value here.

all - Specifies that all the host indexes will be used.

severity - (Optional) Specifies the severity level.

- **emergency** - Severity level 0.
- **alert** - Severity level 1.
- **critical** - Severity level 2.
- **error** - Severity level 3.
- **warning** - Severity level 4.
- **notice** - Severity level 5.
- **informational** - Severity level 6.
- **debug** - Severity level 7.
- **<level 0-7>** - Enter the severity level value here. This value must be between 0 and 7.

facility - (Optional) Some of the operating system daemons and processes have been assigned Facility values. Processes and daemons that have not been explicitly assigned a Facility may use any of the "local use" facilities or they may use the "user-level" Facility. Those Facilities that have been designated are shown below. This facility setting will be put in the syslog packet when it is sent to a specific syslog server.

- **local0** - Specifies that the user-defined facility will be set to local 0.
- **local1** - Specifies that the user-defined facility will be set to local 1.
- **local2** - Specifies that the user-defined facility will be set to local 2.
- **local3** - Specifies that the user-defined facility will be set to local 3.
- **local4** - Specifies that the user-defined facility will be set to local 4.
- **local5** - Specifies that the user-defined facility will be set to local 5.
- **local6** - Specifies that the user-defined facility will be set to local 6.

local7 - Specifies that the user-defined facility will be set to local 7.

udp_port - (Optional) Specifies the UDP port number.

<udp_port_number> - Enter the UDP port number used here.

ipaddress - (Optional) Specifies IP address for the host.

<ipaddr> - Enter the IP address used for the configuration here.

<ipv6addr> - Enter the IPv6 address used for the configuration here.

state - (Optional) Specifies the syslog protocol is used for the transmission of event notification messages across networks to a host. The option enables or disables the host to receive such messages.

enable - Specifies that the host to receive such messages will be enabled.

disable - Specifies that the host to receive such messages will be disabled.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the syslog host configuration:

```
DGS-3000-28XMP:admin# config syslog host all severity debug facility local0
Command: config syslog host all severity debug facility local0

Success.

DGS-3000-28XMP:admin#
```

84-5 config log_save_timing

Description

This command is used to set the method for saving the log.

Format

config log_save_timing [time_interval <min 1-65535> | on_demand | log_trigger]

Parameters

time_interval - Specifies the interval in minutes to save log to flash. (If no new log events occur in this period, the log is not saved.)

<min 1-65535> - Enter the time interval value here. This value must be between 1 and 65535 minutes.

on_demand - Specifies to save log to flash whenever the user enters the **save log** or **save all** command. This is the default setting.

log_trigger - Specifies to save log to flash whenever a new log event occurs.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the method for saving a log as on demand:

```
DGS-3000-28XMP:admin# config log_save_timing on_demand
Command: config log_save_timing on_demand

Success.

DGS-3000-28XMP:admin#
```

84-6 delete syslog host

Description

This command is used to delete the syslog host(s).

Format

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

Parameters

<index> - Enter the host index value here.
all - Specifies that all the host indexes will be used.

Restrictions

Only Administrators and Operators can issue this command.

Example

To delete the specific syslog host:

```
DGS-3000-28XMP:admin# delete syslog host 4
Command: delete syslog host 4

Success.

DGS-3000-28XMP:admin#
```

84-7 clear log

Description

This command is used to clear the Switch's history log.

Format

clear log

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To clear the Switch's history log:

```
DGS-3000-28XMP:admin# clear log
Command: clear log

Success.

DGS-3000-28XMP:admin#
```

84-8 clear attack_log

Description

This command is used to clear the attack log.

Format

clear attack_log

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To clear the master's attack log:

```
DGS-3000-28XMP:admin# clear attack_log
Command: clear attack_log

Success.

DGS-3000-28XMP:admin#
```

84-9 show log

Description

This command is used to display the Switch's history log entries.

Format

show log {[index <value_list> | severity {module <module_list>} {emergency | alert | critical | error | warning | notice | informational | debug | <level_list 0-7>} | module<module_list>]}

Parameters

index - (Optional) Specifies to configure index range of history log entries to display.
- **<value_list>** - Enter the index value here.

severity - (Optional) Specifies the severity level used.
- **module** - (Optional) Specifies the modules which are to be displayed. The module can be obtained by using the **show log_software_module** command. Use a comma to separate multiple modules.
  - **<module_list>** - Enter the module list value here.
- **emergency** - (Optional) Severity level 0
- **alert** - (Optional) Severity level 1
- **critical** - (Optional) Severity level 2
- **error** - (Optional) Severity level 3
- **warning** - (Optional) Severity level 4
- **notice** - (Optional) Severity level 5
- **informational** - (Optional) Severity level 6
- **debug** - (Optional) Severity level 7
- **<level_list 0-7>** - Specifies a list of severity level which is to be displayed. If there is more than one severity level, please separate them by comma. The level number is from 0 to 7.

module - (Optional) Specifies the modules which are to be displayed. The module can be obtained by using the show log_software_module command. Use a comma to separate multiple modules.
- **<module_list>** - Enter the module list value here.

If no parameter is specified, all history log entries will be displayed.

Restrictions

None.

Example

To display the Switch's history log:

```
DGS-3000-28XMP:admin# show log index 1-3
Command: show log index 1-3

Index Date       Time     Level   Log Text
----- ---------- -------- ------- ---------------------------------------------

3     2000-01-01 00:00:40 CRIT(2) System started up
2     2000-01-01 00:00:40 CRIT(2) System cold start
1     2000-01-01 01:49:30 INFO(6) Anonymous: execute command "reset system".

DGS-3000-28XMP:admin#
```

84-10 show log_software_module

Description

This command is used to display the protocols or applications that support the enhanced log. The enhanced log adds the module name and module ID. Network administrators can display logs by module name or module ID.

Format

show log_software_module

Parameters

None.

Restrictions

None.

Example

To display the protocols or applications that support the enhanced log:

```
DGS-3000-28XMP:admin#show log_software_module
Command: show log_software_module

CFM_EXT             DHCPv6_RELAY        ERPS                ERROR_LOG
MSTP

DGS-3000-28XMP:admin#
```

84-11 show syslog

Description

This command is used to display the syslog protocol global state.

Format

show syslog

Parameters

None.

Restrictions

None.

Example

To display the syslog protocol global state:

```
DGS-3000-28XMP:admin# show syslog
Command: show syslog

Syslog Global State: Enabled

DGS-3000-28XMP:admin#
```

84-12 show syslog host

Description

This command is used to display the syslog host configuration.

Format

show syslog host {<index 1-4>}

Parameters

<index> - (Optional) Enter the host index value here.
If no parameter is specified, all hosts will be displayed.

Restrictions

None.

Example

To show the syslog host information:

```
DGS-3000-28XMP:admin#show syslog host
Command: show syslog host

Syslog Global State: Enabled

Host  1
  IP Address        : 10.90.90.1
  Severity          : Debug(7)
  Facility          : Local0
  UDP Port          : 514
  Status            : Disabled

Total Entries : 1

DGS-3000-28XMP:admin#
```

84-13 show log_save_timing

Description

This command is used to show the method for saving the log.

Format

show log_save_timing

Parameters

None.

Restrictions

None.

Example

To show the timing method used for saving the log:

```
DGS-3000-28XMP:admin# show log_save_timing
Command: show log_save_timing

Saving Log Method: On_demand

DGS-3000-28XMP:admin#
```

84-14 show attack_log

Description

This command is used to display the attack log messages. The attack log message refers to log messages driven by modules such as DoS and the IP-MAC-port binding module. This type of log message may generate a large amount of messages and quickly cause the system to run out of system log storage. Therefore, for this type of log messages only the first log that is generated each minute can be stored in the system log, with the rest of them being stored in a separate table named attack log.

Format

show attack_log {index <value_list>}

Parameters

index - (Optional) Specifies the list of index numbers of the entries that need to be displayed. For example, show attack_log index 1-5 will display the attack log messages from 1 to 5. **<value_list>** - Enter the index numbers of the entries that needs to be displayed here.
If no parameter is specified, all entries in the attack log will be displayed.

Restrictions

None.

Example

To show dangerous messages on the master:

```
DGS-3000-28XMP:admin# show attack_log index 1
Command: show attack_log index 1

Index   Date       Time      Level     Log Text
----- ---------- -------- -------- ------------------------------------------
1      2008-10-17 15:00:14 CRIT(2)   Possible spoofing attack from IP: , MAC:
                                     0A-00-00-5A-00-01, port: 3

DGS-3000-28XMP:admin#
```

84-15 create log_discriminator

Description

This command is used to create a syslog logging discriminator.

Format

create log_discriminator <name 15> {facility [drops <module_list> | includes <module_list>] | severity [drops <level_list 0-7> | includes <level_list 0-7>]}(1)

Parameters

<name 15> - Enter the name of the discriminator.
facility - Specifies a sub-filter based on the facility string. **drops** - Specifies to drop the matching message. **<module_list>** - Enter a list of modules. **includes** - Specifies to include the matching message. **<module_list>** - Enter a list of modules.
severity - Specifies a sub-filter based on severity matching. **drops** - Specifies to drop the matching message. **<level_list 0-7>** - Enter a list of severity levels to be displayed. **includes** - Specifies to include the matching message. **<level_list 0-7>** - Enter a list of severity levels to be displayed.

Restrictions

Only Administrators and Operators can issue this command.

Example

To create a syslog logging discriminator, monitor-filter:

```
DGS-3000-28XMP:admin#create log_discriminator monitor-filter facility includes STP severity
includes 1,6
Command: create log_discriminator monitor-filter facility includes STP severity includes 1,6

Success.

DGS-3000-28XMP:admin#
```

84-16 delete log_discriminator

Description

This command is used to delete a syslog logging discriminator.

Format

delete log_discriminator <name 15>

Parameters

<name 15> - Enter the name of the discriminator.

Restrictions

Only Administrators and Operators can issue this command.

Example

To delete a syslog logging discriminator:

```
DGS-3000-28XMP:admin#delete log_discriminator monitor-filter
Command: delete log_discriminator monitor-filter

Success.

DGS-3000-28XMP:admin#
```

84-17 show log_discriminator

Description

This command is used to display syslog logging discriminators.

Format

show log_discriminator

Parameters

None.

Restrictions

None.

Example

To display syslog logging discriminators:

```
DGS-3000-28XMP:admin#show log_discriminator
Command: show log_discriminator

Active Message Discriminator:
   None

InActive Message Discriminator:
monitor-filter:
        severity group includes: 1,6
        facility includes: STP


DGS-3000-28XMP:admin#
```

84-18 enable log_monitor

Description

This command is used to enable logging system messages to Telnet or SSH.

Format

enable log_monitor

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable logging system messages to Telnet or SSH:

```
DGS-3000-28XMP:admin#enable log_monitor
Command: enable log_monitor

Success.

DGS-3000-28XMP:admin#
```

84-19 disable log_monitor

Description

This command is used to disable logging system messages to Telnet or SSH.

Format

disable log_monitor

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To disable logging system messages to Telnet or SSH:

```
DGS-3000-28XMP:admin#disable log_monitor
Command: disable log_monitor

Success.

DGS-3000-28XMP:admin#
```

84-20 config log_monitor severity

Description

This command is used to specify the severity level of messages logging to Telnet or SSH.

When a specific severity level is configured, messages at that severity level or higher will be logged to Telnet or SSH.

Format

config log_monitor severity [emergency | alert | critical | error | warning | notice | informational | debug | <level 0-7>]

Parameters

emergency - Specifies the severity level to 0.
alert - Specifies the severity level to 1.
critical - Specifies the severity level to 2.
error - Specifies the severity level to 3.
warning - Specifies the severity level to 4.
notice - Specifies the severity level to 5.
information - Specifies the severity level to 6.
debug - Specifies the severity level to 7.
<level 0-7> - Enter the severity level here. This value must be between 0 and 7.

Restrictions

Only Administrators and Operators can issue this command.

Example

To specify the severity level of messages at **error** (3):

```
DGS-3000-28XMP:admin#config log_monitor severity error
Command: config log_monitor severity error

Success.

DGS-3000-28XMP:admin#
```

84-21 config log_monitor discriminator

Description

This command is used to specify a discriminator to log system messages to Telnet or SSH.

Format

config log_monitor discriminator {<name 15>}

Parameters

<name 15> - (Optional) Enter the name of the discriminator.

Restrictions

Only Administrators and Operators can issue this command.

Example

To specify the discriminator, monitor-filter, to log system messages to Telnet or SSH:

```
DGS-3000-28XMP:admin#config log_monitor discriminator monitor-filter
Command: config log_monitor discriminator monitor-filter

Success.

DGS-3000-28XMP:admin#
```

84-22 show log_monitor

Description

This command is used to display settings of the log monitor function.

Format

show log_monitor

Parameters

None.

Restrictions

None.

Example

To display settings of the log monitor function:

```
DGS-3000-28XMP:admin#show log_monitor
Command: show log_monitor

Monitor Log Setting
-------------------------
Monitor Log State : Enabled
Monitor Log Level : error
Monitor Log Discriminator: monitor-filter

DGS-3000-28XMP:admin#
```

84-23 enable log_console

Description

This command is used to enable logging system messages to local console.

Format

enable log_console

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable logging system messages to local console:

```
DGS-3000-28XMP:admin#enable log_console
Command: enable log_console

Success.

DGS-3000-28XMP:admin#
```

84-24 disable log_console

Description

This command is used to disable logging system messages to local console.

Format

disable log_console

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To disable logging system messages to local consol:

```
DGS-3000-28XMP:admin#disable log_console
Command: disable log_console

Success.

DGS-3000-28XMP:admin#
```

84-25 config log_console severity

Description

This command is used to specify the severity level of messages logging to local console.

When a specific severity level is configured, messages at that severity level or higher will be logged to local console.

Format

config log_console severity [emergency | alert | critical | error | warning | notice | informational | debug | <level 0-7>]

Parameters

emergency - Specifies the severity level to 0.
alert - Specifies the severity level to 1.
critical - Specifies the severity level to 2.
error - Specifies the severity level to 3.
warning - Specifies the severity level to 4.
notice - Specifies the severity level to 5.
information - Specifies the severity level to 6.
debug - Specifies the severity level to 7.
<level 0-7> - Enter the severity level here. This value must be between 0 and 7.

Restrictions

Only Administrators and Operators can issue this command.

Example

To specify the severity level of messages at **emergency** (0):

```
DGS-3000-28XMP:admin#config log_console severity emergency
Command: config log_console severity emergency

Success.

DGS-3000-28XMP:admin#
```

84-26 config log_console discriminator

Description

This command is used to specify a discriminator to log system messages to local console.

Format

config log_console discriminator {<name 15>}

Parameters

<name 15> - (Optional) Enter the name of the discriminator.

Restrictions

Only Administrators and Operators can issue this command.

Example

To specify the discriminator, monitor-filter, to log system messages to local console:

```
DGS-3000-28XMP:admin#config log_console discriminator monitor-filter
Command: config log_console discriminator monitor-filter

Success.

DGS-3000-28XMP:admin#
```

84-27 show log_console

Description

This command is used to display settings of the log console function.

Format

show log_console

Parameters

None.

Restrictions

None.

Example

To display settings of the log console function:

```
DGS-3000-28XMP:admin#show log_console
Command: show log_console

Console Log Setting
------------------------
Console Log State : Enabled
Console Log Level : emergency
Console Log Discriminator: monitor-filter

DGS-3000-28XMP:admin#
```

Chapter 85 System Severity Command List

config system_severity [trap | log | all] [emergency | alert| critical | error | warning | notice | information | debug | <level 0-7>]
show system_severity

85-1 config system_severity

Description

This command is used to configure the severity level control for the system.

When the user chooses a specific level to log or trap, messages at that severity level or more will be logged or trapped to SNMP managers.

Format

config system_severity [trap | log | all] [emergency | alert| critical | error | warning | notice | information | debug | <level 0-7>]

Parameters

trap - Specifies the severity level control for traps.
log - Specifies the severity level control for the log.
all - Specifies the severity level control for traps and the log.
emergency - Specifies the severity level to 0.
alert - Specifies the severity level to 1.
critical - Specifies the severity level to 2.
error - Specifies the severity level to 3.
warning - Specifies the severity level to 4.
notice - Specifies the severity level to 5.
information - Specifies the severity level to 6.
debug - Specifies the severity level to 7.
<level 0-7> - Enter the severity level here. This value must be between 0 and 7.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure severity level control as information level for trap:

```
DGS-3000-28XMP:admin# config system_severity trap warning
Command: config system_severity trap warning

Success.

DGS-3000-28XMP:admin#
```

85-2 show system_severity

Description

This command is used to display the severity level controls for the system.

Format

show system_severity

Parameters

None.

Restrictions

None.

Example

To show severity level control for system:

```
DGS-3000-28XMP:admin# show system_severity
Command: show system_severity

System Severity Trap : warning(4)
System Severity Log : information(6)

DGS-3000-28XMP:admin#
```

Chapter 86 Telnet Client Command List

telnet [<ipaddr> | <domain_name 255> | <ipv6addr>] {tcp_port <value 1-65535>}

86-1 telnet

Description

This command is used to start the telnet client to connect to the specific telnet server. The parameters specified by the command will only be used for the establishment of this specific session. They will not affect the establishment of other sessions.

Format

telnet [<ipaddr> | <domain_name 255> | <ipv6addr>] {tcp_port <value 1-65535>}

Parameters

<ipaddr> - Enter the IP address of the telnet server.
<domain_name 255> - Enter the domain name of the telnet server.
<ipv6addr> - Enter the IPv6 address of the telnet server.
tcp_port - (Optional) Specifies the Telnet server port number to be connected. If not specified, the default port is 23. **<value 1-65535>** - Enter the TCP port number used here. This value must be between 1 and 65535.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

Telnet to a Switch by specifying the IP address:

```
DGS-3000-28XMP:admin# telnet 10.90.90.90
Command: telnet 10.90.90.90


                            DGS-3000-28XMP Gigabit Ethernet Switch
                                    Command Line Interface

                                   Firmware: Build 4.00.010
                  Copyright(C) 2018 D-Link Corporation. All rights reserved.
UserName:
```

Chapter 87 TFTP/FTP Client Command List

download [firmware_fromTFTP {[<ipaddr> | <ipv6addr> | <domain_name 255>] src_file <path_filename 64> {dest_file <pathname 64>} {boot_up}} | cfg_fromTFTP{[<ipaddr> | <ipv6addr> | <domain_name 255>] src_file <path_filename 64> {dest_file <pathname 64>}} | firmware_fromFTP [<ipaddr> {tcp_port <tcp_port_number 1-65535>} src_file <path_filename 64> | ftp:<string user:password@ipaddr:tcpport/path_filename>] {dest_file <path_filename 64> {boot_up}} | cfg_fromFTP [<ipaddr> {tcp_port < tcp_port_number 1-65535>} src_file <path_filename 64> | ftp: <string user:password@ipaddr:tcpport/path_filename>] {dest_file <path_filename 64>}]
upload [cfg_toTFTP {[<ipaddr> | <ipv6addr> | <domain_name 255>] dest_file <path_filename64> {src_file <pathname 64>} {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}} {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}} {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}}}}}} | log_toTFTP {[<ipaddr> | <ipv6addr> | <domain_name 255>] dest_file <path_filename 64>} | attack_log_toTFTP {[<ipaddr> | <ipv6addr> | <domain_name 255>] dest_file <path_filename 64>} | firmware_toTFTP {[<ipaddr> | <ipv6addr> | <domain_name 255>] dest_file <path_filename 64> {src_file <path_filename 64>}} | cfg_toFTP [<ipaddr> {tcp_port < tcp_port_number 1-65535>} dest_file <path_filename 64> | ftp: <string user:password@ipaddr:tcpport/path_filename>] {src_file <path_filename 64>} {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}} {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}} {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}}}}} | log_toFTP [<ipaddr> {tcp_port < tcp_port_number 1-65535>} dest_file <path_filename 64> | ftp: <string user:password@ipaddr:tcpport/path_filename>] | attack_log_toFTP [<ipaddr> {tcp_port <tcp_port_number 1-65535>} dest_file <path_filename 64> | ftp: <string user:password@ipaddr:tcpport/path_filename>] | firmware_toFTP [<ipaddr> {tcp_port <tcp_port_number 1-65535>} dest_file <path_filename 64> | ftp: <string user:password@ipaddr:tcpport/path_filename>] {src_file <pathname 64>}]
config tftp {server <ipaddr> | firmware_file <path_filename 64> | cfg_file <path_filename 64> | log_file <path_filename 64> | attack_log_file <path_filename 64> | certificate_file <path_filename 64> | key_file <path_filename 64> | tech_support_file <path_filename 64> | debug_error_log_file <path_filename 64> | sim_firmware_file <path_filename 64> | sim_cfg_file <path_filename 64> | sim_log_file <path_filename 64>}
show tftp

87-1 download

Description

This command is used to download the firmware image and configuration from a TFTP/FTP server.

Format

download [firmware_fromTFTP {[<ipaddr> | <ipv6addr> | <domain_name 255>] src_file <path_filename 64> {dest_file <pathname 64>} {boot_up}} | cfg_fromTFTP{[<ipaddr> | <ipv6addr> | <domain_name 255>] src_file <path_filename 64> {dest_file <pathname 64>}} | firmware_fromFTP [<ipaddr> {tcp_port <tcp_port_number 1-65535>} src_file <path_filename 64> | ftp:<string user:password@ipaddr:tcpport/path_filename>] {dest_file <path_filename 64> {boot_up}} | cfg_fromFTP [<ipaddr> {tcp_port < tcp_port_number 1-65535>} src_file <path_filename 64> | ftp: <string user:password@ipaddr:tcpport/path_filename>] {dest_file <path_filename 64>}]

Parameters

firmware_fromTFTP - Specifies to download the firmware from a TFTP server. **<ipaddr>** - (Optional) Enter the IP address of the TFTP server. **<ipv6addr>** - (Optional) Enter the IPv6 address of the TFTP server. **<domain_name 255>** - (Optional) Enter the domain name of the TFTP server.

src_file - (Optional) Specifies to enter the parameter “path_filename”.

<path_filename 64> - Enter the source file pathname here. This name can be up to 64 characters long.

dest_file - (Optional) Specifies to enter the parameter “path_filename”.

<pathname 64> - Enter the destination file pathname here.

boot_up – (Optional) Specifies to assign the downloaded file as boot-up image.

cfg_fromTFTP – Specifies to download a configuration file from a TFTP server.

<ipaddr> - (Optional) Enter the IP address of the TFTP server.

<ipv6addr> - (Optional) Enter the IPv6 address of the TFTP server.

<domain_name 255> - (Optional) Enter the domain name of the TFTP server.

src_file - (Optional) Specifies to enter the parameter “path_filename”.

<path_filename 64> - Enter the pathname specifies the pathname on the TFTP server. It can be a relative pathname or an absolute pathname. This name can be up to 64 characters long.

dest_file - (Optional) Specifies to enter the parameter “path_filename”.

<pathname 64>- Enter the pathname specifies an absolute pathname on the device file system. If pathname is not specified, it refers to the boot-up configuration file.

firmware_fromFTP - Specifies to download firmware from a FTP server.

<ipaddr> - (Optional) Enter the IP address of the FTP server.

tcp_port - Specifies the TCP port.

<tcp_port_number1-65535> - Enter a value between 1 and 65535.

src_file - Specifies the source file location.

<path_filename 64> - Enter the pathname specifies the pathname on the FTP server. It can be a relative pathname or an absolute pathname. This name can be up to 64 characters long.

ftp: - Specifies the FTP site.

<string user:password@ipaddr:tcpport/path_filename> - Enter the FTP directory.

dest_file - Specifies to enter the parameter “path_filename”.

<path_filename 64> - Enter the pathname specifies an absolute pathname on the device file system. If pathname is not specified, it refers to the boot-up image file.

boot_up - (Optional) Specifies to assign the downloaded file as boot-up image.

cfg_fromFTP - Specifies to download a configuration file from a FTP server.

<ipaddr> - Enter the IP address of the FTP server.

tcp_port - (Optional) Specifies the TCP port.

<tcp_port number 1-65535> - Enter a value between 1 and 65535.

src_file - Specifies to enter the parameter “path_filename”.

<path_filename 64> - Enter the pathname specifies the pathname on the FTP server. It can be a relative pathname or an absolute pathname. This name can be up to 64 characters long.

ftp: - Specifies the FTP site.

<string user:password@ipaddr:tcpport/path_filename> - Enter the FTP directory.

dest_file - Specifies to enter the parameter “path_filename”.

<path_filename 64> - Enter the pathname specifies an absolute pathname on the device file system. If pathname is not specified, it refers to the boot-up configuration file.

Restrictions

Only Administrators can issue this command.

Example

To download firmware from TFTP:

```
DGS-3000-28XMP:admin# download firmware_fromTFTP 10.54.71.1 src_file px.had
Command: download firmware_fromTFTP 10.54.71.1 src_file px.had

Connecting to server.................. Done.
Download firmware..................... Done.  Do not power off!
Please wait, programming flash......... Done.

DGS-3000-28XMP:admin#
```

To download configuration from TFTP:

```
DGS-3000-28XMP:admin# download cfg_fromTFTP 10.54.71.1 src_file cfg01.txt
Command: download cfg_fromTFTP 10.54.71.1 src_file cfg01.txt

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

DGS-3000-28XMP:admin#
```

87-2 upload

Description

This command is used to upload firmware and configuration from the device to a TFTP/FTP server.

Format

upload [cfg_toTFTP {[<ipaddr> | <ipv6addr> | <domain_name 255>] dest_file <path_filename64> {src_file <pathname 64>} {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}} {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}} {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}}}}} | log_toTFTP {[<ipaddr> | <ipv6addr> | <domain_name 255>] dest_file <path_filename 64>} | attack_log_toTFTP {[<ipaddr> | <ipv6addr> | <domain_name 255>] dest_file <path_filename 64>} | firmware_toTFTP {[<ipaddr> | <ipv6addr> | <domain_name 255>] dest_file <path_filename 64> {src_file <path_filename 64>}} | cfg_toFTP [<ipaddr> {tcp_port < tcp_port_number 1-65535>} dest_file <path_filename 64> | ftp: <string user:password@ipaddr:tcpport/path_filename>] {src_file <path_filename 64>} {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}} {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}} {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}}}}} | log_toFTP [<ipaddr> {tcp_port < tcp_port_number 1-65535>} dest_file <path_filename 64> | ftp: <string user:password@ipaddr:tcpport/path_filename>] | attack_log_toFTP [<ipaddr> {tcp_port <tcp_port_number 1-65535>} dest_file <path_filename 64> | ftp: <string user:password@ipaddr:tcpport/path_filename>] | firmware_toFTP [<ipaddr> {tcp_port <tcp_port_number 1-65535>} dest_file <path_filename 64> | ftp: <string user:password@ipaddr:tcpport/path_filename>] {src_file <pathname 64>}]

Parameters

cfg_toTFTP - Specifies that the configuration file will be uploaded to the TFTP server.

<ipaddr> - (Optional) Enter the IP address of the TFTP server.

<ipv6addr> - (Optional) Enter the IPv6 address of the TFTP server.

<domain_name 255> - (Optional) Enter the domain name of the TFTP server.

dest_file - (Optional) Specifies to enter the parameter “path_filename”.

<path_filename 64> - Enter the pathname specifies the pathname on the TFTP server. It can be a relative pathname or an absolute pathname. This name can be up to 64 characters long.

src_file - (Optional) Specifies to enter the parameter “path_filename”.

<pathname 64> - Enter the pathname specifies an absolute pathname on the device file system.

include - (Optional) Specifies to include lines that contain the specified filter string.

exclude - (Optional) Specifies to exclude lines that contain the specified filter string.

begin - (Optional) Specifies the first line that contains the specified filter string will be the first line of the output.

<filter_string 80> - Enter a filter string that is enclosed by the symbol ". Thus, the filter string itself cannot contain the “ character. The filter string is case sensitive. This value can be up to 80 characters long.

<filter_string 80> - (Optional) Enter a filter string that is enclosed by the symbol ". Thus, the filter string itself cannot contain the “ character. The filter string is case sensitive. This value can be up to 80 characters long.

<filter_string 80> - (Optional) Enter a filter string that is enclosed by the symbol ". Thus, the filter string itself cannot contain the “ character. The filter string is case sensitive. This value can be up to 80 characters long.

include - (Optional) Specifies to include lines that contain the specified filter string.

exclude - (Optional) Specifies to exclude lines that contain the specified filter string.

begin - (Optional) Specifies the first line that contains the specified filter string will be the first line of the output.

<filter_string 80> - Enter a filter string that is enclosed by the symbol ". Thus, the filter string itself cannot contain the “ character. The filter string is case sensitive. This value can be up to 80 characters long.

<filter_string 80> - (Optional) Enter a filter string that is enclosed by the symbol ". Thus, the filter string itself cannot contain the “ character. The filter string is case sensitive. This value can be up to 80 characters long.

<filter_string 80> - (Optional) Enter a filter string that is enclosed by the symbol ". Thus, the filter string itself cannot contain the “ character. The filter string is case sensitive. This value can be up to 80 characters long.

include - (Optional) Specifies to include lines that contain the specified filter string.

exclude - (Optional) Specifies to exclude lines that contain the specified filter string.

begin - (Optional) Specifies the first line that contains the specified filter string will be the first line of the output.

<filter_string 80> - Enter a filter string that is enclosed by the symbol ". Thus, the filter string itself cannot contain the “ character. The filter string is case sensitive. This value can be up to 80 characters long.

<filter_string 80> - (Optional) Enter a filter string that is enclosed by the symbol ". Thus, the filter string itself cannot contain the “ character. The filter string is case sensitive. This value can be up to 80 characters long.

<filter_string 80> - (Optional) Enter a filter string that is enclosed by the symbol ". Thus, the filter string itself cannot contain the “ character. The filter string is case sensitive. This value can be up to 80 characters long.

---

log_toTFTP - Specifies to upload a log file from the device to the TFTP server.

<ipaddr> - (Optional) Enter the IP address of the TFTP server.

<ipv6addr> - (Optional) Enter the IPv6 address of the TFTP server.

<domain_name 255> - (Optional) Enter the domain name of the TFTP server.

dest_file - (Optional) Specifies to enter the parameter “path_filename”.

<path_filename 64> - Enter the pathname specifies the pathname on the TFTP server. It can be a relative pathname or an absolute pathname. This name can be up to 64 characters long.

---

attack_log_toTFTP - Specifies that the attack log will be uploaded to the TFTP server.

<ipaddr> - (Optional) Enter the IP address of the TFTP server.

<ipv6addr> - (Optional) Enter the IPv6 address of the TFTP server.

<domain_name 255> - (Optional) Enter the domain name of the TFTP server.

dest_file - (Optional) Specifies to enter the parameter “path_filename”.

<path_filename 64> - Enter the pathname on the TFTP server to hold the attack log. This name can be up to 64 characters long.

---

firmware_toTFTP - Specifies that the firmware file will be uploaded to the TFTP server.

<ipaddr> - (Optional) Enter the IP address of the TFTP server.

<ipv6addr> - (Optional) Enter the IPv6 address of the TFTP server.

<domain_name 255> - (Optional) Enter the domain name of the TFTP server.

dest_file - (Optional) Specifies to enter the parameter “path_filename”.

<path_filename 64> - Enter the pathname specifies the pathname on the TFTP server. It can be a relative pathname or an absolute pathname. This name can be up to 64 characters long.

src_file - (Optional) Specifies to enter the parameter “path_filename”.

<pathname 64> - Enter the pathname specifies an absolute pathname on the device file system. If pathname is not specified, it refers to the boot-up image. This name can be up to 64 characters long.

cfg_toFTP - Specifies that the configuration file will be uploaded to the FTP server.

<ipaddr> - Enter the IP address of the FTP server.

tcp_port - Specifies the TCP port.

<tcp_port_number1-65535> - Enter a value between 1 and 65535.

dest_file - Specifies to enter the parameter “path_filename”.

<path_filename 64> - Enter the pathname specifies the pathname on the FTP server. It can be a relative pathname or an absolute pathname. This name can be up to 64 characters long.

ftp: - Specifies the FTP site.

<string user:password@ipaddr:tcpport/path_filename> - Enter the FTP directory.

src_file - (Optional) Specifies to enter the parameter “path_filename”.

<pathname 64> - Enter the pathname specifies an absolute pathname on the device file system. If pathname is not specified, it refers to the boot-up CFG file.

include - (Optional) Specifies to include lines that contain the specified filter string.

exclude - (Optional) Specifies to exclude lines that contain the specified filter string.

begin - (Optional) Specifies the first line that contains the specified filter string will be the first line of the output.

<filter_string 80> - Enter a filter string that is enclosed by the symbol ". Thus, the filter string itself cannot contain the “ character. The filter string is case sensitive. This value can be up to 80 characters long.

<filter_string 80> - (Optional) Enter a filter string that is enclosed by the symbol ". Thus, the filter string itself cannot contain the “ character. The filter string is case sensitive. This value can be up to 80 characters long.

<filter_string 80> - (Optional) Enter a filter string that is enclosed by the symbol ". Thus, the filter string itself cannot contain the “ character. The filter string is case sensitive. This value can be up to 80 characters long.

include - (Optional) Specifies to include lines that contain the specified filter string.

exclude - (Optional) Specifies to exclude lines that contain the specified filter string.

begin - (Optional) Specifies the first line that contains the specified filter string will be the first line of the output.

<filter_string 80> - Enter a filter string that is enclosed by the symbol ". Thus, the filter string itself cannot contain the “ character. The filter string is case sensitive. This value can be up to 80 characters long.

<filter_string 80> - (Optional) Enter a filter string that is enclosed by the symbol ". Thus, the filter string itself cannot contain the “ character. The filter string is case sensitive. This value can be up to 80 characters long.

<filter_string 80> - (Optional) Enter a filter string that is enclosed by the symbol ". Thus, the filter string itself cannot contain the “ character. The filter string is case sensitive. This value can be up to 80 characters long.

include - (Optional) Specifies to include lines that contain the specified filter string.

exclude - (Optional) Specifies to exclude lines that contain the specified filter string.

begin - (Optional) Specifies the first line that contains the specified filter string will be the first line of the output.

<filter_string 80> - Enter a filter string that is enclosed by the symbol ". Thus, the filter string itself cannot contain the “ character. The filter string is case sensitive. This value can be up to 80 characters long.

<filter_string 80> - (Optional) Enter a filter string that is enclosed by the symbol ". Thus, the filter string itself cannot contain the “ character. The filter string is case sensitive. This value can be up to 80 characters long.

<filter_string 80> - (Optional) Enter a filter string that is enclosed by the symbol ". Thus, the filter string itself cannot contain the “ character. The filter string is case sensitive. This value can be up to 80 characters long.

log_toFTP - Specifies to upload a log file from device to FTP server.

<ipaddr> - Enter the IP address of the FTP server.

tcp_port - Specifies the TCP port.

<tcp_port_number1-65535> - Enter a value between 1 and 65535.

dest_file - Specifies to enter the parameter “path_filename”.

<path_filename 64> - Enter the pathname specifies the pathname on the FTP server. It can be a relative pathname or an absolute pathname. This name can be up to 64 characters long.

ftp: - Specifies the FTP site.

<string user:password@ipaddr:tcpport/path_filename> - Enter the FTP directory.

attack_log_toFTP – Specifies that the attack log will be uploaded to the FTP server.

<ipaddr> - Enter the IP address of the FTP server.

tcp_port - Specifies the TCP port.

<tcp_port_number1-65535> - Enter a value between 1 and 65535.

dest_file - Specifies to enter the parameter “path_filename”.

<path_filename 64> - Enter the pathname on the FTP server to hold the attack log. This name can be up to 64 characters long.

ftp: - Specifies the FTP site.

<string user:password@ipaddr:tcpport/path_filename> - Enter the FTP directory.

firmware_toFTP – Specifies that the firmware file will be uploaded to the FTP server.

<ipaddr> - Enter the IP address of the FTP server.

tcp_port - Specifies the TCP port.

<tcp_port_number1-65535> - Enter a value between 1 and 65535.

dest_file - Specifies to enter the parameter “path_filename”.

<path_filename 64> - Enter the pathname specifies the pathname on the FTP server. It can be a relative pathname or an absolute pathname. This name can be up to 64 characters long.

ftp: - Specifies the FTP site.

<string user:password@ipaddr:tcpport/path_filename> - Enter the FTP directory.

src_file - (Optional) Specifies to enter the parameter “path_filename”.

<pathname 64> - Enter the pathname specifies an absolute pathname on the device file system. If pathname is not specified, it refers to the boot-up image. This name can be up to 64 characters long.

Restrictions

Only Administrators and Operators can issue this command.

Example

To upload firmware from a file system device to a TFTP server:

```
DGS-3000-28XMP:admin# upload firmware_toTFTP 10.90.90.10 dest_file d:\firmware.had

Command: upload firmware_toTFTP 10.90.90.10 dest_file d:\firmware.had

 Connecting to server.................. Done.
 Upload firmware....................... Done.
Success.

DGS-3000-28XMP:admin#
```

To display a scenario where the uploading of the firmware to the TFTP server failed, because of an incorrect or missing filename from the source. This error can also be found if the directory, on the source, does not exit.

```
DGS-3000-28XMP:admin# upload firmware_toTFTP 10.90.90.10 dest_file D:/firmware.had src_file
4.00.020.had
Command: upload firmware_toTFTP 10.90.90.10 dest_file D:/firmware.had src_file 4.00.020.had

 No such file or directory.

Fail!

DGS-3000-28XMP:admin#
```

To upload configuration from TFTP:

```
DGS-3000-28XMP:admin# upload cfg_toTFTP 10.90.90.10 dest_file d:\config.cfg
Command: upload cfg_toTFTP 10.90.90.10 dest_file d:\config.cfg

 Connecting to server................... Done.
 Upload configuration................... Done.
Success.

DGS-3000-28XMP:admin#
```

To display a scenario where the uploading of the config file to the TFTP server failed, because of an incorrect or missing filename from the source. This error can also be found if the directory, on the source, does not exit.

```
DGS-3000-28XMP:admin# upload cfg_toTFTP 10.90.90.10 dest_file d:\config.cfg src_file
missing.cfg
Command: upload cfg_toTFTP 10.90.90.10 dest_file d:\config.cfg src_file missing.cfg

 No such file or directory.

Fail!

DGS-3000-28XMP:admin#
```

To upload the attack log:

```
DGS-3000-28XMP:admin# upload attack_log_toTFTP 10.90.90.10 dest_file d:\attack.txt
Command: upload attack_log_toTFTP 10.90.90.10 dest_file d:\attack.txt

Success.

DGS-3000-28XMP:admin#
```

87-3 config tftp

Description

This command is used to pre-configure TFTP server and file pathname on the TFTP server.

Format

config tftp {server <ipaddr> | firmware_file <path_filename 64> | cfg_file <path_filename 64> | log_file <path_filename 64> | attack_log_file <path_filename 64> | certificate_file <path_filename 64> | key_file

<path_filename 64> | tech_support_file <path_filename 64> | debug_error_log_file <path_filename 64> | sim_firmware_file <path_filename 64> | sim_cfg_file <path_filename 64> | sim_log_file <path_filename 64>}

Parameters

server - (Optional) Specifies the IP address of the TFTP server. **<ipaddr>** - Enter the IP address of the TFTP server.
firmware_file - (Optional) Specifies the pathname supports “download/upload firmware_fromTFTP” function. **<path_filename 64>** - Enter the pathname supports “download/upload firmware_fromTFTP” function.
cfg_file - (Optional) Specifies the pathname supports “download/upload cfg_fromTFTP” function. **<path_filename 64>** - Enter the pathname supports “download/upload cfg_fromTFTP” function.
log_file - (Optional) Specifies the pathname supports “upload log_toTFTP” function. **<path_filename 64>** - Enter the pathname supports “upload log_toTFTP” function.
attack_log_file - (Optional) Specifies the pathname supports “upload attack_log_toTFTP” function. **<path_filename 64>** - Enter the pathname supports “upload attack_log_toTFTP” function.
certificate_file - (Optional) Specifies the pathname supports “download ssl certificate” function. **<path_filename 64>** - Enter the pathname supports “download ssl certificate” function.
key_file - (Optional) Specifies the pathname supports “download ssl certificate” function. **<path_filename 64>** - Enter the pathname supports “download ssl certificate” function.
tech_support_file - (Optional) Specifies specifying the pathname supports “upload tech_support_toTFTP” function. **<path_filename 64>** - Enter specifying the pathname supports “upload tech_support_toTFTP” function.
debug_error_log_file - (Optional) Specifies the pathname supports “debug error_log” function. **<path_filename 64>** - Enter the pathname supports “debug error_log” function.
sim_firmware_file - (Optional) Specifies the pathname supports “download/upload sim_ms firmware_fromTFTP” function. **<path_filename 64>** - Enter the pathname supports “download/upload sim_ms firmware_fromTFTP” function.
sim_cfg_file - (Optional) Specifies the pathname supports “download/upload sim_ms configuration_fromTFTP” function. **<path_filename 64>** - Enter the pathname supports “download/upload sim_ms configuration_fromTFTP” function.
sim_log_file - (Optional) Specifies the pathname supports “upload sim_ms log_toTFTP” function. **<path_filename 64>** - Enter the pathname supports “upload sim_ms log_toTFTP” function.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure TFTP server:

```
DGS-3000-28XMP:admin# config tftp server 10.90.90.10
Command: config tftp server 10.90.90.10

Success.

DGS-3000-28XMP:admin#
```

To configure TFTP server and specify the predefined firmware file, log file:

```
DGS-3000-28XMP:admin# config tftp server 10.90.90.1 firmware_file DES3200.had cfg_file
log_tmp
Command: config tftp server 10.90.90.1 firmware_file DES3200.had cfg_file log_tmp

Success.

DGS-3000-28XMP:admin#
```

87-4 show tftp

Description

This command is used to display the TFTP server settings.

Format

show tftp

Parameters

None.

Restrictions

None.

Example

To display the TFTP server settings:

```
DGS-3000-28XMP:admin# show tftp
Command: show tftp

 TFTP Server Settings
 IPv4 Address : 10.90.90.1

 File Type              Path_filename
 --------------------   ----------------------
 firmware_file          DES3200.had
 cfg_file               log_tmp
 log_file
 attack_log_file
 certificate_file
 key_file
 tech_support_file
 debug_error_log_file
 sim_firmware_file
 sim_cfg_file
 sim_log_file


DGS-3000-28XMP:admin#
```

Chapter 88 Time and SNTP Command List

config sntp {primary <ipaddr> | secondary <ipaddr> | poll-interval <int 30-99999>}
show sntp
enable sntp
disable sntp
config time <date ddmthyyyy> <time hh:mm:ss>
config time_zone {operator [+ | -] | hour <gmt_hour 0-13> | min <minute 0-59>}
config dst [disable | repeating {s_week <start_week 1-4,last> | s_day <start_weekday sun-sat> | s_mth <start_mth 1-12> | s_time <start_time hh:mm> | e_week <end_week 1-4,last> | e_day <end_weekday sun-sat> | e_mth <end_mth 1-12> | e_time <end_time hh:mm> | offset [30 | 60 | 90 | 120]} | annual {s_date <start_date 1-31> | s_mth <start_mth 1-12> | s_time <start_time hh:mm> | e_date <end_date 1-31> | e_mth <end_mth 1-12> | e_time <end_time hh:mm> | offset [30 | 60 | 90 | 120]}]
show time

88-1 config sntp

Description

This command is used to change SNTP configurations.

Format

config sntp {primary <ipaddr> | secondary <ipaddr> | poll-interval <int 30-99999>}

Parameters

primary - (Optional) Specifies the SNTP primary server IP address. **<ipaddr>** - Enter the IP address used for this configuration here.
secondary - (Optional) Specifies the SNTP secondary server IP address. **<ipaddr>** - Enter the IP address used for this configuration here.
poll-interval - (Optional) Specifies the polling interval range seconds. **<int 30-99999>** - Enter the polling interval range here. This value must be between 30 and 99999 seconds.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure SNTP:

```
DGS-3000-28XMP:admin# config sntp primary 10.1.1.1 secondary 10.1.1.2 poll-interval 30
Command: config sntp primary 10.1.1.1 secondary 10.1.1.2 poll-interval 30

Success.

DGS-3000-28XMP:admin#
```

88-2 show sntp

Description

This command is used to display SNTP current time source and configuration.

Format

show sntp

Parameters

None.

Restrictions

None.

Example

To show SNTP:

```
DGS-3000-28XMP:admin#show sntp
Command: show sntp

     Current Time Source   : System Clock
     SNTP                  : Disabled
     SNTP Primary Server   : 0.0.0.0
     SNTP Secondary Server : 0.0.0.0
     SNTP Poll Interval    : 720 sec

DGS-3000-28XMP:admin#
```

88-3 enable sntp

Description

This command is used to turn on SNTP support.

Format

enable sntp

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable SNTP:

```
DGS-3000-28XMP:admin# enable sntp
Command: enable sntp

Success.

DGS-3000-28XMP:admin#
```

88-4 disable sntp

Description

This command is used to turn off SNTP support.

Format

disable sntp

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To disable SNTP:

```
DGS-3000-28XMP:admin# disable sntp
Command: disable sntp

Success.

DGS-3000-28XMP:admin#
```

88-5 config time

Description

This command is used to configure time and date settings of the device.

Format

config time <date ddmthyyyy> <time hh:mm:ss>

Parameters

<date ddmthyyyy> - Specifies the system clock date. An example would look like this: '30jun2010'.
<time hh:mm:ss> - Specifies the system clock time. An example would look like this: '12:00:00'.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure time:

```
DGS-3000-28XMP:admin# config time 30jun2003 16:30:30
Command: config time 30jun2003 16:30:30

Success.

DGS-3000-28XMP:admin#
```

88-6 config time_zone

Description

This command is used to configure time zone of the device.

Format

config time_zone {operator [+ | -] | hour <gmt_hour 0-13> | min <minute 0-59>}

Parameters

operator - (Optional) Specifies the operator of time zone. **[+ | -]** - Specifies that time should be added or subtracted to or from the GMT.
hour - (Optional) Specifies the hour of time zone. **<gmt_hour 0-13>** - Enter the hour value of the time zone here. This value must be between 0 and 13.
min - (Optional) Specifies the minute of time zone. **<minute 0-59>** - Enter the minute value of the time zone here. This value must be between 0 and 59.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure time_zone:

```
DGS-3000-28XMP:admin# config time_zone operator + hour 2 min 30
Command: config time_zone operator + hour 2 min 30

Success.

DGS-3000-28XMP:admin#
```

88-7 config dst

Description

This command is used to configure Daylight Saving Time of the device.

Format

config dst [disable | repeating {s_week <start_week 1-4,last> | s_day <start_weekday sun-sat> | s_mth <start_mth 1-12> | s_time <start_time hh:mm> | e_week <end_week 1-4,last> | e_day <end_weekday sun-sat> | e_mth <end_mth 1-12> | e_time <end_time hh:mm> | offset [30 | 60 | 90 | 120]} | annual {s_date <start_date 1-31> | s_mth <start_mth 1-12> | s_time <start_time hh:mm> | e_date <end_date 1-31> | e_mth <end_mth 1-12> | e_time <end_time hh:mm> | offset [30 | 60 | 90 | 120]}]

Parameters

disable - Specifies to disable the Daylight Saving Time of the Switch.

repeating - Specifies to set the Daylight Saving Time to repeating mode.

- **s_week** - (Optional) Specifies to configure the start number of Daylight Saving Time.
  - **<start_week 1-4, last>** - Enter the starting week number of Daylight Saving Time here. This value must be between 1 and 4.
- **s_day** - (Optional) Specifies to configure the start day number of Daylight Saving Time.
  - **<start_weekday sun-sat>** - Enter the starting day value of Daylight Saving Time here. This value must either be sun, mon, tue, wed, thu, fri or sat.
- **s_mth, e_mt** - (Optional) Specifies to configure the start month number of Daylight Saving Time.
  - **<start_mth 1-12>** - Enter the starting month number of Daylight Saving Time here. This value must be between 1 and 12.
- **s_time** - (Optional) Specifies to configure the start time of Daylight Saving Time.
  - **<start_time hh:mm>** - Enter the starting time of Daylight Saving Time here. This value must be in the hh:mm format.
- **e_week** - (Optional) Specifies to configure the end week number of Daylight Saving Time.
  - **<end_week 1-4, last>** - Enter the ending week number of Daylight Saving Time here. This value must be between 1 and 4.
- **e_day** - (Optional) Specifies to configure the end day number of Daylight Saving Time.
  - **<end_weekday sun-sat>** - Enter the ending day value of Daylight Saving Time here. This value must either be sun, mon, tue, wed, thu, fri or sat.
- **e_mth** - (Optional) Specifies to configure the end month number of Daylight Saving Time.
  - **<end_mth 1-12>** - Enter the ending month number of Daylight Saving Time here. This value must be between 1 and 12.
- **e_time** - (Optional) Specifies to configure the end time of Daylight Saving Time.
  - **<end_time hh:mm>** - Enter the starting time of Daylight Saving Time here. This value must be in the hh:mm format.
- **offset** - (Optional) Specifies the number of minutes to add or to subtract during summertime. The ranges of offset are 30, 60, 90,120. The default value is 60.
  - **30** - Specifies that the offset range will 30 minutes.
  - **60** - Specifies that the offset range will 60 minutes.

90 - Specifies that the offset range will 90 minutes.

120 - Specifies that the offset range will 120 minutes.

annual - Specifies to set the Daylight Saving Time to annual mode.

s_date - (Optional) Specifies to configure the start date of Daylight Saving Time.

<start_date 1-31> - Enter the starting date of Daylight Saving Time here. This range must be between 1 and 31.

s_mth - (Optional) Specifies to configure the start month number of Daylight Saving Time.

<start_mth 1-12> - Enter the starting month number of Daylight Saving Time here. This value must be between 1 and 12.

s_time - (Optional) Specifies to configure the start time of Daylight Saving Time.

<start_time hh:mm> - Enter the starting time of Daylight Saving Time here. This value must be in the hh:mm format.

e_date - (Optional) Specifies to configure the end date of Daylight Saving Time.

<end_date 1-31> - Enter the ending date of Daylight Saving Time here. This range must be between 1 and 31.

e_mth - (Optional) Specifies to configure the end month number of Daylight Saving Time.

<end_mth 1-12> - Enter the ending month number of Daylight Saving Time here. This value must be between 1 and 12.

e_time - (Optional) Specifies to configure the end time of Daylight Saving Time.

<end_time hh:mm> - Enter the ending time of Daylight Saving Time here. This value must be in the hh:mm format.

offset - (Optional) Specifies the number of minutes to add or to subtract during summertime. The ranges of offset are 30, 60, 90,120; default value is 60.

30 - Specifies that the offset range will 30 minutes.

60 - Specifies that the offset range will 60 minutes.

90 - Specifies that the offset range will 90 minutes.

120 - Specifies that the offset range will 120 minutes.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure time:

```
DGS-3000-28XMP:admin# config dst repeating s_week 2 s_day tue s_mth 4 s_time 15:00 e_week
 2 e_day wed e_mth 10 e_time 15:30 offset 30
Command: config dst repeating s_week 2 s_day tue s_mth 4 s_time 15:00 e_week 2 e
_day wed e_mth 10 e_time 15:30 offset 30

Success.

DGS-3000-28XMP:admin#
```

88-8 show time

Description

This command is used to display time states.

Format

show time

Parameters

None.

Restrictions

None.

Example

To show time:

```
DGS-3000-28XMP:admin# show time
Command: show time

     Current Time Source  : System Clock
     Boot Time    : 9 May 2011  06:20:55
     Current Time : 9 May 2011  07:46:10
     Time Zone    : GMT +00:00
     Daylight Saving Time  : Disabled
         Offset In Minutes : 60
         Repeating    From : Apr 1st  Sun 00:00
                      To   : Oct last Sun 00:00
         Annual       From : 29 Apr 00:00
                      To   : 12 Oct 00:00

DGS-3000-28XMP:admin#
```

Chapter 89 Trace Route Command List

t**raceroute** [<ipaddr> | <domain_name 255>] {ttl <value 1-60> | port <value 30000-64900> | timeout <sec 1-65535> | probe <value 1-9>}
traceroute6 [<ipv6addr> | <domain_name 255>] {ttl <value 1-60> | port <value 30000-64900> | timeout <sec 1-65535> | probe <value 1-9>}

89-1 traceroute

Description

This command is used to trace the routed path between the Switch and a destination end station.

Format

traceroute [<ipaddr> | <domain_name 255>] {ttl <value 1-60> | port <value 30000-64900> | timeout <sec 1-65535> | probe <value 1-9>}

Parameters

<ipaddr> - Enter the IP address of the destination end station.
<domain_name 255> - Enter the domain name of the destination end station.
ttl - (Optional) Specifies the time to live value of the trace route request. This is the maximum number of routers that a trace route packet can pass. The **traceroute** command will cross while seeking the network path between two devices. The range for the TTL is 1 to 60 hops. **<value 1-60>** - Enter the time to live value here. This value must be between 1 and 60.
port - (Optional) Specifies the port number. The value range is from 30000 to 64900. **<value 30000-64900>** - Enter the port number here. This value must be between 30000 and 64900.
timeout - (Optional) Specifies the timeout period while waiting for a response from the remote device. A value of 1 to 65535 seconds can be specified. The default is 5 seconds. **<sec 1-65535>** - Enter the timeout period value here. This value must be between 1 and 65535 seconds.
probe - (Optional) Specifies the number of probing. The range is from 1 to 9. If unspecified, the default value is 1. **<value 1-9>** - Enter the probing number value here. This value must be between 1 and 9.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

Trace the routed path between the Switch and 10.48.74.121:

```
DGS-3000-28XMP:admin# traceroute 10.48.74.121 probe 3
Command: traceroute 10.48.74.121 probe 3

1   <10 ms.     10.12.73.254
2   <10 ms.     10.19.68.1
3   <10 ms.     10.48.74.121

Trace complete.
DGS-3000-28XMP:admin#
```

89-2 traceroute6

Description

This command is used to trace the IPv6 routed path between the Switch and a destination end station.

Format

traceroute6 [<ipv6addr> | <domain_name 255>] {ttl <value 1-60> | port <value 30000-64900> | timeout <sec 1-65535> | probe <value 1-9>}

Parameters

<ipv6addr> - Enter the IPv6 address of the destination end station.
<domain_name 255> - Enter the domain name of the destination end station.
ttl - (Optional) Specifies the time to live value of the trace route request. This is the maximum number of routers that a trace route packet can pass. The **traceroute6** command will cross while seeking the network path between two devices. The range for the TTL is 1 to 60 hops. **<value 1-60>** - Enter the time to live value here. This value must be between 1 and 60.
port - (Optional) Specifies the port number. The value range is from 30000 to 64900. **<value 30000-64900>** - Enter the port number here. This value must be between 30000 and 64900.
timeout - (Optional) Specifies the timeout period while waiting for a response from the remote device. A value of 1 to 65535 seconds can be specified. The default is 5 seconds. **<sec 1-65535>** - Enter the timeout period value here. This value must be between 1 and 65535 seconds.
probe - (Optional) Specifies the number of probing. The range is from 1 to 9. If unspecified, the default value is 1. **<value 1-9>** - Enter the probing number value here. This value must be between 1 and 9.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

Trace the IPv6 routed path between the Switch and 3000::1:

```
DGS-3000-28XMP:admin# traceroute6 3000::1 probe 3
Command: traceroute6 3000::1 probe 3

1   <10 ms.     1345:142::11
2   <10 ms.     2011:14::100
3   <10 ms.     3000::1

Trace complete.
DGS-3000-28XMP:admin#
```

Trace the IPv6 routed path between the Switch and 1210:100::11 with port 40000:

```
DGS-3000-28XMP:admin# traceroute6 1210:100::11 port 40000
Command: traceroute6 1210:100::11 port 40000

1   <10 ms.     3100::25
2   <10 ms.     4130::100
3   <10 ms.     1210:100::11

Trace complete.
DGS-3000-28XMP:admin#
```

Chapter 90 Traffic Control Command List

config traffic control [<portlist> | all] {broadcast [enable | disable] | multicast [enable | disable] |unicast [enable | disable] | action [drop | shutdown] | threshold <value 0-255000> | countdown [<min 0> | <min 3-30> | disable] | time_interval <sec 5-600>}
config traffic trap [none | storm_occurred | storm_cleared | both]
show traffic control {<portlist>}
config traffic control log state [enable | disable]
config traffic control auto_recover_time [<min 0> | <min 1-65535>]

90-1 config traffic control

Description

This command is used to configure broadcast/multicast/unicast packet storm control. Shutdown mode is provided to monitor the traffic rate in addition to the storm control drop mode. If traffic rate is too high, this port will be shut down.

Format

config traffic control [<portlist> | all] {broadcast [enable | disable] | multicast [enable | disable] | unicast [enable | disable] | action [drop | shutdown] | threshold <value 0-255000> | countdown [<min 0> | <min 3-30> | disable] | time_interval <sec 5-600>}

Parameters

<portlist> - Enter a range of ports to be configured.
all - Specifies that all the ports will be used for this configuration.
broadcast - (Optional) Specifies to enable or disable broadcast storm control. **enable** - Specifies that broadcast storm control will be enabled. **disable** - Specifies that broadcast storm control will be disabled.
multicast - (Optional) Specifies to enable or disable multicast storm control. **enable** - Specifies that multicast storm control will be enabled. **disable** - Specifies that multicast storm control will be disabled.
unicast - (Optional) Specifies to enable or disable unknown packet storm control (supported for drop mode only). **enable** - Specifies that unicast storm control will be enabled. **disable** - Specifies that unicast storm control will be disabled.
action - (Optional) Specifies the storm control action as shutdown or drop mode. Shutdown mode is a function of software, drop mode is implemented by the chip. If shutdown mode is specified, it is necessary to configure values for the **countdown** and **time_interval** parameters. **drop** - Specifies that the action applied will be drop mode. **shutdown** - Specifies that the action applied will be shutdown mode.
threshold - (Optional) Specifies the upper threshold, at which point the specified storm control is triggered. **<value 0-255000>** - Enter the upper threshold value here. This is the number of broadcast/multicast packets per second received by the Switch that will trigger the storm traffic control measure. The threshold is expressed as packets per second (PPS) and must be an unsigned integer. This value must be between 0 and 255000.
countdown - (Optional) Specifies timer for shutdown mode. If a port enters the shutdown Rx state and this timer

runs out, port will be shutdown forever. This parameter is not applicable if the **drop** parameter is specified as the **action**.

<min 0> - Enter 0 to disable the forever state, which means that the port will not enter the shutdown forever state.

<min 3-30> - Enter the countdown timer value here. This value must be between 3 and 30.

disable - Specifies that the countdown timer will be disabled.

time_interval - (Optional) Specifies the sampling interval of received packet counts. This parameter is not applicable if the **drop** parameter is specified as the **action**.

<sec 5-600> - Enter the time interval value here. This value must be between 5 and 600.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the parameters so that the traffic control status is enabled on ports 1-12:

```
DGS-3000-28XMP:admin# config traffic control 1-12 broadcast enable action shutdown
threshold 1 countdown 5 time_interval 10
Command: config traffic control 1-12 broadcast enable action shutdown threshold
1 countdown 5 time_interval 10

Success.

DGS-3000-28XMP:admin#
```

90-2 config traffic trap

Description

This command is used to configure trap modes.

Occurred Mode: This trap is sent when a packet storm is detected by the packet storm mechanism.

Cleared Mode: This trap is sent when the packet storm is cleared by the packet storm mechanism.

Format

config traffic trap [none | storm_occurred | storm_cleared | both]

Parameters

none - Specifies that no trap state is specified for storm control.

storm_occurred - Specifies that storm occurred mode is enabled and storm cleared mode is disabled.

storm_cleared - Specifies that storm occurred mode is disabled and storm cleared mode is enabled.

both - Specifies that both storm occurred and storm cleared modes are enabled.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable both the occurred mode and cleared mode traffic control traps:

```
DGS-3000-28XMP:admin# config traffic trap both
Command: config traffic trap both

Success.

DGS-3000-28XMP:admin#
```

90-3 show traffic control

Description

This command is used to display the current traffic control settings.

Format

show traffic control {<portlist>}

Parameters

<portlist> - (Optional) Specifies the range of ports to be shown.
If no parameter is specified, the system will display the packet storm control configuration for all ports.

Restrictions

None.

Example

To display the traffic control parameters for ports 1 to 10:

```
DGS-3000-28XMP:admin# show traffic control 1-10
Command: show traffic control 1-10


Traffic Control Trap             : [Both]
Traffic Control Log              : Enabled
Traffic Control Auto Recover Time: 0 Minutes

Port Thres  Broadcast Multicast Unicast  Action   Count    Time     Shutdown
     hold   Storm     Storm     Storm              down     Interval Forever
---- ------ --------- --------- -------- -------- -------- -------- --------
1    1      Enabled   Disabled  Disabled shutdown 5        10
2    1      Enabled   Disabled  Disabled shutdown 5        10
3    1      Enabled   Disabled  Disabled shutdown 5        10
4    1      Enabled   Disabled  Disabled shutdown 5        10
5    1      Enabled   Disabled  Disabled shutdown 5        10
6    1      Enabled   Disabled  Disabled shutdown 5        10
7    1      Enabled   Disabled  Disabled shutdown 5        10
8    1      Enabled   Disabled  Disabled shutdown 5        10
9    1      Enabled   Disabled  Disabled shutdown 5        10
10   1      Enabled   Disabled  Disabled shutdown 5        10

DGS-3000-28XMP:admin#
```

90-4 config traffic control log state

Description

This command is used to configure the traffic control log state. When the log state is enabled, traffic control states are logged when a storm occurs and when a storm is cleared. If the log state is disabled, traffic control events are not logged.

NOTE: The log state is only applicable for shutdown mode. Since shutdown mode only support broadcast and multicast storm control, doesn't support unicast storm control. The log only generate for broadcast and multicast storm control.

Format

config traffic control log state [enable | disable]

Parameters

enable - Specifies that both storm occurred and storm cleared events are logged.
disable - Specifies that neither storm occurred nor storm cleared events are logged.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the traffic log state on the Switch:

```
DGS-3000-28XMP:admin# config traffic control log state enable
Command: config traffic control log state enable

Success.

DGS-3000-28XMP:admin#
```

90-5 config traffic control auto_recover_time

Description

This command is used to configure the traffic auto recover time that is allowed for a port to recover from shutdown forever status.

Format

config traffic control auto_recover_time [<min 0> | <min 1-65535>]

Parameters

auto_recover_time - Specifies the time allowed for auto-recovery after shutting down a port. The default value is 0, so no auto recovery is possible; the port remains in shutdown mode forever. This requires manual entry of the **config ports [<portlist> | all] state enable** command to return the port to a forwarding state.

<min 0> - Enter 0 to disable the auto recovery time.

<min 1-65535> - Enter the auto recovery time value here. This value must be between 1 and 65535.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the auto recover time to 5 minutes:

```
DGS-3000-28XMP:admin# config traffic control auto_recover_time 5
Command: config traffic control auto_recover_time 5

Success.

DGS-3000-28XMP:admin#
```

Chapter 91 Traffic Segmentation Command List

config traffic_segmentation [<portlist> | all] forward_list [null | all | <portlist>]
show traffic_segmentation {<portlist>}

91-1 config traffic_segmentation

Description

This command is used to configure the traffic segmentation.

Format

config traffic_segmentation [<portlist> | all] forward_list [null | all | <portlist>]

Parameters

<portlist> - Enter a range of ports to be configured.
all - Specifies that all the ports will be used for this configuration.
forward_list - Specifies a range of port forwarding domain. **null** - Specifies a range of port forwarding domain is null. **all** – Specifies all ports to be configured. **<portlist>** - Enter a range of ports to be configured.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure traffic segmentation:

```
DGS-3000-28XMP:admin# config traffic_segmentation 1-10 forward_list 11-15
Command: config traffic_segmentation 1-10 forward_list 11-15

Success.

DGS-3000-28XMP:admin#
```

91-2 show traffic_segmentation

Description

This command is used to display current traffic segmentation table.

Format

show traffic_segmentation {<portlist>}

Parameters

<portlist> - (Optional) Enter a range of ports to be displayed.
If no parameter is specified, the system will display all current traffic segmentation tables.

Restrictions

None.

Example

To display traffic segmentation table:

```
DGS-3000-28XMP:admin# show traffic_segmentation 1-10
Command: show traffic_segmentation 1-10

Traffic Segmentation Table

Port  Forward Portlist
----  ------------------------------------------------------------------------
1      11-15
2      11-15
3      11-15
4      11-15
5      11-15
6      11-15
7      11-15
8      11-15
9      11-15
10     11-15


DGS-3000-28XMP:admin#
```

Chapter 92 Trusted Host Command List

create trusted_host [<ipaddr> | <ipv6addr> | network <network_address> | ipv6_prefix <ipv6networkaddr>] {snmp | telnet | ssh | http | https | ping}
delete trusted_host [ipaddr <ipaddr> | ipv6address <ipv6addr> | network <network_address> | ipv6_prefix <ipv6networkaddr> | all]
config trusted_host [<ipaddr> | <ipv6addr> | network <network_address> | ipv6_prefix <ipv6networkaddr>] [add | delete] {snmp | telnet | ssh | http | https | ping | all}
show trusted_host

92-1 create trusted_host

Description

This command is used to create the trusted host. The switch allows you to specify up to ten IP addresses that are allowed to manage the Switch via in-band SNMP or Telnet based management software. These IP addresses must be members of the Management VLAN. If no IP addresses are specified, then there is nothing to prevent any IP address from accessing the Switch, provided the user knows the Username and Password.

When the access interface is not specified, the trusted host will be created for all interfaces.

Format

create trusted_host [<ipaddr> | <ipv6addr> | network <network_address> | ipv6_prefix <ipv6networkaddr>] {snmp | telnet | ssh | http | https | ping}

Parameters

<ipaddr> - Enter the IP address of the trusted host.
<ipv6addr> - Enter the IPv6 address of the trusted host.
network - Specifies the network address of the trusted network. The form of network address is xxx.xxx.xxx.xxx/y. **<network_address>** - Enter the network address used here.
ipv6_prefix - Specifies the IPv6 prefix here. **<ipv6networkaddr>** - Enter the IPv6 network address here.
snmp - (Optional) Specifies trusted host for SNMP.
telnet - (Optional) Specifies trusted host for Telnet.
ssh - (Optional) Specifies trusted host for SSH.
http - (Optional) Specifies trusted host for HTTP.
https - (Optional) Specifies trusted host for HTTPs.
ping - (Optional) Specifies trusted host for ping.

Restrictions

Only Administrators and Operators can issue this command.

Example

To create the trusted host:

```
DGS-3000-28XMP:admin# create trusted_host 10.48.74.121
Command: create trusted_host 10.48.74.121

Success.

DGS-3000-28XMP:admin#
```

92-2 delete trusted_host

Description

This command is used to delete a trusted host entry made using the **create trusted_host** command above.

Format

delete trusted_host [ipaddr <ipaddr> | ipv6address <ipv6addr> | network <network_address> | ipv6_prefix <ipv6networkaddr> | all]

Parameters

ipaddr - Specifies the IP address of the trusted host. **<ipaddr>** - Enter the IP address used for this configuration here.
ipv6addr - Specifies the IPv6 address of the trusted host. **<ipv6addr>** - Enter the IPv6 address used for this configuration here.
network - Specifies the network address of the trusted network. **<network_address>** - Enter the network address used for this configuration here.
ipv6_prefix - Specifies the IPv6 subnet prefix of the trusted network. **<ipv6networkaddr>** - Enter the IPv6 subnet prefix here.
all - Specifies that all trusted hosts will be deleted.

Restrictions

Only Administrators and Operators can issue this command.

Example

To delete the trusted host:

```
DGS-3000-28XMP:admin# delete trusted_host ipaddr 10.48.74.121
Command: delete trusted_host ipaddr 10.48.74.121

Success.

DGS-3000-28XMP:admin#
```

92-3 config trusted_host

Description

This command is used to configure the access interfaces for the trusted host.

Format

config trusted_host [<ipaddr> | <ipv6addr> | network <network_address> | ipv6_prefix <ipv6networkaddr>] [add | delete] {snmp | telnet | ssh | http | https | ping | all}

Parameters

<ipaddr> - Enter the IP address of the trusted host.
<ipv6addr> - Enter the IPv6 address of the trusted host.
network - Specifies the network address of the trusted network. The form of network address is xxx.xxx.xxx.xxx/y. **<network_address>** - Enter the network address used here.
ipv6_prefix - Specifies the IPv6 prefix here. **<ipv6networkaddr>** - Enter the IPv6 network address here.
add - Specifies to add interfaces for that trusted host.
delete - Specifies to delete interfaces for that trusted host.
snmp - (Optional) Specifies trusted host for SNMP.
telnet - (Optional) Specifies trusted host for Telnet.
ssh - (Optional) Specifies trusted host for SSH.
http - (Optional) Specifies trusted host for HTTP.
https - (Optional) Specifies trusted host for HTTPs.
ping - (Optional) Specifies trusted host for ping.
all - (Optional) Specifies trusted host for all applications.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the trusted host:

```
DGS-3000-28XMP:admin# config trusted_host 10.48.74.121 add ssh telnet
Command: config trusted_host 10.48.74.121 add ssh telnet

Success.

DGS-3000-28XMP:admin#
```

92-4 show trusted_host

Description

This command is used to display a list of trusted hosts entered on the Switch using the **create trusted_host** command above.

Format

show trusted_host

Parameters

None.

Restrictions

None.

Example

To display trusted host:

```
DGS-3000-28XMP:admin#show trusted_host
Command: show trusted_host


Management Stations

IP Address                                  Access Interface
-----------------------------------------------------------------
10.48.74.121/32                             SNMP Telnet SSH HTTP HTTPs Ping

Total Entries: 1


DGS-3000-28XMP:admin#
```

Chapter 93 UDP Helper Command List

enable udp_helper
disable udp_helper
config udp_helper udp_port add [time | tacacs | dns | tftp | netbios-ns | netbios-ds | <port_number 1-65535>]
config udp_helper udp_port delete [time | tacacs | dns | tftp | netbios-ns | netbios-ds | <port_number 1-65535>]
config udp_helper server add ipif <ipif_name 12> <ipaddr>
config udp_helper server delete ipif <ipif_name 12> <ipaddr>
show udp_helper {[udp_port | ipif <ipif_name 12>]}

93-1 enable udp_helper

Description

This command is used to enable the UDP Helper function on the Switch.

Format

enable udp_helper

Parameters

None.

Restrictions

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

Example

To enable the UDP Helper function:

```
DGS-3000-28XMP:admin#enable udp_helper
Command: enable udp_helper

Success.

DGS-3000-28XMP:admin#
```

93-2 disable udp_helper

Description

This command is used to disable the UDP Helper function on the Switch.

Format

disable udp_helper

Parameters

None.

Restrictions

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

Example

To disable the UDP Helper function:

```
DGS-3000-28XMP:admin#disable udp_helper
Command: disable udp_helper

Success.

DGS-3000-28XMP:admin#
```

93-3 config udp_helper udp_port add

Description

This command is used to add a UDP port for the UDP Helper function on the Switch.

Format

config udp_helper udp_port add [time | tacacs | dns | tftp | netbios-ns | netbios-ds | <port_number 1-65535>]

Parameters

time - Specifies the Time service. The UDP port number is 37.
tacacs - Specifies the Terminal Access Controller Access Control System service. The UDP port number is 49.
dns - Specifies the Domain Naming System service. The UDP port number is 53.
tftp - Specifies the Trivial File Transfer Protocol service. The UDP port number is 69.
netbios-ns - Specifies the NetBIOS Name Server service. The UDP port number is 137.
netbios-ds - Specifies the NetBIOS Datagram Server service. The UDP port number is 138.
<port_number 1-65535> - Enter any UDP ports used for services not listed. This value must be between 1 and 65535.

Restrictions

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

Example

To add a UDP port:

```
DGS-3000-28XMP:admin#config udp_helper udp_port add 55
Command: config udp_helper udp_port add 55

Success.

DGS-3000-28XMP:admin#
```

93-4 config udp_helper udp_port delete

Description

This command is used to delete a UDP port for the UDP Helper function on the Switch.

Format

config udp_helper udp_port delete [time | tacacs | dns | tftp | netbios-ns | netbios-ds | <port_number 1-65535>]

Parameters

time - Specifies the Time service. The UDP port number is 37.
tacacs - Specifies the Terminal Access Controller Access Control System service. The UDP port number is 49.
dns - Specifies the Domain Naming System service. The UDP port number is 53.
tftp - Specifies the Trivial File Transfer Protocol service. The UDP port number is 69.
netbios-ns - Specifies the NetBIOS Name Server service. The UDP port number is 137.
netbios-ds - Specifies the NetBIOS Datagram Server service. The UDP port number is 138.
<port_number 1-65535> - Enter any UDP ports used for services not listed. This value must be between 1 and 65535.

Restrictions

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

Example

To delete a UDP port:

```
DGS-3000-28XMP:admin#config udp_helper udp_port delete 55
Command: config udp_helper udp_port delete 55

Success.

DGS-3000-28XMP:admin#
```

93-5 config udp_helper server add ipif

Description

This command is used to add a UDP Helper server address for specific interface of Switch.

Format

config udp_helper server add ipif <ipif_name 12> <ipaddr>

Parameters

<ipif_name 12> - Enter the name of the IP interface that receives the UDP broadcast. This name can be up to 12 characters long.
<ipaddr> - Enter the UDP Helper server IP address here.

Restrictions

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

Example

To add a server address for System interface:

```
DGS-3000-28XMP:admin#config udp_helper server add ipif System 20.0.0.90
Command: config udp_helper server add ipif System 20.0.0.90

Success.

DGS-3000-28XMP:admin#
```

93-6 config udp_helper server delete ipif

Description

This command is used to delete a UDP Helper server address for specific interface of Switch.

Format

config udp_helper server delete ipif <ipif_name 12> <ipaddr>

Parameters

<ipif_name 12> - Enter the name of the IP interface that receives the UDP broadcast. This name can be up to 12 characters long.
<ipaddr> - Enter the UDP Helper server IP address here.

Restrictions

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

Example

To delete a server address for System interface:

```
DGS-3000-28XMP:admin#config udp_helper server delete ipif System 20.0.0.90
Command: config udp_helper server delete ipif System 20.0.0.90

Success.

DGS-3000-28XMP:admin#
```

93-7 show udp_helper

Description

This command is used to display the current UDP Helper configuration on the Switch.

Format

show udp_helper {[udp_port | ipif <ipif_name 12>]}

Parameters

udp_port - (Optional) Specifies the UDP port configured for the UDP Helper.
ipif - (Optional) Specifies the name of the IP interface name to be displayed. **<ipif_name 12>** - Enter the IP interface name used here. This name can be up to 12 characters long.

Restrictions

None.

Example

To display the current UDP Helper configuration:

```
DGS-3000-28XMP:admin#show udp_helper
Command: show udp_helper

UDP Helper Status  : Disabled

Application          UDP Port
-------------        ---------------
User App1            55

Interface            Server
-------------        ---------------
System               20.0.0.90


DGS-3000-28XMP:admin#
```

To display the current UDP Helper all configured ports:

```
DGS-3000-28XMP:admin#show udp_helper udp_port
Command: show udp_helper udp_port

UDP Helper Status  : Disabled

Application          UDP Port
-------------        ---------------
User App1            55



DGS-3000-28XMP:admin#
```

To display the current UDP Helper for System interface:

```
DGS-3000-28XMP:admin#show udp_helper ipif System
Command: show udp_helper ipif System

UDP Helper Status  : Disabled

Interface            Server
-------------        ---------------
System               20.0.0.90


DGS-3000-28XMP:admin#
```

Chapter 94 VLAN Trunking Command List

enable vlan_trunk
disable vlan_trunk
config vlan_trunk ports [<portlist> | all] | state [enable | disable]
show vlan_trunk

94-1 enable vlan_trunk

Description

This command is used to enable the VLAN trunk function. When the VLAN trunk function is enabled, the VLAN trunk ports shall be able to forward all tagged frames with any VID.

Format

enable vlan_trunk

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To enable the VLAN Trunk:

```
DGS-3000-28XMP:admin# enable vlan_trunk
Command: enable vlan_trunk

Success.

DGS-3000-28XMP:admin#
```

94-2 disable vlan_trunk

Description

This command is used to disable the VLAN trunk function.

Format

disable vlan_trunk

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To disable the VLAN Trunk:

```
DGS-3000-28XMP:admin# disable vlan_trunk
Command: disable vlan_trunk

Success.

DGS-3000-28XMP:admin#
```

94-3 config vlan_trunk

Description

This command is used to configure a port as a VLAN trunk port. By default, none of the port is a VLAN trunk port.

If the user enables the global VLAN trunk function and configures the VLAN trunk ports, then the trunk port will be a member port of all VLANs. That is, if a VLAN is already configured by the user, and the trunk port is not a member port of that VLAN, the trunk port will automatically become a tagged member port of that VLAN. If the VLAN is not created, the VLAN will be automatically created, and the trunk port will become tagged member of this VLAN.

When the user disables the VLAN trunk globally, all VLANs automatically created by VLAN Trunk enabled shall be destroyed, and all the automatically added port membership will be removed.

A VLAN trunk port and a non-VLAN trunk port cannot be grouped as an aggregated link. To change the VLAN trunk setting for an aggregated link, the user must apply the command to the master port. However, this setting will disappear as the aggregated link is destroyed, and the VLAN trunk setting of the individual port will follow the original setting of the port.

If the command is applied to link aggregation member port excluding the master, the command will be rejected.

The ports with different VLAN configurations are not allowed to form an aggregated link. However, if they are specified as VLAN trunk port, they are allowed to form an aggregated link.

For a VLAN trunk port, the VLANs on which the packets can be by passed will not be advertised by GVRP on this port. However, since the traffic on these VLANs is forwarded, this VLAN trunk port should participate in the MSTP instances corresponding to these VLANs.

Format

config vlan_trunk ports [<portlist> | all] | state [enable | disable]

Parameters

<portlist> - Enter a list of ports used for the configuration here.
all - Specifies that all the ports will be used for this configuration.
state - Specifies that the port is a VLAN trunk port or not. **enable** - Specifies that the port is a VLAN trunk port. **disable** - Specifies that the port is not a VLAN trunk port.

Restrictions

Only Administrators can issue this command.

Example

To configure VLAN trunk ports:

```
DGS-3000-28XMP:admin# config vlan_trunk ports 1-5 state enable
Command: config vlan_trunk ports 1-5 state enable

Success.

DGS-3000-28XMP:admin#
```

Port 6 is LA-1 member port; port 7 is LA-2 master port:

```
DGS-3000-28XMP:admin# config vlan_trunk ports 6-7 state enable
Command: config vlan_trunk ports 6-7 state enable

Success.

DGS-3000-28XMP:admin# config vlan_trunk ports 7 state disable
Command: config vlan_trunk ports 7 state disable

Success.

DGS-3000-28XMP:admin# config vlan_trunk ports 6-7 state disable
Command: config vlan_trunk ports 6-7 state disable

Success.

DGS-3000-28XMP:admin#
```

Port 6 is LA-1 member port; port 7 is LA-1 master port:

```
DGS-3000-28XMP:admin# config vlan_trunk ports 6-7 state enable
Command: config vlan_trunk ports 6-7 state enable

Success.

DGS-3000-28XMP:admin#
```

Port 6, 7 have different VLAN configurations before enabling VLAN trunk.

Port 6 is LA-1 member port; port 7 is LA-1 master port.

```
DGS-3000-28XMP:admin# config vlan_trunk ports 7 state disable
Command: config vlan_trunk ports 7 state disable

Success.

DGS-3000-28XMP:admin#
```

Port 6, 7 have the same VLAN configuration before enabling VLAN trunk.

Port 6 is LA-1 member port; port 7 is LA-1 master port.

```
DGS-3000-28XMP:admin# config vlan_trunk ports 7 state disable
Command: config vlan_trunk ports 7 state disable

Success.

DGS-3000-28XMP:admin# config vlan_trunk ports 6-7 state disable
Command: config vlan_trunk ports 6-7 state disable

Success.

DGS-3000-28XMP:admin#
```

94-4 show vlan_trunk

Description

This command is used to show the VLAN trunk configuration.

Format

show vlan_trunk

Parameters

None.

Restrictions

None.

Example

To show the VLAN Trunk information:

```
DGS-3000-28XMP:admin# show vlan_trunk
Command: show vlan_trunk


VLAN Trunk Global Setting
----------------------------
VLAN Trunk Status  : Disabled
VLAN Trunk Member Ports : 1-5


DGS-3000-28XMP:admin#
```

The following example displays the VLAN information which will also display the VLAN trunk setting:

```
DGS-3000-28XMP:admin# show vlan
Command: show vlan


VLAN Trunk State        : Enabled
VLAN Trunk Member Ports : 1-5


VID             : 1               VLAN Name     : default
VLAN Type       : Static          Advertisement : Enabled
Member Ports    : 1-28
Static Ports    : 1-28
Current Tagged Ports  :
Current Untagged Ports: 1-28
Static Tagged Ports   :
Static Untagged Ports : 1-28
Forbidden Ports       :

Total Static VLAN Entries: 1
Total GVRP VLAN Entries: 0


DGS-3000-28XMP:admin#
```

Chapter 95 Voice VLAN Command List

enable voice_vlan [<vlan_name 32> | vlanid <vlanid 1-4094>]
disable voice_vlan
config voice_vlan priority <int 0-7>
config voice_vlan oui [add | delete] <macaddr> <macmask> {description <desc 32>}
config voice_vlan ports [<portlist> | all] [state [enable | disable] | mode [auto {[tag | untag]} | manual]]
config voice_vlan aging_time <min 1-65535>
config voice_vlan log state [enable | disable]
show voice_vlan
show voice_vlan oui
show voice_vlan ports {<portlist>}
show voice_vlan voice_device {ports <portlist>}
show voice_vlan lldp_med voice_device

95-1 enable voice_vlan

Description

This command is used to enable the global voice VLAN function on a switch. To enable the voice VLAN, the voice VLAN must be also assigned .At the same time, the VLAN must be an existing static 802.1Q VLAN. To change the voice VLAN, the user must disable the voice VLAN function, and re-issue this command. By default, the global voice VLAN state is disabled.

Format

enable voice_vlan [<vlan_name 32> | vlanid <vlanid 1-4094>]

Parameters

<vlan_name 32> - Enter the name of the voice VLAN here. This name can be up to 32 characters long.
vlanid - Specifies the VLAN ID of the voice VLAN. **<vlanid 1-4094>** - Enter the voice VLAN ID here. This value must be between 1 and 4094.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable a voice VLAN with name “v2”:

```
DGS-3000-28XMP:admin#enable voice_vlan v2
Command: enable voice_vlan v2

Success.

DGS-3000-28XMP:admin#
```

95-2 disable voice_vlan

Description

This command is used to disable the voice VLAN function on a switch. When the voice VLAN function is disabled, the voice VLAN will become unassigned.

Format

disable voice_vlan

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To disable the voice VLAN:

```
DGS-3000-28XMP:admin#disable voice_vlan
Command: disable voice_vlan

Success.

DGS-3000-28XMP:admin#
```

95-3 config voice_vlan priority

Description

This command is used to configure the voice VLAN priority. The voice VLAN priority will be the priority associated with the voice VLAN traffic to distinguish the QoS of the voice traffic from data traffic.

Format

config voice_vlan priority <int 0-7>

Parameters

<int 0-7> - Enter the priotity of the voice VLAN. This value must be between 0 and 7. The default priority is 5.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To set the priority of the voice VLAN to be 6:

```
DGS-3000-28XMP:admin#config voice_vlan priority 6
Command: config voice_vlan priority 6

Success.

DGS-3000-28XMP:admin#
```

95-4 config voice_vlan oui

Description

This command is used to configure the user-defined voice traffic's OUI. The OUI is used to identify the voice traffic. There are a number of pre-defined OUIs. The user can further define the user-defined OUIs if needed.The user-defined OUI cannot be the same as the pre-defined OUI.

The following are the pre-defined voice traffic's OUI:

OUI	Vendor	Mnemonic Name
00:E0:BB	3COM.	3com
00:03:6B	Cisco	cisco
00:E0:75	Veritel	veritel
00:D0:1E	Pingtel	pingtel
00:01:E3	Siemens	siemens
00:60:B9	NEC/ Philips	nec&philips
00:0F:E2	Huawei-3COM	huawei&3com
00:09:6E	Avaya	avaya

Format

config voice_vlan oui [add | delete] <macaddr> <macmask> {description <desc 32>}

Parameters

add - Adds a user-defined OUI of a voice device vendor.

delete - Delets a user-defined OUI of a voice device vendor.

<macaddr> - Enter the user-defined OUI MAC address.

<macmask> - Enter the user-defined OUI MAC address mask.

description - (Optional) The description for the user-defined OUI.
<desc 32> - Enter the description here. This value can be up to 32 characters long.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To add a user-defined OUI for a voice device:

```
DGS-3000-28XMP:admin#config voice_vlan oui add 00-0A-0B-00-00-00 FF-FF-FF-00-00-00
Command: config voice_vlan oui add 00-0A-0B-00-00-00 FF-FF-FF-00-00-00

Success.

DGS-3000-28XMP:admin#
```

95-5 config voice_vlan ports

Description

This command is used to enable or disable the voice VLAN function on ports.

Format

config voice_vlan ports [<portlist> | all] [state [enable | disable] | mode [auto {[tag | untag]} | manual]]

Parameters

<portlist> - Enter a list of ports to be configured.

all - Specifies to configure all ports.

state - The voice VLAN function state on ports. The default state is disabled.
- **enable** - Specifies that the voice VLAN function for this switch will be enabled.
- **disable** - Specifies that the voice VLAN function for this switch will be disabled.

mode - The voice VLAN mode. The default mode is auto.
- **auto** - Specifies that the voice VLAN mode will be set to auto.
  - **tag** - (Optional) When the port is working in auto-tagged mode, and learns about a voice device through the device's OUI, it will join the voice VLAN as a tagged member automatically. When the voice device sends voice VLAN tagged packets, the Switch will change its priority. When the voice device sends untagged packets, it will forward them to port's PVID VLAN.
  - **untag** - (Optional) When the port is working in auto-untagged mode, and the port captures a voice device through the device's OUI, it will join the voice VLAN as an untagged member automatically. When the voice device sends voice VLAN tagged packets, the Switch will forward them according to the tag. When the voice device sends voice VLAN untagged packets, it will assign priority and voice VLAN ID into this packet. When the Switch receives LLDP-MED packets, it checks the VLAN ID, tagged flag and priority flag.The switch should follow the tagged flag and priority setting. By default, the mode is auto untagged.
- **manual** - Specifies that the voice VLAN mode will be set to manual.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure voice VLAN ports 4-6 to enable:

```
DGS-3000-28XMP:admin#config voice_vlan ports 4-6 state enable
Command: config voice_vlan ports 4-6 state enable

Success.

DGS-3000-28XMP:admin#
```

To set the mode auto to voice VLAN ports 3-5:

```
DGS-3000-28XMP:admin#config voice_vlan ports 3-5 mode auto
Command: config voice_vlan ports 3-5 mode auto

Success.

DGS-3000-28XMP:admin#
```

95-6 config voice_vlan aging_time

Description

This command is used to set the aging time of the voice VLAN. The aging time is used to remove a port from voice VLAN if the port is an automatic VLAN member. When the last voice device stops sending traffic and the MAC address of this voice device is aged out, the voice VLAN aging timer will be started. The port will be removed from the voice VLAN after expiration of the voice VLAN aging timer.

If the voice traffic resumes during the aging time, the aging timer will be stopped and reset.

Format

config voice_vlan aging_time <min 1-65535>

Parameters

<min 1-65535> - Enter the aging time between 1 and 65535.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To set 60 minutes as the aging time of voice VLAN:

```
DGS-3000-28XMP:admin#config voice_vlan aging_time 60
Command: config voice_vlan aging_time 60

Success.

DGS-3000-28XMP:admin#
```

95-7 config voice_vlan log state

Description

This command is used to configure the log state for voice VLAN. If there is a new voice device detected/or a port joins/leaves the voice VLAN dynamically, and the log is enabled, a log will be triggered.

Format

config voice_vlan log state [enable | disable]

Parameters

enable - Specifies that the sending of a voice VLAN log will be enabled.
disable - Specifies that the sending of a voice VLAN log will be disabled.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable the log state for voice VLAN:

```
DGS-3000-28XMP:admin#config voice_vlan log state enable
Command: config voice_vlan log state enable

Success.

DGS-3000-28XMP:admin#
```

95-8 show voice_vlan

Description

This command is used to show the voice VLAN global information.

Format

show voice_vlan

Parameters

None.

Restrictions

None.

Example

To display the voice VLAN global information when voice VLAN is enabled:

```
DGS-3000-28XMP:admin#show voice_vlan
Command: show voice_vlan

Voice VLAN State     : Enabled
VLAN ID              : 2
VLAN Name            : v2
Priority             : 6
Aging Time           : 60 minutes
Log State            : Enabled
Member Ports         :
Dynamic Member Ports :

DGS-3000-28XMP:admin#
```

To display the voice VLAN global information when voice VLAN is disabled:

```
DGS-3000-28XMP:admin#show voice_vlan
Command: show voice_vlan

Voice VLAN State     : Disabled
Voice VLAN           : Unassigned
Priority             : 6
Aging Time           : 60 minutes
Log State            : Enabled

DGS-3000-28XMP:admin#
```

95-9 show voice_vlan oui

Description

This command is used to display OUI information of voice VLAN.

Format

show voice_vlan oui

Parameters

None.

Restrictions

None.

Example

To display the OUI information of voice VLAN:

```
DGS-3000-28XMP:admin#show voice_vlan oui
Command: show voice_vlan oui

OUI Address         Mask                Description
------------------  ------------------  --------------
00-01-E3-00-00-00   FF-FF-FF-00-00-00   Siemens
00-03-6B-00-00-00   FF-FF-FF-00-00-00   Cisco
00-09-6E-00-00-00   FF-FF-FF-00-00-00   Avaya
00-0A-0B-00-00-00   FF-FF-FF-00-00-00
00-0F-E2-00-00-00   FF-FF-FF-00-00-00   Huawei&3COM
00-60-B9-00-00-00   FF-FF-FF-00-00-00   NEC&Philips
00-D0-1E-00-00-00   FF-FF-FF-00-00-00   Pingtel
00-E0-75-00-00-00   FF-FF-FF-00-00-00   Veritel
00-E0-BB-00-00-00   FF-FF-FF-00-00-00   3COM

Total Entries: 9

DGS-3000-28XMP:admin#
```

95-10 show voice_vlan ports

Description

This command is used to display the port voice VLAN information.

Format

show voice_vlan ports {<portlist>}

Parameters

<portlist> - (Optional) Enter a list of ports to be displayed.

Restrictions

None.

Example

To display the voice VLAN information of ports 1-5:

```
DGS-3000-28XMP:admin#show voice_vlan ports 1-5
Command: show voice_vlan ports 1-5

Ports  Status     Mode
-----  ---------  --------------
1      Disabled   Auto Untagged
2      Disabled   Auto Untagged
3      Disabled   Auto Untagged
4      Enabled    Auto Untagged
5      Enabled    Auto Untagged

DGS-3000-28XMP:admin#
```

95-11 show voice_vlan voice_device

Description

This command is used to show voice devices that are connected to the ports. The start time is the time when the device is detected on this port and the activate time is the latest time the device sent traffic.

Format

show voice_vlan voice_device {ports <portlist>}

Parameters

ports - (Optional) Specifies the list of ports to be configured here.
<portlist> - Enter a list of ports used to be displayed here.

Restrictions

None.

Example

To display the voice devices that are connected to the ports 1-5:

```
DGS-3000-28XMP:admin#show voice_vlan voice_device ports 1-5
Command: show voice_vlan voice_device ports 1-5

Ports  Voice Device       Start Time        Last Active Time
-----  -----------------  ----------------  ----------------
1      00-E0-BB-00-00-01  2018-1-15 09:00   2018-1-15 10:30
1      00-E0-BB-00-00-02  2018-1-15 14:10   2018-1-15 15:00
1      00-E0-BB-00-00-03  2018-1-15 14:20   2018-1-15 15:30
2      00-03-6B-00-00-01  2018-1-15 17:15   2018-1-15 18:00
4      00-E0-75-00-00-02  2018-1-15 18:15   2018-1-15 20:00
5      00-01-E3-01-02-03  2018-1-15 18:30   2018-1-15 20:30

Total Entries : 6

DGS-3000-28XMP:admin#
```

95-12 show voice_vlan lldp_med voice_device

Description

This command is used to show the voice devices being discovered by the LLDP-MED.

Format

show voice_vlan lldp_med voice_device

Parameters

None.

Restrictions

None.

Example

To display the voice devices discovered by LLDP-MED:

```
DGS-3000-28XMP:admin#show voice_vlan lldp_med voice_device
Command: show voice_vlan lldp_med voice_device

Index                 : 1
Local Port            : 1
Chassis ID Subtype : MAC Address
Chassis ID            : 00-E0-BB-00-00-11
Port ID Subtype     : Network Address
Port ID               : 172.18.1.1
Create Time          : 10/6/2008 09:00
Remain Time          : 120 Seconds

Index                 : 2
Local Port            : 3
Chassis ID Subtype : MAC Address
Chassis ID            : 00-E0-BB-00-00-12
Port ID Subtype     : Network Address
Port ID               : 172.18.1.2
Create Time          : 10/6/2008 09:00
Remain Time          : 120 Seconds


Total Entries: 2
DGS-3000-28XMP:admin#
```

Chapter 96 Web-based Access Control (WAC) Command List

enable wac
disable wac
config wac authorization attributes {radius [enable | disable] | local [enable | disable]}(1)
config wac ports [<portlist> | all] {state [enable | disable] | aging_time [infinite | <min 1-1440>] | idle_time [infinite | <min 1-1440>] | block_time [<sec 0-300>]}(1)
config wac method [local | radius]
config wac default_redirpath <string 128>
config wac clear_default_redirpath
config wac virtual_ip {<ipaddr> | <ipv6addr>}(1)
config wac switch_http_port <tcp_port_number 1-65535> {[http | https]}
create wac user <username 15> {[vlan <vlan_name 32> | vlanid <vlanid 1-4094>]}
delete wac [user <username 15> | all_users]
config wac user <username 15> [vlan <vlan_name 32> | vlanid <vlanid 1-4094> | clear_vlan]
show wac
show wac ports {<portlist>}
show wac user
show wac auth_state ports {<portlist>}
clear wac auth_state [ports [<portlist> | all] {authenticated | authenticating | blocked} | macaddr <macaddr>]
config wac authentication_page element [default | page_title <desc 128> | login_window_title <desc 64> | user_name_title <desc 32> | password_title <desc 32> | logout_window_title <desc 64> | notification_line <value 1-5> <desc 128>]
show wac authenticate_page
config wac trap state [enable | disable]

96-1 enable wac

Description

This command is used to enable the WAC function.

Format

enable wac

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable the WAC function:

```
DGS-3000-28XMP:admin#enable wac
Command: enable wac

Success.

DGS-3000-28XMP:admin#
```

96-2 disable wac

Description

This command is used to disable the WAC function.

Format

disable wac

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To disable the WAC function:

```
DGS-3000-28XMP:admin#disable wac
Command: disable wac

Success.

DGS-3000-28XMP:admin#
```

96-3 config wac authorization attributes

Description

This command is used to configure the acceptance of an authorized configuration. When the authorization is enabled for WAC's RADIUS, the authorized data assigned by the RADUIS server will be accepted if the global authorization network is enabled. When the authorization is enabled for WAC's local, the authorized data assigned by the local database will be accepted.

Format

config wac authorization attributes {radius [enable | disable] | local [enable | disable]}(1)

Parameters

radius - If specified to enable, the authorized data assigned by the RADUIS server will be accepted if the global authorization network is enabled. The default state is enabled. **enable** - Specifies to enable authorized data assigned by the RADIUS server to be accepted. **disable** - Specifies to disable authorized data assigned by the RADIUS server from being accepted.
local - If specified to enable, the authorized data assigned by the local database will be accepted if the global authorization network is enabled. The default state is enabled. **enable** - Specifies to enable authorized data assigned by the local database to be accepted. **disable** - Specifies to disable authorized data assigned by the local database from being accepted.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the acceptance of an authorized configuration:

```
DGS-3000-28XMP:admin#config wac authorization attributes local disable
Command: config wac authorization attributes local disable

Success.

DGS-3000-28XMP:admin#
```

96-4 config wac ports

Description

This command is used to configure the WAC port parameters.

Format

config wac ports [<portlist> | all] {state [enable | disable] | aging_time [infinite | <min 1-1440>] | idle_time [infinite | <min 1-1440>] | block_time [<sec 0-300>]}(1)

Parameters

<portlist> - Enter a range of ports to configure.
all - Specifies to configure all ports.
state - Specifies to enable or disable the WAC state. **enable** - Specifies to enable the WAC state. **disable** - Specifies to disable the WAC state.
aging_time - Specifies a time period during which an authenticated host will be kept in authenticated state. The default value is 1440 minutes. **infinite** - Specifies to indicate the authenticated host on the port will not ageout. **<min 1-1440>** - Enter an ageout value between 1 and 1440 minutes.
idle_time - Specifies a time period after which an authenticated host will be moved to un-authenticated state if there is no traffic during that period. The default value is infinite. **infinite** - Specifies to indicate the host will not be removed from the authenticated state due to idle of traffic.

<min 1-1440> - Enter an idle time between 1 and 1440 minutes.

block_time - If a host fails to pass the authentication, it will be blocked for this period of time before it can be re-authenticated.The default value is 60 seconds.

<sec 0-300> - Enter a block time between 0 and 300 seconds.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the WAC port state:

```
DGS-3000-28XMP:admin#config wac ports 1-8 state enable
Command: config wac ports 1-8 state enable

Success.

DGS-3000-28XMP:admin#
```

To configure the WAC port aging time:

```
DGS-3000-28XMP:admin#config wac ports 1-5 aging_time 200
Command: config wac ports 1-5 aging_time 200

Success.

DGS-3000-28XMP:admin#
```

96-5 config wac method

Description

This command is used to allow specification of the RADIUS protocol used by WAC to complete RADIUS authentication. WAC shares other RADIUS configuration with 802.1X. When using this command to set the RADIUS protocol, users must make sure the RADIUS server added by the config RADIUS command supports the protocol.

Format

config wac method [local | radius]

Parameters

local - Specifies the authentication will be done via the local database.

radius - Specifies the authentication will be done via the RADIUS server.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the WAC authentication method:

```
DGS-3000-28XMP:admin#config wac method radius
Command: config wac method radius

Success.

DGS-3000-28XMP:admin#
```

96-6 config wac default_redirpath

Description

This command is used to configure the WAC default redirect path. If default redirect path is configured, the user will be redirected to the default redirect path after successful authentication. When the string is cleared, the client will not be redirected to another URL after successful authentication.

Format

config wac default_redirpath <string 128>

Parameters

<string 128> - Enter the URL that the client will be redirected to after successful authentication. By default, the redirected path is cleared.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the WAC default redirect path:

```
DGS-3000-28XMP:admin#config wac default_redirpath http://www.dlink.com
Command: config wac default_redirpath http://www.dlink.com

Success.

DGS-3000-28XMP:admin#
```

96-7 config wac clear_default_redirpath

Description

This command is used to clear the WAC default redirect path. When the string is cleared, the client will not be redirected to another URL after successful authentication.

Format

config wac clear_default_redirpath

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To clear the WAC default redirect path:

```
DGS-3000-28XMP:admin#config wac clear_default_redirpath
Command: config wac clear_default_redirpath

Success.

DGS-3000-28XMP:admin#
```

96-8 config wac virtual_ip

Description

This command is used to configure the virtual IP address for WAC. The virtual IP of WAC is used to accept authentication request from unauthenticated host. Only requests sent to this IP will get response correctly.

This IP does not respond to ARP request or ICMP packet!

NOTE: The WAC virtual IP address should be configured before enabling WAC because WAC will not work correctly if the virtual IP address is not set. A warning message “Warning! WAC virtual IPv4 or IPv6 address is not configured.” will be prompted even when enabling WAC successfully.

Format

config wac virtual_ip {<ipaddr> | <ipv6addr>}(1)

Parameters

<ipaddr> - Enter the IPv4 address of the virtual IP.
<ipv6addr> - Enter the IPv6 address of the virtual IP

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

Set virtual IP address:

```
DGS-3000-28XMP:admin#config wac virtual_ip 1.1.1.1
Command: config wac virtual_ip 1.1.1.1

Success.

DGS-3000-28XMP:admin#
```

96-9 config wac switch_http_port

Description

This command is used to configure the TCP port which the WAC switch listens to. The TCP port for HTTP or HTTPs is used to identify the HTTP or HTTPs packets that will be trapped to CPU for authentication processing, or to access the login page. If not specified, the default port number for HTTP is 80, and the default port number for HTTPS is 443. If no protocol is specified, the protocol is HTTP.

Format

config wac switch_http_port <tcp_port_number 1-65535> {[http | https]}

Parameters

<tcp_port_number 1-65535> - Enter a TCP port which the WAC switch listens to and uses to finish the authenticating process.
http - (Optional) Specifies that WAC runs HTTP protocol on this TCP port.
https - (Optional) Specifies that WAC runs HTTPS protocol on this TCP port.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure a TCP port which the WAC switch listens to:

```
DGS-3000-28XMP:admin#config wac switch_http_port 8888 http
Command: config wac switch_http_port 8888 http

Success.

DGS-3000-28XMP:admin#
```

96-10 create wac user

Description

This command is used to create accounts for Web-based Access Control. This user account is independent of the login user account. If VLAN is not specified, the user will not get a VLAN assigned after the authentication.

Format

create wac user <username 15> {[vlan <vlan_name 32> | vlanid <vlanid 1-4094>]}

Parameters

<username 15> - Enter the user account for Web-based Access Control.
vlan - (Optional) Specifies the authentication VLAN name. **<vlan_name 32>** - Enter the authentication VLAN name. The VLAN name can be up to 32 characters long.
vlanid - (Optional) Specifies the authentication VLAN ID number. **<vlanid 1-4094>** - Enter the authentication VLAN ID number. The VLAN ID must be between 1 and 4094.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To create a WAC account:

```
DGS-3000-28XMP:admin#create wac user abc vlanid 123
Command: create wac user abc vlanid 123

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

DGS-3000-28XMP:admin#
```

96-11 delete wac

Description

This command is used to delete an account.

Format

delete wac [user <username 15> | all_users]

Parameters

user - Specifies the user account for Web-based Access Control. **<username 15>** - Enter the user account for Web-based Access Control. The username can be up to 15 characters long.
all_users - Specifies this option to delete all current WAC users.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete a WAC account:

```
DGS-3000-28XMP:admin#delete wac user duhon
Command: delete wac user duhon

Success.

DGS-3000-28XMP:admin#
```

96-12 config wac user

Description

This command is used to change the VLAN associated with a user.

Format

config wac user <username 15> [vlan <vlan_name 32> | vlanid <vlanid 1-4094> | clear_vlan]

Parameters

<username 15> - Enter the name of user account which will change its VID.
vlan - Specifies the authentication VLAN name. **<vlan_name 32>** - Enter the authentication VLAN name. The VLAN name can be up to 32 characters long.
vlanid - Specifies the authentication VLAN ID. **<vlanid 1-4094>** - Enter the authentication VLAN ID. The VLAN ID must be between 1 and 4094.
clear_vlan - Specifies to clear the specified VLAN.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the user's VLAN:

```
DGS-3000-28XMP:admin#config wac user abc vlanid 100
Command: config wac user abc vlanid 100

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

DGS-3000-28XMP:admin#
```

96-13 show wac

Description

This command is used to display the WAC global setting.

Format

show wac

Parameters

None.

Restrictions

None.

Example

To show WAC:

```
DGS-3000-28XMP:admin#admin#show wac
Command: show wac

 Web-based Access Control
 --------------------------------
 State                   : Enabled
 Method                  : RADIUS
 Redirect Path           : http://www.dlink.com
 Virtual IP              : 1.1.1.1
 Virtual IPv6            : ::
 Switch HTTP Port        : 8888 (HTTP)
 RADIUS Authorization    : Enabled
 Local Authorization     : Disabled
 Trap State              : Enabled

DGS-3000-28XMP:admin#
```

96-14 show wac ports

Description

This command is used to display WAC port information.

Format

show wac ports {<portlist>}

Parameters

<portlist> - (Optional) Enter a range of member ports to display the status.

Restrictions

None.

Example

To display WAC ports 1 to 3:

```
DGS-3000-28XMP:admin#show wac ports 1-3
Command: show wac ports 1-3

 Port    State        Aging Time    Idle Time      Block Time
                        (min)         (min)          (sec)
 -----  --------    -------------  -------------  -------------
 1      Enabled     200            Infinite       60
 2      Enabled     200            Infinite       60
 3      Enabled     200            Infinite       60

DGS-3000-28XMP:admin#
```

96-15 show wac user

Description

This command is used to display WAC user accounts.

Format

show wac user

Parameters

None.

Restrictions

None.

Example

To show Web authentication user accounts:

```
DGS-3000-28XMP:admin#show wac user
Command: show wac user

 User Name          Password           VID
 -----------------  -----------------  ---------
   abc                12345              100

 Total Entries:1


DGS-3000-28XMP:admin#
```

96-16 show wac auth_state ports

Description

This command is used to display the authentication state for ports.

Format

show wac auth_state ports {<portlist>}

Parameters

<portlist> - (Optional) Enter the list of ports whose WAC authentication state will be displayed.

Restrictions

None.

Example

To display the WAC authentication status of ports:

```
DGS-3000-28XMP:admin#show wac auth_state ports
Command: show wac auth_state ports

P:Port-based   Pri:Priority

Port    MAC Address       Original  State       VID Pri Aging Time/ Idle
                           RX VID                    Block Time  Time
------ ------------------- ---- -------------- ---- -- ----------- ----
1      00-23-7D-BC-2E-18(P) 1    Authenticating -    -  17          -

 Total Authenticating Hosts  : 1
 Total Authenticated Hosts   : 0
 Total Blocked Hosts         : 0

DGS-3000-28XMP:admin#
```

96-17 clear wac auth_state

Description

This command is used to clear the authentication state of a port. The port will return to un-authenticated state. All the timers associated with the port will be reset.

Format

clear wac auth_state [ports [<portlist> | all] {authenticated | authenticating | blocked} | macaddr <macaddr>]

Parameters

ports - Specifies the list of ports whose WAC state will be cleared.
- **<portlist>** - Enter a range of ports.
- **all** - Specifies to clear all ports.
- **authenticated** - (Optional) Specifies to clear all authenticated users for a port.
- **authenticating** - (Optional) Specifies to clear all authenticating users for a port.
- **blocked** - (Optional) Specifies to clear all blocked users for a port.

macaddr - Specifies to clear a specific user.
- **<macaddr>** - Enter the MAC address here.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To clear the WAC authentication state of ports 1 to 5:

```
DGS-3000-28XMP:admin#clear wac auth_state ports 1-5
Command: clear wac auth_state ports 1-5

Success.

DGS-3000-28XMP:admin#
```

96-18 config wac authentication_page element

Description

This command is used to customize the authentication page elements.

Format

config wac authentication_page element [default | page_title <desc 128> | login_window_title <desc 64> | user_name_title <desc 32> | password_title <desc 32> | logout_window_title <desc 64> | notification_line <value 1-5> <desc 128>]

Parameters

default - Specifies to reset the page elements to default.
page_title - Specifies to configure the title of the authentication page. **<desc 128>** - Enter the page title used here. This value can be up to 128 characters long.
login_window_title - Specifies to configure the login window title of the authentication page **<desc 64>** - Enter the login window title used here. This value can be up to 64 characters long.
user_name_title - Specifies to configure the user name title of the authentication page **<desc 32>** - Enter the user name title used here. This value can be up to 32 characters long.
password_title - Specifies to configure the password title of the authentication page. **<desc 32>** - Enter the password title used here. This value can be up to 32 characters long.
logout_window_title - Specifies to configure the logout window title of the authentication page. **<desc 64>** - Enter the lohout window title used here. This value can be up to 64 characters long.
notification_line - Specifies to set the notification information by line in authentication Web pages. **<value 1-5>** - Enter the notification line number used here. This value must be between 1 and 5. **<desc 128>** - Enter the notification line description used here. This value can be up to 128 characters long.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To customize the authentication page elements:

```
DGS-3000-28XMP:admin#config wac authentication_page element notification_line 1 Copyright @ 2018 D-Link All Rights Reserved
Command: config wac authentication_page element notification_line 1 Copyright @ 2018 D-Link All Rights Reserved


Success.


DGS-3000-28XMP:admin#
```

96-19 show wac authenticate_page

Description

This command is used to show the elements of the customized authenticate pages.

Format

show wac authenticate_page

Parameters

None.

Restrictions

None.

Example

The following example displays the authentication page elements:

```
DGS-3000-28XMP:admin#show wac authenticate_page
Command: show wac authenticate_page


Page Title              : D-Link
Login Window Title      : Authentication Login
User Name Title         : User Name
Password Title          : Password
Logout Window Title     : Logout From The Network
Notification            :
  Copyright @ 2018 D-Link All Rights Reserved




DGS-3000-28XMP:admin#
```

96-20 config wac trap state

Description

This command is used to enable or disable the WAC trap state.

Format

config wac trap state [enable | disable]

Parameters

enable - Specifies to enable the WAC trap state.
disable - Specifies to disable the WAC trap state.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

This example show how to enable the WAC trap state.

```
DGS-3000-28XMP:admin#config wac trap state enable
Command: config wac trap state enable

Success.

DGS-3000-28XMP:admin#
```

Chapter 97 Zero Touch Provisioning (ZTP) Command List

config reset_button reboot state [enable | disable]
config reset_button ztp state [enable | disable]
config reset_button factory state [enable | disable]
show reset_button state

97-1 config reset_button reboot state

Description

This command is used to configure the reboot state of the reset button on the Switch.

Format

config reset_button reboot state [enable | disable]

Parameters

enable - Specifies to enable the reboot state. When enabled, pressing the reset button on the Switch within 5 seconds will reboot the Switch.
disable - Specifies to disable the reboot state.

Restrictions

Only Administrators can issue this command.

Example

To enable the reboot state:

```
DGS-3000-28XMP:admin#config reset_button reboot state enable
Command: config reset_button reboot state enable

Success.

DGS-3000-28XMP:admin#
```

97-2 config reset_button ztp state

Description

This command is used to configure the ZTP state of the reset button on the Switch.

Format

config reset_button ztp state [enable | disable]

Parameters

enable - Specifies to enable the ZTP state. When enabled, pressing the reset button on the Switch between 5 and 10 seconds will initiate ZTP.
disable - Specifies to disable the ZTP state.

Restrictions

Only Administrators can issue this command.

Example

To enable the ZTP state:

```
DGS-3000-28XMP:admin#config reset_button ztp state enable
Command: config reset_button ztp state enable

Success.

DGS-3000-28XMP:admin#
```

97-3 config reset_button factory state

Description

This command is used to configure the factory reset state of the reset button on the Switch.

Format

config reset_button factory state [enable | disable]

Parameters

enable - Specifies to enable the factory reset state. When enabled, pressing the reset button on the Switch more than 10 seconds will reset the Switch to factory defaults.
disable - Specifies to disable the factory reset state.

Restrictions

Only Administrators can issue this command.

Example

To enable the factory reset state:

```
DGS-3000-28XMP:admin#config reset_button factory state enable
Command: config reset_button factory state enable

Success.

DGS-3000-28XMP:admin#
```

97-4 show reset_button state

Description

This command is used to display the state of the reset button on the Switch.

Format

show reset_button state

Parameters

None.

Restrictions

None.

Example

To display the state of the reset button on the Switch:

```
DGS-3000-28XMP:admin#show reset_button state
Command: show reset_button state

Reset Status
-------------------------
Reboot          : Enabled
ZTP             : Enabled
Factory default : Enabled

DGS-3000-28XMP:admin#
```

Appendix A Password Recovery Procedure

This chapter describes the procedure for resetting passwords on D-Link switches. Authenticating any user who tries to access networks is necessary and important. The basic authentication method used to accept qualified users is through a local login, utilizing a Username and Password. Sometimes, passwords get forgotten or destroyed, so network administrators need to reset these passwords. This chapter explains how the Password Recovery feature can help network administrators reach this goal.

The following steps explain how to use the Password Recovery feature on D-Link devices to easily recover passwords.

Complete these steps to reset the password:

1. For security reasons, the Password Recovery feature requires the user to physically access the device. Therefore this feature is only applicable when there is a direct connection to the console port of the device. It is necessary for the user needs to attach a terminal or PC with terminal emulation to the console port of the Switch.
2. Power on the Switch. After the 'Starting runtime image' message, the Switch will allow 2 seconds for the user to press the hotkey [^] (Shift + 6) to enter the "Password Recovery Mode." Once the Switch enters the "Password Recovery Mode," all ports on the Switch will be disabled and all port LEDs will be lit.

```
  Boot Procedure                                          V4.00.001
-------------------------------------------------------------------------------

  Power On Self Test ....................................  100 %

  MAC Address   : F0-7D-68-15-10-00
  H/W Version   : B1

  Please Wait, Loading V4.00.010 Runtime Image ..............  100 %
  UART init .................................................  100 %
  Starting runtime image
```

```
Password Recovery Mode
>
```

3. In the "Password Recovery Mode" only the following commands can be used.

Command	Parameters
reset config {force_agree}	The **reset config** command resets the whole configuration back to the default values. If **force_agree** is specified, the configuration will reset to default without the user's agreement.
reboot	The **reboot** command exits the Reset Password Recovery Mode and restarts the Switch. A confirmation message will be displayed to allow the user to save the current settings.
reset account	The **reset** account command deletes all the previously created accounts.
reset password {<username>}	The **reset password** command resets the password of the specified user. If a username is not specified, the passwords of all users will be reset.
show account	The **show account** command displays all previously created accounts.

Appendix B System Log Entries

The following table lists all possible entries and their corresponding meanings that will appear in the System Log of this Switch.

Category	Event Description	Log Information	Severity
System	System started up	System started up	Critical
	System warm start	System warm start	Critical
	System cold start	System cold start	Critical
	Configuration saved to flash by console	Configuration saved to flash by console (Username: <username>)	Informational
	System log saved to flash by console	System log saved to flash by console (Username: <username>)	Informational
	Configuration and log saved to flash by console	Configuration and log saved to flash by console (Username: <username>)	Informational
	Configuration saved to flash	Configuration saved to flash (Username: <username>, IP: <ipaddr | ipv6addr>)	Informational
	System log saved to flash	System log saved to flash (Username: <username>, IP: <ipaddr | ipv6addr>)	Informational
	Configuration and log saved to flash	Configuration and log saved to flash (Username: <username>, IP: <ipaddr | ipv6addr>)	Informational
	Side fan failed	Right Side Fan <fanID> failed	Critical
	Side fan recovered	Right Side Fan <fanID> recovered	Critical
	Temperature sensor enters alarm state	Temperature sensor <sensorID> enters alarm state (current temperature: <temperature>)	Warning
	Temperature recovers to normal	Temperature sensor <sensorID> recovers to normal state (current temperature: <temperature>)	Informational
Upload/Download	Firmware upgraded successfully by Web/SNMP/Telnet/SSH/SIM	Firmware upgraded by <session> successfully (Username: <username>, IP: <ipaddr | ipv6addr>, MAC: <macaddr>)	Informational
	Firmware upgrade was unsuccessful by Web/SNMP/Telnet/SSH/SIM	Firmware upgrade by <session> was unsuccessful! (Username: <username>, IP: <ipaddr | ipv6addr>, MAC: <macaddr>)	Warning
	Firmware successfully uploaded by Web/SNMP/Telnet/SSH/SIM	Firmware successfully uploaded by <session> (Username: <username>, IP: <ipaddr | ipv6addr>, MAC: <macaddr>)	Informational
	Firmware upload was unsuccessful by Web/SNMP/Telnet/SSH/SIM	Firmware upload by <session> was unsuccessful! (Username: <username>, IP: <ipaddr | ipv6addr>, MAC: <macaddr>)	Warning
	Configuration successfully downloaded by Web/SNMP/Telnet/SSH/SIM	Configuration successfully downloaded by <session> (Username: <username>, IP: <ipaddr | ipv6addr>, MAC: <macaddr>)	Informational
	Configuration download was unsuccessful by Web/SNMP/Telnet/SSH/SIM	Configuration download by <session> was unsuccessful! (Username: <username>, IP: <ipaddr | ipv6addr>, MAC: <macaddr>)	Warning
	Configuration successfully uploaded by Web/SNMP/Telnet/SSH/SIM	Configuration successfully uploaded by <session> (Username: <username>, IP: <ipaddr | ipv6addr>, MAC: <macaddr>)	Informational
	Configuration upload was unsuccessful by Web/SNMP/Telnet/SSH/SIM	Configuration upload by <session> was unsuccessful! (Username: <username>, IP: <ipaddr | ipv6addr>, MAC: <macaddr>)	Warning
	Log message successfully uploaded by	Log message successfully uploaded by <session> (Username: <username>, IP: <ipaddr | ipv6addr>,	Informational

Category	Event Description	Log Information	Severity
	Web/SNMP/Telnet/SSH/SIM	MAC: <macaddr>)	
	Log message upload was unsuccessful by Web/SNMP/Telnet/SSH/SIM	Log message upload by <session> was unsuccessful! (Username: <username>, IP: <ipaddr | ipv6addr>, MAC: <macaddr>)	Warning
	Firmware upgraded successfully by console	Firmware upgraded by console successfully (Username: <username>)	Informational
	Firmware upgrade was unsuccessful by console	Firmware upgrade by console was unsuccessful! (Username: <username>)	Warning
	Firmware successfully uploaded by console	Firmware successfully uploaded by console (Username: <username>)	Informational
	Firmware upload was unsuccessful by console	Firmware upload by console was unsuccessful! (Username: <username>)	Warning
	Configuration successfully downloaded by console	Configuration successfully downloaded by console (Username: <username>)	Informational
	Configuration download was unsuccessful by console	Configuration download by console was unsuccessful! (Username: <username>)	Warning
	Configuration successfully uploaded by console	Configuration successfully uploaded by console (Username: <username>)	Informational
	Configuration upload was unsuccessful by console	Configuration upload by console was unsuccessful! (Username: <username>)	Warning
	Log message successfully uploaded by console	Log message successfully uploaded by console (Username: <username>)	Informational
	Log message upload was unsuccessful by console	Log message upload by console was unsuccessful! (Username: <username>)	Warning
Port	Port link up	Port <portNum> link up, <link state>	Informational
	Port link down	Port <portNum> link down	Informational
Login/Logout	Successful login through Console	Successful login through Console (Username: <username>)	Informational
	Login failed through Console	Login failed through Console (Username: <username>)	Warning
	Logout through Console	Logout through Console (Username: <username>)	Informational
	Console session timed out	Console session timed out (Username: <username>)	Informational
	Successful login through Web/Web(SSL)/Telnet/SSH	Successful login through <session> (Username: <username>, IP: <ipaddr | ipv6addr>)	Informational
	Login failed through Web/Web(SSL)/Telnet/SSH	Login failed through <session> (Username: <username>, IP: <ipaddr | ipv6addr>)	Warning
	Logout through Web/Web(SSL)/Telnet/SSH	Logout through <session> (Username: <username>, IP: <ipaddr | ipv6addr>)	Informational
	Web/Web(SSL)/Telnet/SSH session timed out	<session> session timed out (Username: <username>, IP: <ipaddr | ipv6addr>)	Informational
SNMP	SNMP request received with invalid community string	SNMP request received from <ipaddr | ipv6addr> with invalid community string!	Informational
STP	Topology changed	Topology changed (Instance: <InstanceID>, Port: <portNum>, MAC: <macaddr>)	Notice
	Enable Spanning Tree Protocol	Spanning Tree Protocol is enabled	Informational
	Disable Spanning Tree Protocol	Spanning Tree Protocol is disabled	Informational
	New root bridge	CIST New Root bridge selected (MAC: <macaddr> Priority: <value>)	Informational
	New root bridge	CIST Region New Root bridge selected (MAC: <macaddr> Priority: <value>)	Informational
	New root bridge	MSTI Region New Root bridge selected (Instance: <InstanceID>, MAC: <macaddr> Priority: <value>)	Informational

Category	Event Description	Log Information	Severity
	New root bridge	New Root bridge selected (MAC: <macaddr> Priority: <value>)	Informational
	New root port	New root port selected (Instance: <InstanceID>, Port: <portNum>)	Notice
	Spanning Tree port status changed	Spanning Tree port status changed (Instance: <InstanceID>, Port: <portNum>) <old_status> -> <new_status>	Notice
	Spanning Tree port role changed	Spanning Tree port role changed (Instance: <InstanceID>, Port: <portNum>) <old_role> -> <new_role>	Informational
	Spanning Tree instance created	Spanning Tree instance created (Instance: <InstanceID>)	Informational
	Spanning Tree instance deleted	Spanning Tree instance deleted (Instance: <InstanceID>)	Informational
	Spanning Tree Version changed	Spanning Tree version changed (new version: <new_version>)	Informational
	Spanning Tree MST configuration ID name and revision level changed	Spanning Tree MST configuration ID name and revision level changed (name: <name>, revision level <revision_level>)	Informational
	Spanning Tree MST configuration ID VLAN mapping table added	Spanning Tree MST configuration ID VLAN mapping table changed (instance: <InstanceID> add vlan <startvlanid> [- <endvlanid>])	Informational
	Spanning Tree MST configuration ID VLAN mapping table deleted	Spanning Tree MST configuration ID VLAN mapping table changed (instance: <InstanceID> delete vlan <startvlanid> [- <endvlanid>])	Informational
DoS Attack Prevention	Spoofing attack 1. The source IP is same as switch's interface ip but the source mac is different 2. Source IP is the same as the switch's IP in ARP packet 3. Self IP packet detected	Possible spoofing attack from IP: <ipaddr | ipv6addr>, MAC: <macaddr>, port: <portNum>	Critical
	The DoS attack is blocked	<dos_name> is blocked from (IP: <ipaddr | ipv6addr> Port: <portNum>)	Critical
SSH Server	SSH server is enabled	SSH server is enabled	Informational
	SSH server is disabled	SSH server is disabled	Informational
AAA	Authentication policy is enabled	Authentication Policy is enabled (Module: AAA)	Informational
	Authentication policy is disabled	Authentication Policy is disabled (Module: AAA)	Informational
	Successful login through Console authenticated by AAA local method	Successful login through Console authenticated by AAA local method (Username: <username>)	Informational
	Login failed through Console authenticated by AAA local method	Login failed through Console authenticated by AAA local method (Username: <username>)	Warning
	Successful login through Web/Web(SSL)/Telnet/SSH authenticated by AAA local method	Successful login through <session> from <ipaddr | ipv6addr> authenticated by AAA local method (Username: <username>)	Informational
	Login failed through Web/Web(SSL)/Telnet/SSH authenticated by AAA local method	Login failed through <session> from <ipaddr | ipv6addr> authenticated by AAA local method (Username: <username>)	Warning
	Successful login through Console authenticated by AAA	Successful login through Console authenticated by AAA none method (Username: <username>)	Informational

Category	Event Description	Log Information	Severity
	none method		
	Successful login through Web/Web(SSL)/Telnet/SSH authenticated by AAA none method	Successful login through <session> from <ipaddr | ipv6addr> authenticated by AAA none method (Username: <username>)	Informational
	Successful login through Console authenticated by AAA server	Successful login through Console authenticated by AAA server <ipaddr | ipv6addr> (Username: <username>)	Informational
	Login failed through Console authenticated by AAA server	Login failed through Console authenticated by AAA server <ipaddr | ipv6addr> (Username: <username>)	Warning
	Login failed through Console due to AAA server timeout or improper configuration	Login failed through Console due to AAA server timeout or improper configuration (Username: <username>)	Warning
	Successful login through Web/Web(SSL)/Telnet/SSH authenticated by AAA server	Successful login through <session> from <ipaddr | ipv6addr> authenticated by AAA server <ipaddr | ipv6addr> (Username: <username>)	Informational
	Login failed through Web/Web(SSL)/Telnet/SSH authenticated by AAA server	Login failed through <session> from <ipaddr | ipv6addr> authenticated by AAA server <ipaddr | ipv6addr> (Username: <username>)	Warning
	Login failed through Web/Web(SSL)/Telnet/SSH due to AAA server timeout or improper configuration	Login failed through <session> from <ipaddr | ipv6addr> due to AAA server timeout or improper configuration (Username: <username>)	Warning
	Successful Enable Admin through Console authenticated by AAA local_enable method	Successful Enable Admin through Console authenticated by AAA local_enable method (Username: <username>)	Informational
	Enable Admin failed through Console authenticated by AAA local_enable method	Enable Admin failed through Console authenticated by AAA local_enable method (Username: <username>)	Warning
	Successful Enable Admin through Web/Web(SSL)/Telnet/SSH authenticated by AAA local_enable method	Successful Enable Admin through <session> from <ipaddr | ipv6addr> authenticated by AAA local_enable method (Username: <username>)	Informational
	Enable Admin failed through Web/Web(SSL)/Telnet/SSH authenticated by AAA local_enable method	Enable Admin failed through <session> from <ipaddr | ipv6addr> authenticated by AAA local_enable method (Username: <username>)	Warning
	Successful Enable Admin through Console authenticated by AAA none method	Successful Enable Admin through Console authenticated by AAA none method (Username: <username>)	Informational
	Successful Enable Admin through Web/Web(SSL)/Telnet/SSH authenticated by AAA none method	Successful Enable Admin through <session> from <ipaddr | ipv6addr> authenticated by AAA none method (Username: <username>)	Informational
	Successful Enable Admin through Console authenticated by AAA server	Successful Enable Admin through Console authenticated by AAA server <ipaddr | ipv6addr> (Username: <username>)	Informational
	Enable Admin failed through Console authenticated by AAA server	Enable Admin failed through Console authenticated by AAA server <ipaddr | ipv6addr> (Username: <username>)	Warning
	Enable Admin failed through Console due to AAA server timeout or improper configuration	Enable Admin failed through Console due to AAA server timeout or improper configuration (Username: <username>)	Warning
	Successful Enable Admin through	Successful Enable Admin through <session> from <ipaddr | ipv6addr> authenticated by AAA server	Informational

Category	Event Description	Log Information	Severity
	Web/Web(SSL)/Telnet/SSH authenticated by AAA server	<ipaddr | ipv6addr> (Username: <username>)	
	Enable Admin failed through Web/Web(SSL)/Telnet/SSH authenticated by AAA server	Enable Admin failed through <session> from <ipaddr | ipv6addr> authenticated by AAA server <ipaddr | ipv6addr> (Username: <username>)	Warning
	Enable Admin failed through Web/Web(SSL)/Telnet/SSH due to AAA server timeout or improper configuration	Enable Admin failed through <session> from <ipaddr | ipv6addr> due to AAA server timeout or improper configuration (Username: <username>)	Warning
	AAA server timed out	AAA server <ipaddr | ipv6addr> (Protocol: <protocol>) connection failed	Warning
	AAA server ACK error	AAA server <ipaddr | ipv6addr> (Protocol: <protocol>) response is wrong	Warning
	AAA does not support this functionality	AAA doesn't support this functionality	Informational
Port Security	Port security is exceeded to its maximum learning size and will not learn any new address	Port security violation (MAC address: <macaddr> on port: <portNum>)	Warning
IMPB	Unauthenticated IP address encountered and discarded by IP-MAC port binding	Unauthenticated IP-MAC address and discarded by IMPB (IP: <ipaddr>, MAC: <macaddr>, Port <portNum>)	Warning
	Dynamic IMPB entry is conflict with static ARP	Dynamic IMPB entry conflicts with static ARP (IP: <ipaddr>, MAC: <macaddr>, Port <portNum>)	Warning
	Dynamic IMPB entry is conflict with static FDB	Dynamic IMPB entry conflicts with static FDB (IP: <ipaddr>, MAC: <macaddr>, Port <portNum>)	Warning
	Dynamic IMPB entry conflicts with static IMPB	Dynamic IMPB entry conflicts with static IMPB (IP: <ipaddr>, MAC: <macaddr>, Port <portNum>)	Warning
	Creating IMPB entry failed due to no ACL rule available	Creating IMPB entry failed due to no ACL rule being available (IP: <ipaddr>, MAC: <macaddr>, Port <portNum>)	Warning
IP and Password Changed	IP Address change activity by console	Management IP address was changed by console (Username: <username>)	Informational
	IP Address change activity	Management IP address was changed by (Username: <username>, IP: <ipaddr | ipv6addr>)	Informational
	Password change activity by console	Password was changed by console (Username: <username>)	Informational
	Password change activity	Password was changed by (Username: <username>, IP: <ipaddr | ipv6addr>)	Informational
Safeguard Engine	Safeguard Engine is in normal mode	Safeguard Engine enters NORMAL mode	Informational
	Safeguard Engine is in filtering packet mode	Safeguard Engine enters EXHAUSTED mode	Warning
Packet Storm	Broadcast storm occurrence	Port <portNum> Broadcast storm is occurring	Warning
	Broadcast storm cleared	Port <portNum> Broadcast storm has cleared	Informational
	Multicast storm occurrence	Port <portNum> Multicast storm is occurring	Warning
	Multicast storm cleared	Port <portNum> Multicast storm has cleared	Informational
	Port shut down due to a packet storm	Port <portNum> is currently shut down due to a packet storm	Warning
Loop Back Detection	Port loop occurred	Port <portNum> LBD loop occurred. Port blocked.	Critical
	Port loop detection restarted after interval time	Port <portNum> LBD port recovered. Loop detection restarted.	Informational

Category	Event Description	Log Information	Severity
	Port with VID loop occurred	Port <portNum> VID <vlanID> LBD loop occurred. Packet discard begun.	Critical
	Port with VID Loop detection restarted after interval time	Port <portNum> VID <vlanID> LBD recovered. Loop detection restarted.	Informational
802.1X	VID assigned from radius server after radius client authenticated by radius server successfully. This VID will assign to the port and this port will be the VLAN untagged port member.	Radius server <ipaddr | ipv6addr> assigned vid: <vlanID> to port <portNum> (account: <username>)	Informational
	Ingress bandwidth assigned from radius server after radius client authenticated by radius server successfully. This Ingress bandwidth will assign to the port.	Radius server <ipaddr | ipv6addr> assigned ingress bandwidth: <ingressBandwidth> to port <portNum> (account: <username>)	Informational
	Egress bandwidth assigned from radius server after radius client authenticated by radius server successfully. This egress bandwidth will assign to the port.	Radius server <ipaddr | ipv6addr> assigned egress bandwidth: <egressBandwidth> to port <portNum> (account: <username>)	Informational
	802.1p default priority assigned from radius server after radius client authenticated by radius server successfully. This 802.1p default priority will assign to the port.	Radius server <ipaddr | ipv6addr> assigned 802.1p default priority: <priority> to port <portNum> (account: <username>)	Informational
	802.1X authentication failure	802.1x Authentication failure [for <reason>] from (Username: <username>, Port: <portNum>, MAC: <macaddr>)	Warning
	802.1X authentication success	802.1x Authentication success from (Username: <username>, Port: <portNum>, MAC: <macaddr>)	Informational
CFM	Cross-connect is detected	CFM cross-connect. VLAN: <vlanid>, Local(MD Level: <mdlevel>, Port <portNum>, Direction: <mepdirection>) Remote(MEPID: <mepid>, MAC: <macaddr>)	Critical
	Error CFM CCM packet is detected	CFM error ccm. MD Level: <mdlevel>, VLAN: <vlanid>, Local(Port <portNum>, Direction: <mepdirection>) Remote(MEPID: <mepid>, MAC: <macaddr>)	Warning
	Cannot receive remote MEP's CCM packet	CFM remote down. MD Level: <mdlevel>, VLAN: <vlanid>, Local(Port <portNum>, Direction: <mepdirection>)	Warning
	Remote MEP's MAC reports an error status	CFM remote MAC error. MD Level: <mdlevel>, VLAN: <vlanid>, Local(Port <portNum>, Direction: <mepdirection>)	Warning
	Remote MEP detects CFM defects	CFM remote detects a defect. MD Level: <mdlevel>, VLAN: <vlanid>, Local(Port <portNum>, Direction: <mepdirection>)	Informational
Gratuitous ARP	Gratuitous ARP detected duplicate IP.	Conflict IP was detected with this device (IP: <ipaddr>, MAC: <macaddr>, Port <portNum>, Interface: <ipif_name>).	Warning
DHCP Server Screening	Detect untrusted DHCP server IP address	Detected untrusted DHCP server (IP: <ipaddr>, Port: <portNum>)	Informational
	Detected untrusted DHCPv6 server IP address.	Detected untrusted DHCPv6 server (IP: <ipv6addr>, Port:<[unitID:]portNum>)	Informational
	Detected untrusted source IP in ICMPv6 Router Advertisement Message.	Detected untrusted source IP of ICMPv6 Router Advertisement message (IP: <ipv6addr>, Port:<[unitID:]portNum>)	Informational
Command	Command logging	<username>: execute command "<string>"	Informational

Category	Event Description	Log Information	Severity
Logging			
MAC-based Access Control	A host passes the authentication	MAC-based Access Control host login successful (MAC: <macaddr>, port: <portNum>, VID: <vid>)	Informational
	A host fails to pass the authentication	MAC-based Access Control unauthenticated host(MAC: <macaddr>, Port <portNum>, VID: <vid>)	Critical
	A host is aged out	MAC-based Access Control host aged out (MAC: <macaddr>, port: <portNum>, VID: <vid>)	Informational
	The authorized user number on a port reaches the maximum user limit	Port <portNum> enters MAC-based Access Control stop learning state	Warning
	The authorized user number on a port is below the maximum user limit in a time interval (interval is project depended)	Port <portNum> recovers from MAC-based Access Control stop learning state	Warning
	The authorized user number on whole device reaches the maximum user limit	MAC-based Access Control enters stop learning state	Warning
	The authorized user number on whole device is below the maximum user limit in a time interval (interval is project depended)	MAC-based Access Control recovers from stop learning state	Warning
BPDU Protection	BPDU attack happened	Port <port> enter BPDU under protection state (mode: drop)	Informational
	BPDU attack happened	Port <port> enter BPDU under protection state (mode: block)	Informational
	BPDU attack happened	Port <port> enter BPDU under protection state (mode: shutdown)	Informational
	BPDU attack automatically recover	Port <port> recover from BPDU under protection state automatically	Informational
	BPDU attack manually recover	Port <port> recover from BPDU under protection state manually	Informational
Debug	System restart reason: system fatal error	System re-start reason: system fatal error	Emergent
	System restart reason: CPU exception	System re-start reason: CPU exception	Emergent
DULD	A unidirectional link has been detected on this port	Port: <portNum> is unidirectional	Informational
ERPS	Signal failure detected	Signal failure detected on node (MAC: <macaddr>)	Notice
	Signal failure cleared	Signal failure cleared on node (MAC: <macaddr>)	Notice
	RPL owner conflict	RPL owner conflicted on the ring (MAC: <macaddr>)	Warning
	Manual switch is issued	Manual switch is issued on node (MAC: <macaddr>, instance <instance_id>)	Warning
	Force switch is issued	Force switch is issued on node (MAC: <macaddr>, instance <instance_id>)	Warning
	Clear command is issued	Clear command is issued on node (MAC: <macaddr>, instance <instance_id>)	Warning
LLDP-MED	LLDP-MED topology change detected	LLDP-MED topology change detected (on port <portNum>. chassis id: <chassisType>, <chassisID>, port id: <portType>, <portID>, device class: <deviceClass>)	Notice
	Conflict LLDP-MED device type detected	Conflict LLDP-MED device type detected (on port <portNum>, chassis id: <chassisType>, <chassisID>, port id: <portType>, <portID>, device class:	Notice

Category	Event Description	Log Information	Severity
		<deviceClass>)	
	Incompatible LLDP-MED TLV set detected	Incompatible LLDP-MED TLV set detected (on port <portNum>, chassis id: <chassisType>, <chassisID>, port id: <portType>, <portID>, device class: <deviceClass>)	Notice
DDM	DDM exceeded DDM warning threshold	Port <portNum> SFP <thresholdType> exceeded the <thesholdSubType> warning threshold	Warning
	DDM exceeded DDM alarm threshold	Port <portNum> SFP <thresholdType> exceeded the <thesholdSubType> alarm threshold	Critical
	DDM recover from DDM warning threshold	Port <portNum> SFP <thresholdType> recover from the <thesholdSubType> warning threshold	Warning
	DDM recover from DDM alarm threshold	Port <portNum> SFP <thresholdType> recover from the <thesholdSubType> alarm threshold	Critical
WAC	When a client host authenticated successful.	WAC authenticated user (Username: <string>, IP: <ipaddr | ipv6address>, MAC: <macaddr>, Port: <portNum>)	Informational
	When a client host fail to authenticate.	WAC unauthenticated user (User Name: <string>, IP: <ipaddr | ipv6address>, MAC: <macaddr>, Port: <portNum>)	Warning
	This log will be triggered when the number of authorized users reaches the maximum user limit on the whole device.	WAC enters stop learning state.	Warning
	This log will be triggered when the number of authorized users is below the maximum user limit on whole device in a time interval (The interval is project dependent).	WAC recovered from stop learning state.	Warning
Y.1731	AIS condition detected	AIS condition detected. MD Level: <mdlevel>, VLAN: <vlanid>, Local(Port <portNum>, Direction: <mepdirection>, MEPID: <mepid>)	Notice
	AIS condition cleared	AIS condition cleared. MD Level: <mdlevel>, VLAN: <vlanid>, Local(Port <portNum>, Direction: <mepdirection>, MEPID: <mepid>)	Notice
	LCK condition detected	LCK condition detected. MD Level: <mdlevel>, VLAN: <vlanid>, Local(Port <portNum>, Direction: <mepdirection>, MEPID: <mepid>)	Notice
	LCK condition cleared	LCK condition cleared. MD Level: <mdlevel>, VLAN: <vlanid>, Local(Port <portNum>, Direction: <mepdirection>, MEPID: <mepid>)	Notice
DHCPv6 Client	DHCPv6 client interface administrator state changed	DHCPv6 client on interface <intf-name> changed state to <enabled | disabled>	Informational
	DHCPv6 client obtains an ipv6 address from a DHCPv6 server	DHCPv6 client obtains an ipv6 address <ipv6address> on interface <intf-name>	Informational
	The IPv6 address obtained from a DHCPv6 server starts renewing	The IPv6 address <ipv6address> on interface <intf-name> starts renewing.	Informational
	The IPv6 address obtained from a DHCPv6 server renews success	The IPv6 address <ipv6address> on interface <intf-name> renews success.	Informational
	The IPv6 address obtained from a DHCPv6 server starts rebinding	The IPv6 address <ipv6address> on interface <intf-name> starts rebinding.	Informational
	The IPv6 address obtained from a DHCPv6 server rebinds	The IPv6 address <ipv6address> on interface <intf-name> rebinds success.	Informational

Category	Event Description	Log Information	Severity
	success		
	The IPv6 address was deleted	The IPv6 address <ipv6address> on interface <intf-name> was deleted.	Informational
Voice VLAN	When a new voice device is detected in the port	New voice device detected (Port <portNum>, MAC <macaddr>)	Informational
	When a port which is in auto-Voice VLAN mode joins the Voice VLAN	Port <portNum> add into voice VLAN <vid>	Informational
	When a port leaves the Voice VLAN and at the same time, no voice device is detected in the aging interval for that port, the log message will be sent	Port <portNum> remove from voice VLAN <vid>	Informational
DHCPv6 Relay	DHCPv6 relay on a specific interface's administrator state changed.	[DHCPv6_RELAY(1):]DHCPv6 relay on interface <intf-name> changed state to <enabled | disabled>	Informational
PD Alive	PD doesn't reply the ping request.	PD alive check failed. (Port: <portNum>, PD: <ipaddr>)	Warning
ARP Spoofing Prevention	Detect hacker's fake ARP packet.	Gateway <ipaddr> is under attack by <macaddr> from <unitId:portNum>.	Warning
Auto-Backup	System backups the running configuration successfully.	Auto backup has been completed. (file name: <filename>)	Informational
	Running configuration backup failed.	Running configuration backup failed.	Warning
Auto-Image	Auto-image firmware upgraded successfully.	The downloaded firmware was successfully executed by DHCP AutoImage update (TFTP Server IP: <ipaddr>)	Warning
	Auto-image firmware upgrade was unsuccessful.	The downloaded firmware was not successfully executed by DHCP AutoImage update (TFTP Server IP: <ipaddr>)	Warning
RPS	Redundant power is working	Redundant Power is working	Critical
	Redundant power failed	Redundant Power failed	Critical
ZTP	Detect reset button being pressed and trigger the ZTP function	Detect Reset Button being pressed. (Triggering <mode>)	Warning

Appendix C Trap Log Entries

This table lists the trap logs found on the Switch.

Trap Name	Variable Bind	Format	MIB Name
coldStart		V1	RFC-1215 (Rfc-1215.mib)
		V2	SNMPv2-MIB (SNMPv2-MIB.mib)
warmStart		V1	RFC-1215 (Rfc-1215.mib)
		V2	SNMPv2-MIB (SNMPv2-MIB.mib)
linkDown	ifIndex	V1	RFC-1215 (Rfc-1215.mib)
		V2	IF-MIB (IF-MIB.mib)
linkup	ifIndex	V1	RFC-1215 (Rfc-1215.mib)
		V2	IF-MIB (IF-MIB.mib)
authenticationFailure		V1	RFC-1215 (Rfc-1215.mib)
		V2	SNMPv2-MIB (SNMPv2-MIB.mib)
newRoot		V2	BRIDGE-MIB (BRIDGE-MIB.mib)
topologyChange		V2	BRIDGE-MIB (BRIDGE-MIB.mib)
risingAlarm	1: alarmIndex	V2	RMON-MIB (RMON-MIB.mib)
	2: alarmVariable		
	3: alarmSampleType		
	4: alarmValue		
	5: alarmRisingThreshold		
fallingAlarm	1: alarmIndex	V2	RMON-MIB (RMON-MIB.mib)
	2: alarmVariable		
	3: alarmSampleType		
	4: alarmValue		
	5: alarmFallingThreshold		
lldpRemTablesChange	1: lldpStatsRemTablesInserts	V2	LLDP-MIB (LLDP-MIB.mib)
	2: lldpStatsRemTablesDeletes		
	3: lldpStatsRemTablesDrops		
	4: lldpStatsRemTablesAgeouts		
lldpXMedTopologyChangeDetected	1: lldpRemChassisIdSubtype	V2	LLDP-EXT-MED-MIB (LLDP-EXT-MED.mib)
	2: lldpRemChassisId		
	3: lldpXMedRemDeviceClass		
dot1agCfmFaultAlarm	dot1agCfmMepHighestPrDefect	V2	IEEE8021-CFM-MIB (IEEE8021-CFM-MIB.mib)
dot3OamNonThresholdEvent	1: dot3OamEventLogTimestamp	V2	DOT3-OAM-MIB (DOT3-OAM-MIB.mib)
	2: dot3OamEventLogOui		
	3: dot3OamEventLogType		
	4: dot3OamEventLogLocation		
	5: dot3OamEventLogEventTotal		
dot3OamThresholdEvent	1: dot3OamEventLogTimestamp	V2	DOT3-OAM-MIB (DOT3-OAM-MIB.mib)
	2: dot3OamEventLogOui		

Trap Name	Variable Bind	Format	MIB Name
	3: dot3OamEventLogType		
	4: dot3OamEventLogLocation		
	5: dot3OamEventLogWindowHi		
	6: dot3OamEventLogWindowLo		
	7: dot3OamEventLogThresholdHi		
	8: dot3OamEventLogThresholdLo		
	9: dot3OamEventLogValue		
	10: dot3OamEventLogRunningTotal		
	11: dot3OamEventLogEventTotal		
swPowerFailure	1: swPowerUnitIndex	V2	EQUIPMENT-MIB (Equipment.mib)
	2: swPowerID		
	3: swPowerStatus		
swPowerRecover	1: swPowerUnitIndex	V2	EQUIPMENT-MIB (Equipment.mib)
	2: swPowerID		
	3: swPowerStatus		
swFanFailure	1: swFanUnitIndex	V2	EQUIPMENT-MIB (Equipment.mib)
	2: swFanID		
swFanRecover	1: swFanUnitIndex	V2	EQUIPMENT-MIB (Equipment.mib)
	2: swFanID		
swHighTemperature	1: swTemperatureUnitIndex	V2	EQUIPMENT-MIB (Equipment.mib)
	2: swTemperatureCurrent		
swHighTemperatureRecover	1: swTemperatureUnitIndex	V2	EQUIPMENT-MIB (Equipment.mib)
	2: swTemperatureCurrent		
swLowTemperature	1: swTemperatureUnitIndex	V2	EQUIPMENT-MIB (Equipment.mib)
	2: swTemperatureCurrent		
swLowTemperatureRecover	1: swTemperatureUnitIndex	V2	EQUIPMENT-MIB (Equipment.mib)
	2: swTemperatureCurrent		
swPktStormOccurred	swPktStormCtrlPortIndex	V2	PKT-STORM-CTRL-MIB (PktStormCtrl.mib)
swPktStormCleared	swPktStormCtrlPortIndex	V2	PKT-STORM-CTRL-MIB (PktStormCtrl.mib)
swSafeGuardChgToExhausted	swSafeGuardCurrentStatus	V2	SAFEGUARD-ENGINE-MIB (SafeGuard.mib)
swSafeGuardChgToNormal	swSafeGuardCurrentStatus	V2	SAFEGUARD-ENGINE-MIB (SafeGuard.mib)
swIpMacBindingViolationTrap	1: swIpMacBindingPortIndex	V2	IP-MAC-BIND-MIB (IPMacBind.mib)
	2: swIpMacBindingViolationIP		
	3: swIpMacBindingViolationMac		
swMacBasedAccessControlLoggedSuccess	1: swMacBasedAuthInfoMacIndex	V2	Mac-Based-Authentication-MIB (mba.mib)
	2: swMacBasedAuthInfoPortIndex		
	3: swMacBasedAuthVID		
swMacBasedAccessControlLoggedFail	1: swMacBasedAuthInfoMacIndex	V2	Mac-Based-Authentication-MIB (mba.mib)
	2: swMacBasedAuthInfoPortIndex		

Trap Name	Variable Bind	Format	MIB Name
	3: swMacBasedAuthVID		
swMacBasedAccessControlAgesOut	1: swMacBasedAuthInfoMacIndex	V2	Mac-Based-Authentication-MIB (mba.mib)
	2: swMacBasedAuthInfoPortIndex		
	3: swMacBasedAuthVID		
swFilterDetectedTrap	1: swFilterDetectedIP	V2	FILTER-MIB (Filter.mib)
	2: swFilterDetectedport		
swFilterDHCPv6ServerDetectedTrap	1: swFilterDetectedIPv6	V2	FILTER-MIB (Filter.mib)
	2: swFilterDetectedport		
swFilterICMPv6RaAllNodeDetectedTrap	1: swFilterDetectedIPv6	V2	FILTER-MIB (Filter.mib)
	2: swFilterDetectedport		
swPortLoopOccurred	swLoopDetectPortIndex	V2	LOOPBACK-DETECT-MIB (LBD.mib)
swPortLoopRestart	swLoopDetectPortIndex	V2	LOOPBACK-DETECT-MIB (LBD.mib)
swVlanLoopOccurred	swLoopDetectPortIndex	V2	LOOPBACK-DETECT-MIB (LBD.mib)
swVlanLoopRestart	1: swLoopDetectPortIndex	V2	LOOPBACK-DETECT-MIB (LBD.mib)
	2: swVlanLoopDetectVID		
swDdmAlarmTrap	1: swDdmPort	V2	DDM-MGMT-MIB (DDM.mib)
	2: swDdmThresholdType		
	3: swDdmThresholdExceedType		
swDdmWarningTrap	1: swDdmPort	V2	DDM-MGMT-MIB (DDM.mib)
	2: swDdmThresholdType		
	3: swDdmThresholdExceedType		
swBpduProtectionUnderAttackingTrap	1: swBpduProtectionPortIndex	V2	BPDU-PROTECTION-MIB (BPDUProtection.mib)
	2: swBpduProtectionPortMode		
swBpduProtectionRecoveryTrap	1: swBpduProtectionPortIndex	V2	BPDU-PROTECTION-MIB (BPDUProtection.mib)
	2: swBpduProtectionRecoveryMethod		
swERPSSFDetectedTrap	swERPSNodeId	V2	ERPS-MIB (erps.mib)
swERPSSFClearedTrap	swERPSNodeId	V2	ERPS-MIB (erps.mib)
swERPSRPLOwnerConflictTrap	swERPSNodeId	V2	ERPS-MIB (erps.mib)
swERPSMSDectectedTrap	swERPSNodeId	V2	ERPS-MIB (erps.mib)
swERPSFSDectectedTrap	swERPSNodeId	V2	ERPS-MIB (erps.mib)
swERPSClearDectectedTrap	swERPSNodeId	V2	ERPS-MIB (erps.mib)
agentCfgOperCompleteTrap	1: unitID	V2	AGENT-GENERAL-MIB (Genmgmt.mib)
	2: agentCfgOperate		
	3: agentLoginUserName		
agentFirmwareUpgrade	swMultiImageVersion	V2	AGENT-GENERAL-MIB (Genmgmt.mib)
agentGratuitousARPTrap	1: agentGratuitousARPIpAddr	V2	AGENT-GENERAL-MIB (Genmgmt.mib)
	2: agentGratuitousARPMacAddr		
	3: agentGratuitousARPPortNumber		
	4: agentGratuitousARPInterfaceName		

Trap Name	Variable Bind	Format	MIB Name
swSingleIPMSLinkDown	1: swSingleIPMSID	V2	SINGLE-IP-MIB (SingleIP.mib)
	2: swSingleIPMSMacAddr		
	3: ifIndex		
swSingleIPMSLinkUp	1: swSingleIPMSID	V2	SINGLE-IP-MIB (SingleIP.mib)
	2: swSingleIPMSMacAddr		
	3: ifIndex		
swSingleIPMSAuthFail	1: swSingleIPMSID	V2	SINGLE-IP-MIB (SingleIP.mib)
	2: swSingleIPMSMacAddr		
swSingleIPMSnewRoot	1: swSingleIPMSID	V2	SINGLE-IP-MIB (SingleIP.mib)
	2: swSingleIPMSMacAddr		
swSingleIPMSTopologyChange	1: swSingleIPMSID	V2	SINGLE-IP-MIB (SingleIP.mib)
	2: swSingleIPMSMacAddr		
swDoSAttackDetected	1: swDoSCtrlType	V2	DOS-PREV-MI (DOSPrev.mib)
	2: swDoSNotifyVarIpAddr		
	3: swDoSNotifyVarPortNumber		
swL2macNotification	swL2macNotifyInfo	V2	DGS3000-XXX-L2MGMT-MIB (L2mgmtDGS3000-XXX.mib)
swL2PortSecurityViolationTrap	1: swL2PortSecurityPortIndex,	V2	DGS3000-XXX-L2MGMT-MIB (L2mgmtDGS3000-XXX.mib)
	2: swL2PortSecurityViolationMac		
swWACLoggedSuccess	1: swWACAuthStatePort	V2	WebBase-Access-Control-MIB (wac.mib)
	2: swWACAuthStateOriginalVid		
	3: swWACAuthStateMACAddr		
	4: swWACAuthUserName		
	5: swWACClientAddrType		
	6: swWACClientAddress		
swWACLoggedFail	1: swWACAuthStatePort	V2	WebBase-Access-Control-MIB (wac.mib)
	2: swWACAuthStateOriginalVid		
	3: swWACAuthStateMACAddr		
	4: swWACAuthUserName		
	5: swWACClientAddrType		
	6: swWACClientAddress		
swCFMExtAISOccurred	1: dot1agCfmMdIndex	V2	CFMEXTENSION-MIB (CFMExtension.MIB)
	2: dot1agCfmMaIndex		
	3: dot1agCfmMepIdentifier		
swCFMExtAISCleared	1: dot1agCfmMdIndex	V2	CFMEXTENSION-MIB (CFMExtension.MIB)
	2: dot1agCfmMaIndex		
	3: dot1agCfmMepIdentifier		
swCFMExtLockOccurred	1: dot1agCfmMdIndex	V2	CFMEXTENSION-MIB (CFMExtension.MIB)
	2: dot1agCfmMaIndex		
	3: dot1agCfmMepIdentifier		
swCFMExtLockCleared	1: dot1agCfmMdIndex	V2	CFMEXTENSION-MIB (CFMExtension.MIB)
	2: dot1agCfmMaIndex		

Trap Name	Variable Bind	Format	MIB Name
	3: dot1agCfmMepIdentifier		
swPoEPortPdAliveFailOccurNotification	1: swPoEPortCtrlPortIndex	V2	PoE-MIB (PoE.mib)
	2: swPoEPortPdAliveCtrlPdIpType		
	3: swPoEPortPdAliveCtrlPdIpAddr		
ntpEntNotifModeChange	1: ntpEntStatusCurrentMode	V2	NTPv4-MIB (Ntpv4.mib)
ntpEntNotifStratumChange	1: ntpEntStatusDateTime	V2	NTPv4-MIB (Ntpv4.mib)
	2: ntpEntStatusStratum		
	3: ntpEntNotifMessage		
ntpEntNotifSyspeerChanged	1: ntpEntStatusDateTime	V2	NTPv4-MIB (Ntpv4.mib)
	2: ntpEntStatusActiveRefSourceId		
	3: ntpEntNotifMessage		
ntpEntNotifAddAssociation	1: ntpEntStatusDateTime	V2	NTPv4-MIB (Ntpv4.mib)
	2: ntpAssocName		
	3: ntpEntNotifMessage		
ntpEntNotifRemoveAssociation	1: ntpEntStatusDateTime	V2	NTPv4-MIB (Ntpv4.mib)
	2: ntpAssocName		
	3: ntpEntNotifMessage		
ntpEntNotifConfigChanged	1: ntpEntStatusDateTime	V2	NTPv4-MIB (Ntpv4.mib)
	2: ntpEntNotifMessage		
ntpEntNotifLeapSecondAnnounced	1: ntpEntStatusDateTime	V2	NTPv4-MIB (Ntpv4.mib)
	2: ntpEntNotifMessage		
ntpEntNotifHeartbeat	1: ntpEntStatusDateTime	V2	NTPv4-MIB (Ntpv4.mib)
	2: ntpEntStatusCurrentMode		
	3: ntpEntHeartbeatInterval		
	4: ntpEntNotifMessage		
swAutoBackupSuccessTrap	swAutoBackupPathTftpFileName	V2	AUTOBACKUP-MIB (AutoBackup.mib)
swAutoBackupFailTrap	swAutoBackupPathTftpFileName	V2	AUTOBACKUP-MIB (AutoBackup.mib)
swResetButtonPressedTrap	swResetButtonMode	V2	ZTP-MIB (ZTP.mib)

Appendix D RADIUS Attributes Assignment

The RADIUS Attributes Assignment on the DGS-3000 series is used in the following modules: 802.1X (Port-based and Host-based), and MAC-based Access Control.

The description that follows explains the following RADIUS Attributes Assignment types:

- Ingress/Egress Bandwidth
- 802.1p Default Priority
- VLAN
- ACL

To assign **Ingress/Egress bandwidth by RADIUS Server**, the proper parameters should be configured on the RADIUS Server. The tables below show the parameters for bandwidth.

The parameters of the Vendor-Specific attributes are:

Vendor-Specific Attribute	Description	Value	Usage
Vendor-ID	Defines the vendor.	171 (DLINK)	Required
Vendor-Type	Defines the attribute.	2 (for ingress bandwidth) 3 (for egress bandwidth)	Required
Attribute-Specific Field	Used to assign the bandwidth of a port.	Unit (Kbits)	Required

If the user has configured the bandwidth attribute of the RADIUS server (for example, ingress bandwidth 1000Kbps) and the 802.1X authentication is successful, the device will assign the bandwidth (according to the RADIUS server) to the port. However, if the user does not configure the bandwidth attribute and authenticates successfully, the device will not assign any bandwidth to the port. If the bandwidth attribute is configured on the RADIUS server with a value of “0” or more, than the effective bandwidth (100Mbps on an Ethernet port or 1Gbps on a Gigabit port) of the port will be set to *no_limited*.

To assign **802.1p default priority by RADIUS Server**, the proper parameters should be configured on the RADIUS Server. The tables below show the parameters for 802.1p default priority.

The parameters of the Vendor-Specific attributes are:

Vendor-Specific Attribute	Description	Value	Usage
Vendor-ID	Defines the vendor.	171 (DLINK)	Required
Vendor-Type	Defines the attribute.	4	Required
Attribute-Specific Field	Used to assign the 802.1p default priority of the port.	0-7	Required

If the user has configured the 802.1p priority attribute of the RADIUS server (for example, priority 7) and the 802.1X, or MAC-based authentication is successful, the device will assign the 802.1p default priority (according to the RADIUS server) to the port. However, if the user does not configure the priority attribute and authenticates successfully, the device will not assign a priority to this port. If the priority attribute is configured on the RADIUS server is a value out of range (>7), it will not be set to the device.

To assign **VLAN by RADIUS Server**, the proper parameters should be configured on the RADIUS Server. To use VLAN assignment, RFC3580 defines the following tunnel attributes in RADIUS packets.

The table below shows the parameters for a VLAN:

RADIUS Tunnel Attribute	Description	Value	Usage
Tunnel-Type	This attribute indicates the tunneling protocol(s) to be used (in the case of a tunnel initiator) or the tunneling protocol in use (in the case of a tunnel terminator).	13 (VLAN)	Required
Tunnel-Medium-Type	This attribute indicates the transport medium being used.	6 (802)	Required
Tunnel-Private-Group-ID	This attribute indicates group ID for a particular tunneled session.	A string (VID)	Required

If the user has configured the VLAN attribute of the RADIUS server (for example, VID 3) and the 802.1X, or MAC-based Access Control authentication is successful, the port will be added to VLAN 3. However, if the user does not configure the VLAN attribute and authenticates successfully, the port will be kept in its original VLAN. If the VLAN attribute configured on the RADIUS server does not exist, the port will not be assigned to the requested VLAN.

To assign **ACL by RADIUS Server**, the proper parameters should be configured on the RADIUS Server. The table below shows the parameters for an ACL. The RADIUS ACL assignment is only used in MAC-based Access Control.

The parameters of the Vendor-Specific Attribute are:

RADIUS Tunnel Attribute	Description	Value	Usage
Vendor-ID	Defines the vendor.	171 (DLINK)	Required
Vendor-Type	Defines the attribute.	12 (for ACL profile) 13 (for ACL rule)	Required
Attribute-Specific Field	Used to assign the ACL profile or rule.	ACL Command For example: ACL profile: **create access_profile profile_id 1 profile_name profile1 ethernet vlan 0xFFF**; ACL rule: **config access_profile profile_id 1 add access_id auto_assign ethernet vlan_id 1 port all deny**;	Required

If the user has configured the ACL attribute of the RADIUS server (for example, ACL profile: **create access_profile profile_id 1 profile_name profile1 ethernet vlan 0xFFF**; ACL rule: **config access_profile profile_id 1 add access_id auto_assign ethernet vlan_id 1 port all deny**), and the MAC-based Access Control authentication is successful, the device will assign the ACL profiles and rules according to the RADIUS server. For more information about the ACL module, please refer to **Chapter 6 Access Control List (ACL) Command List**.

Appendix E IETF RADIUS Attributes Support

Remote Authentication Dial-In User Service (RADIUS) attributes carry specific authentication, authorization, and configuration details for the request and reply. This appendix lists the RADIUS attributes currently supported by the Switch.

RADIUS attributes are supported by the IETF standard and Vendor-Specific Attribute (VSA). VSA allows the vendor to create an additionally owned RADIUS attribute. For more information about D-Link VSA, refer to **Appendix D RADIUS Attributes Assignment**.

IETF standard RADIUS attributes are defined in the RFC 2865 Remote Authentication Dial-In User Service (RADIUS), RFC 2866 RADIUS Accounting, RFC 2868 RADIUS Attributes for Tunnel Protocol Support, and RFC 2869 RADIUS Extensions.

The following table lists the IETF RADIUS attributes supported by the D-Link switch.

1. RADIUS Authentication Attributes

Number	IETF Attribute
1	User-Name
2	User-Password
3	CHAP-Password
4	NAS-IP-Address
5	NAS-Port
6	Service-Type
7	Framed-Protocol
8	Framed-IP-Address
12	Framed-MTU
18	Reply-Message
24	State
26	Vendor-Specific
27	Session-Timeout
29	Termination-Action
30	Called-Station-ID
31	Calling-Station-ID
32	NAS-Identifier
60	CHAP-Challenge
61	NAS-Port-Type
64	Tunnel-Type
65	Tunnel-Medium-Type
77	Connect-Info
79	EAP-Message
80	Message-Authenticator
81	Tunnel-Private-Group-ID

85	Acct-Interim-Interval
87	NAS-Port-ID
95	NAS-IPv6-Address

2. RADIUS Accounting Attributes

Number	IETF Attribute
1	User-Name
4	NAS-IP-Address
5	NAS-Port
6	Service-Type
8	Framed-IP-Address
31	Calling-Station-ID
32	NAS-Identifier
40	Acct-Status-Type
41	Acct-Delay-Time
42	Acct-Input-Octets
43	Acct-Output-Octets
44	Acct-Session-ID
45	Acct-Authentic
46	Acct-Session-Time
47	Acct-Input-Packets
48	Acct-Output-Packets
49	Acct-Terminate-Cause
52	Acct-Input-Gigawords
53	Acct-Output-Gigawords
61	NAS-Port-Type
95	NAS-IPv6-Address

Appendix F ERPS Information

The following switch ports support the ERPS Fast Link Drop Interrupt feature with a recovery time of less than 50 ms:

Model Name	Port 1 to 8
DGS-3000-28L DGS-3000-28LP DGS-3000-28X DGS-3000-28XMP	V

Model Name	Port 1 to 8	Port 25 to 32
DGS-3000-52L DGS-3000-52X (HW: B1)	V	V

Model Name	Port 17 to 24	Port 41 to 48
DGS-3000-52X (HW: B2)	V	V