



CLI Reference Guide

Product Model: DGS-3000 Series
Layer 2 Managed Gigabit Switch
Release 1.00



Table of Contents

| | | |
|------------|--|-----|
| Chapter 1 | Using Command Line Interface..... | 1 |
| Chapter 2 | Basic Command List | 8 |
| Chapter 3 | 802.1Q VLAN Command List..... | 22 |
| Chapter 4 | 802.1X Command List..... | 37 |
| Chapter 5 | Access Authentication Control Command List..... | 55 |
| Chapter 6 | Access Control List (ACL) Command List..... | 82 |
| Chapter 7 | Address Resolution Protocol (ARP) Command List..... | 103 |
| Chapter 8 | ARP Spoofing Prevention Command List | 108 |
| Chapter 9 | Auto-Configuration Command List..... | 110 |
| Chapter 10 | Basic Commands Command List..... | 113 |
| Chapter 11 | BPDU Attack Protection Command List..... | 129 |
| Chapter 12 | Cable Diagnostics Command List..... | 134 |
| Chapter 13 | Command Logging Command List..... | 137 |
| Chapter 14 | Compound Authentication Command List | 139 |
| Chapter 15 | Configuration Command List..... | 143 |
| Chapter 16 | Connectivity Fault Management (CFM) Command List..... | 148 |
| Chapter 17 | CPU Interface Filtering Command List | 175 |
| Chapter 18 | Debug Software Command List | 184 |
| Chapter 19 | DHCP Local Relay Command List..... | 191 |
| Chapter 20 | DHCP Relay Command List..... | 197 |
| Chapter 21 | DHCP Server Screening Command List..... | 215 |
| Chapter 22 | Digital Diagnostic Monitoring (DDM) Commands | 218 |
| Chapter 23 | D-Link Unidirectional Link Detection (DULD) Command List | 223 |
| Chapter 24 | Domain Name System (DNS) Resolver Command List..... | 225 |
| Chapter 25 | DoS Attack Prevention Command List..... | 231 |
| Chapter 26 | Energy Efficient Ethernet (EEE) Commands | 235 |
| Chapter 27 | Ethernet Ring Protection Switching (ERPS) Command List..... | 237 |
| Chapter 28 | External Alarm Command List | 246 |
| Chapter 29 | Filter Command List | 248 |
| Chapter 30 | Filter Database (FDB) Command List..... | 251 |
| Chapter 31 | Flash File System (FFS) Command List..... | 261 |
| Chapter 32 | Gratuitous ARP Command List..... | 270 |
| Chapter 33 | IGMP Snooping Command List..... | 276 |
| Chapter 34 | IP-MAC-Port Binding (IMPB) Command List | 302 |

| | | |
|------------|--|-----|
| Chapter 35 | IPv6 Neighbor Discover Command List | 325 |
| Chapter 36 | IPv6 Route Command List | 329 |
| Chapter 37 | Japanese Web-Based Access Control (JWAC) Command List | 332 |
| Chapter 38 | Jumbo Frame Command List..... | 355 |
| Chapter 39 | Layer 2 Protocol Tunneling (L2PT) Command List..... | 357 |
| Chapter 40 | Link Aggregation Command List | 361 |
| Chapter 41 | Link Layer Discovery Protocol (LLDP) Command List..... | 368 |
| Chapter 42 | Loop Back Detection (LBD) Command List | 393 |
| Chapter 43 | MAC Notification Command List | 399 |
| Chapter 44 | MAC-based Access Control Command List..... | 404 |
| Chapter 45 | MAC-based VLAN Command List..... | 420 |
| Chapter 46 | Mirror Command List..... | 423 |
| Chapter 47 | MLD Snooping Command List | 426 |
| Chapter 48 | MSTP debug enhancement Command List | 449 |
| Chapter 49 | Multicast Filter Command List..... | 455 |
| Chapter 50 | Multicast VLAN Command List | 468 |
| Chapter 51 | Multiple Spanning Tree Protocol (MSTP) Command List | 479 |
| Chapter 52 | Network Load Balancing (NLB) Command List | 492 |
| Chapter 53 | Network Monitoring Command List..... | 497 |
| Chapter 54 | OAM Commands..... | 504 |
| Chapter 55 | Peripherals Command List..... | 512 |
| Chapter 56 | Ping Command List..... | 515 |
| Chapter 57 | Port Security Command List | 518 |
| Chapter 58 | Power Saving Command List..... | 526 |
| Chapter 59 | PPPoE Circuit ID Insertions Command List..... | 533 |
| Chapter 60 | Protocol VLAN Command List | 537 |
| Chapter 61 | QinQ Command List..... | 543 |
| Chapter 62 | Quality of Service (QoS) Command List | 551 |
| Chapter 63 | RADIUS Client Command List | 568 |
| Chapter 64 | Safeguard Engine Command List | 574 |
| Chapter 65 | Secure Shell (SSH) Command List..... | 576 |
| Chapter 66 | Secure Sockets Layer (SSL) Command List | 585 |
| Chapter 67 | Show Technical Support Command List..... | 591 |
| Chapter 68 | Simple Mail Transfer Protocol (SMTP) Command List | 594 |
| Chapter 69 | Simple Network Management Protocol (SNMP) Command List | 599 |
| Chapter 70 | Single IP Management Command List | 625 |

| | | |
|------------|---|-----|
| Chapter 71 | Syslog and Trap Source-interface Command List | 635 |
| Chapter 72 | System Log Command List | 639 |
| Chapter 73 | System Severity Command List | 650 |
| Chapter 74 | Telnet Client Command List | 652 |
| Chapter 75 | TFTP/FTP Client Command List | 653 |
| Chapter 76 | Time and SNTP Command List | 663 |
| Chapter 77 | Trace Route Command List | 670 |
| Chapter 78 | Traffic Control Command List | 673 |
| Chapter 79 | Traffic Segmentation Command List | 678 |
| Chapter 80 | Trusted Host Command List | 680 |
| Chapter 81 | Unicast Routing Command List | 684 |
| Chapter 82 | VLAN Trunking Command List | 687 |
| Chapter 83 | Voice VLAN Command List | 692 |
| Chapter 84 | Password Recovery Command List | 703 |
| Appendix A | Password Recovery Procedure | 705 |
| Appendix B | System Log Entries | 707 |
| Appendix C | Trap Log Entries | 718 |
| Appendix D | RADIUS Attributes Assignment | 725 |

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-3000-26TC Gigabit Ethernet Switch
Command Line Interface

Firmware: Build 1.00.015
Copyright(C) 2013 D-Link Corporation. All rights reserved.
UserName:
PassWord:

DGS-3000-26TC:admin#
```

There is no initial username or password. Just press the **Enter** key twice to display the CLI input cursor – **DGS-3000-26TC: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 V1.00.001
-----
Power On Self Test ..... 100 %

MAC Address : 00-01-02-03-04-00
H/W Version : A1

Please Wait, Loading V1.00.015 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-3000-26TC: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-3000-26TC: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 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 ethernet_oam ports
clear fdb
clear igmp_snooping data_driven_group
clear igmp_snooping statistics counter
clear jwac auth_state
clear log
clear mac_based_access_control auth_state
clear mld_snooping data_driven_group
clear mld_snooping statistics counter
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-3000-26TC:admin#config account
Command: config account
Next possible completions:
<username>

DGS-3000-26TC: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-3000-26TC:admin#config account
Command: config account
Next possible completions:
<username>

DGS-3000-26TC: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-3000-26TC:admin#the
Available commands:
..          ?          cable_diag      cd
cfm         clear          config          copy
create      debug          del             delete
dir         disable        download        enable
erase       login          logout          md
move        no             ping            ping6
rd          reboot         reconfig        rename
reset       save           show            smtp
telnet      traceroute    traceroute6     upload

DGS-3000-26TC: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-3000-26TC:admin#show
Command: show
Next possible completions:
802.1p          802.1x          aaa              access_profile
account         accounting      acct_client     address_binding
arp_spoofing_prevention  arpretry       attack_log
auth_client     auth_diagnostics  auth_session_statistics
auth_statistics  authen          authen_enable   authen_login
authen_policy   authentication    authorization    autoconfig
bandwidth_control  boot_file      bpdu_protection  cfm
command         command_history  config          control_pkt
cpu            cpu_filter      current_config   ddm
device_status    dhcp_local_relay  dhcp_relay      dos_prevention
dot1v_protocol_group  dscp          duld
environment      erps           error           ethernet_oam
external_alarm   fdb            filter          flow_meter
gratuitous_arp   greeting_message  gvrp           host_name
igmp            igmp_snooping   ipif
ipif_ipv6_link_local_auto  iproute        ipv6
ipv6route       jumbo_frame     jwac           l2protocol_tunnel
lacp_port       led            limited_multicast_addr
link_aggregation  lldp          lldp_med       log
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
packet          password_recovery  per_queue       port
port_security    port_security_entry  port_vlan
ports           power_saving     pppoe          private_vlan
pvid            qinq            radius          rmon
router_ports     safeguard_engine  scheduling
scheduling_mechanism  serial_port     session
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     utilization     vlan
vlan_translation  vlan_trunk      voice_vlan
DGS-3000-26TC: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

| Syntax | Description |
|--|---|
| angle brackets < > | <p>Encloses a variable or value. Users must specify the variable or value. For example, in the syntax</p> <pre>create ipif <ipif_name 12> {<network_address>} <vlan_name 32> {secondary state [enable disable] proxy_arp [enable disable] {local [enable disable]}}</pre> <p>users must supply an IP interface name for <ipif_name 12> ,a VLAN name for <vlan_name 32> and an address for <network_address> when entering the command. DO NOT TYPE THE ANGLE BRACKETS.</p> |
| square brackets [] | <p>Encloses a required value or list of required arguments. Only one value or argument must be specified. For example, in the syntax</p> <pre>create account [admin operator power_user user] <username 15> {encrypt [plain_text sha_1] <password>}</pre> <p>users must specify either the admin-level or user-level account when entering the command. DO NOT TYPE THE SQUARE BRACKETS.</p> |
| vertical bar | <p>Separates mutually exclusive items in a list, one of which must be entered. For example, in the syntax</p> <pre>create ipif <ipif_name 12> {<network_address>} <vlan_name 32> {secondary state [enable disable] proxy_arp [enable disable] {local [enable disable]}}</pre> <p>users must specify either the community or trap receiver in the command. DO NOT TYPE THE VERTICAL BAR.</p> |
| braces { } | <p>Encloses an optional value or a list of optional arguments. One or more values or arguments can be specified. For example, in the syntax</p> <pre>reset {[config system]} {force_agree}</pre> <p>users may choose configure or system in the command. DO NOT TYPE THE BRACES.</p> |
| parentheses () | <p>Indicates at least one or more of the values or arguments in the preceding syntax enclosed by braces must be specified. For example, in the syntax</p> <pre>config bpd protection ports [<portlist> all] {state [enable disable] mode [drop block shutdown]}(1)</pre> <p>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.</p> |
| ipif <ipif_name 12> metric <value 1-31> | <p>12 means the maximum length of the IP interface name.</p> <p>1-31 means the legal range of the metric value.</p> |

1-4 Line Editing Keys

| Keys | Description |
|-------------|---|
| Delete | Delete character under cursor and shift remainder of line to left. |
| Backspace | Delete character to left of cursor and shift remainder of line to left. |
| Insert | Toggle on and off. When toggled on, inserts text and shifts previous text to right. |
| Left Arrow | Move cursor to left. |
| Right Arrow | Move cursor to right |
| Tab | Help user to select appropriate token. |
| P | Display the previous page. |
| N or Space | Display the next page. |
| CTRL+C | Escape from displayed pages. |
| ESC | Escape from displayed pages. |
| Q | Escape from displayed pages. |
| R | refresh the displayed pages |
| a | Display the remaining pages. (The screen display will not pause again.) |
| Enter | Display the next line. |

The screen display pauses when the show command output reaches the end of the page.

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.

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]}} flow_control [enable disable] learning [enable disable] state [enable disable] mdix [auto normal cross] [description <desc 1-32> clear_description]} |
| show ports [<portlist>] {[description err_disabled details media_type]} |

2-1 show session

Description

This command is used to display a list of currently users which are login to the Switch.

Format

show session

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To display the session entries:

```
DGS-3000-26TC:admin#show session
Command: show session
```

| ID | Live Time | From | Level | Name |
|----|--------------|-------------|--------|--------|
| 0 | 00:01:46.360 | 10.90.90.10 | puuser | puuser |
| 8 | 00:05:49.340 | Serial Port | admin | admin |

Total Entries: 2

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-3000-26TC: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-3000-26TC: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 auto 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) 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) The auto logout time out setting.

never - Never timeout.

2_minutes - When idle over 2 minutes, the device will auto logout.

5_minutes - When idle over 5 minutes, the device will auto logout.

10_minutes - When idle over 10 minutes, the device will auto logout.

15_minutes - When idle over 15 minutes, the device will auto logout.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure baud rate:

```
DGS-3000-26TC:admin#config serial_port baud_rate 9600
Command: config serial_port baud_rate 9600

Success.

DGS-3000-26TC: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-3000-26TC:admin#enable clipaging
Command: enable clipaging

Success.

DGS-3000-26TC: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-3000-26TC:admin#disable clipaging
Command: disable clipaging

Success.

DGS-3000-26TC:admin#
```

2-6 login

Description

This command is used to allow user login to the Switch.

Format

login

Parameters

None.

Restrictions

None.

Example

To login the Switch with a user name dlink:

```
DGS-3000-26TC:admin#login
Command: login

UserName:dlink
PassWord:****

DGS-3000-26TC:admin#
```

2-7 logout

Description

This command is used to logout the facility.

Format

logout

Parameters

None.

Restrictions

None.

Example

To logout current user:


```
DGS-3000-26TC:admin#logout
Command: logout

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

                DGS-3000-26TC Gigabit Ethernet Switch
                Command Line Interface

                Firmware: Build 1.00.015
                Copyright(C) 2013 D-Link Corporation. All rights reserved.
UserName:
```

2-8 ?

Description

This command is used to display the usage description for all commands or the specific one.

Format

?

Parameters

None.

Restrictions

None.

Example

To get "ping" command usage, descriptions:

```
DGS-3000-26TC:admin#? ping
Command: ? ping

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

DGS-3000-26TC:admin#
```

2-9 clear

Description

The command is used to clear screen.

Format

clear

Parameters

None.

Restrictions

None.

Example

To clear screen:

```
DGS-3000-26TC:admin#clear
Command: clear

DGS-3000-26TC:admin#
```

2-10 show command_history

Description

The command is used to display command history.

Format

show command_history

Parameters

None.

Restrictions

None.

Example

To display command history:

```
DGS-3000-26TC: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-3000-26TC: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” upto 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-3000-26TC:admin#config command_history 25
Command: config command_history 25

Success.

DGS-3000-26TC: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) Adds this parameter to the **config greeting_message** command will 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-3000-26TC:admin#config greeting_message
Command: config greeting_message

Greeting Messages Editor
=====

                DGS-3000-26TC Gigabit Ethernet Switch
                Command Line Interface

                Firmware: Build 1.00.015
                Copyright(C) 2013 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**

The command is used to display greeting message.

Format**show greeting_message****Parameters**

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To display greeting message:

```
DGS-3000-26TC:admin#show greeting_message
Command: show greeting_message

=====

                DGS-3000-26TC Gigabit Ethernet Switch
                Command Line Interface

                Firmware: Build 1.00.015
                Copyright(C) 2013 D-Link Corporation. All rights reserved.

=====

DGS-3000-26TC: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-3000-26TC: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 users’ login user name.

When users issue the “reset” command, the current command prompt will remain in tact. Yet, issuing the “reset system” will return the command prompt 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** - Enter this command to set the login username as the command prompt.
 - default** - Enter this command 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-3000-26TC:admin#config command_prompt Prompt#
Command: config command_prompt Prompt#

Success.

Prompt#:admin#
```

2-15 config terminal width

Description

The command is used to set current terminal width.

The usage is described as below:

1. Users login and configure the terminal width to 120, this configuration take effect on this login section. If users implement “save” command, the configuration is saved. After users log out and log in again, the terminal width is 120.
2. If user did not save the configuration, another user login, the terminal width is default value.
3. If at the same time, two CLI sessions are running, once section configure to 120 width and save it, the other section will not be effected, unless it log out and then log in.

Format

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

Parameters

default - The default setting of terminal width. The default value is 80.

<value 80-200> - The terminal width which will be configured. The width is between 80 and 200 characters.

Restrictions

None.

Example

To configure the current terminal width:

```
DGS-3000-26TC:admin#config terminal width 120
Command: config terminal width 120

Success.

DGS-3000-26TC:admin#
```

2-16 show terminal width

Description

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

Format

show terminal width

Parameters

None.

Restrictions

None.

Example

To display the configuration of current terminal width:

```
DGS-3000-26TC:admin#show terminal width
Command: show terminal width

Global terminal width      : 80
Current terminal width    : 80

DGS-3000-26TC:admin#
```

2-17 config ports

Description

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

Format

config ports [**<portlist>** | **all**] {**medium_type** [**fiber** | **copper**]} {**speed** [**auto** | **10_half** | **10_full** | **100_half** | **100_full** | **1000_full** {[**master** | **slave**]}] | **flow_control** [**enable** | **disable**] | **learning** [**enable** | **disable**] | **state** [**enable** | **disable**] | **mdix** [**auto** | **normal** | **cross**] | [**description** **<desc 1-32>** | **clear_description**]}

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 the medium type while the configure ports are combo ports
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 - Sets port speed to auto negotiation.
10_half - Sets port speed to 10_half.

10_full - Sets port speed to 10_full.

100_half - Sets port speed to 100_half.

100_full - Sets port speed to 100_full.

1000_full - Sets port speed to 1000_full. While set port speed to 1000_full, user should specify master or slave mode for 1000BASE-T interface, and leave the 1000_full without any master or slave setting for other interface.

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

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

flow_control - (Optional) Turns on or turns off the flow control on one or more ports by enabling or disabling this function.

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

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

learning - (Optional) Turns on or turns off the 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) Enables or disables the specified port. If the specified ports are in error-disabled status, configure 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) The MDIX mode can be specified as auto, normal, and cross. If set to the normal state, the port is in the MDIX mode and can be connected to PC NIC using a straight cable. If set to the 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.

auto - Specifies that the MDIX mode for the port will be set to auto.

normal - Specifies that the MDIX mode for the port will be set to normal.

cross - Specifies that the MDIX mode for the port will be set to cross.

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

<desc 1-32> - Enter the port interface description. This value can be up to 32 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-3000-26TC:admin#config ports all medium_type copper speed auto
Command: config ports all medium_type copper speed auto

Success.

DGS-3000-26TC:admin#
```

2-18 show ports

Description

This command is used to display the current configurations of a range of 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 list of ports to be configured.

description - (Optional) Indicates if the port description will be included in the display.

err_disabled - (Optional) Displays ports that were disabled because of an error condition.

details - (Optional) Displays the port details.

media_type - (Optional) Displays the port transceiver type.

Restrictions

None.

Example

To display the port details:

```
DGS-3000-26TC:admin#show ports details
Command: show ports details

Port : 1
-----
Port Status           : Link Up
Description           :
HardWare Type         : Fast Ethernet
MAC Address           : 00-01-02-03-04-01
Bandwidth              : 100000Kbit
Auto-Negotiation      : Enabled
Duplex Mode           : Full Duplex
Flow Control          : Disabled
MDI                   : Normal
Address Learning       : Enabled
Last Clear of Counter : 2 hours 43 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
```

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 for 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 - Creates the VLAN ID. |
| <vlanid 2-4094> - Enter the VLAN ID. The VLAN ID value must be between 2 and 4094. |
| type - (Optional) Specifies the type of VLAN here. |
| 1q_vlan - (Optional) Specifies that the type of VLAN used is based on the 802.1Q standard. |
| private_vlan - (Optional) Specifies that the private VLAN type will be used. |
| advertisement - (Optional) Specifies the VLAN as being able to be advertised out. |

Restrictions

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

Example

To create a VLAN with name "p1" and VLAN ID 2:

```
DGS-3000-26TC:admin#create vlan p1 tag 2 type private_vlan advertisement
Command: create vlan p1 tag 2 type private_vlan advertisement

Success.

DGS-3000-26TC:admin#
```

3-2 create vlan vlanid

Description

This command is used to create more than one VLANs at a time. A unique VLAN name (e.g. VLAN10) will be automatically assigned by the system. The automatic assignment of 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 conflict 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 - (Optional) Specifies that the VLAN created will be a 1Q VLAN.

private_vlan - (Optional) Specifies that the private VLAN type will be used.

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

Restrictions

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

Example

To create some VLANs using VLAN ID:

```
DGS-3000-26TC:admin#create vlan vlanid 10-30
Command: create vlan vlanid 10-30

Success.

DGS-3000-26TC:admin#
```

3-3 delete vlan

Description

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

Format

delete vlan <vlan_name 32>

Parameters

vlan - The VLAN name of the VLAN to be deleted.

<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 remove a vlan v1:

```
DGS-3000-26TC:admin#delete vlan v1
Command: delete vlan v1

Success.

DGS-3000-26TC:admin#
```

3-4 delete vlan vlanid

Description

This command is used to delete one or a number of previously configured VLAN by VID list.

Format

delete vlan vlanid <vidlist>

Parameters

vlanid - The VLAN ID list to be deleted.

<vidlist> - Enter the VLAN ID list here.

Restrictions

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

Example

To remove VLANs from 10-30:

```
DGS-3000-26TC:admin#delete vlan vlanid 10-30
Command: delete vlan vlanid 10-30

Success.

DGS-3000-26TC: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 you want to add ports to. This name can be up to 32 characters long.

add - (Optional) 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 - (Optional) Specifies to delete ports from the VLAN.

<portlist> - (Optional) Enter the list of ports used for the configuration here.

advertisement - (Optional) Specifies the 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 4 through 8 as tagged ports to the VLAN v2:

```
DGS-3000-26TC:admin#config vlan v2 add tagged 4-8
Command: config vlan v2 add tagged 4-8

Success.

DGS-3000-26TC:admin#
```

3-6 config vlan vlanid

Description

This command allows you to configure multiple VLANs at one time. But conflicts will be generated if you configure the name of multiple VLANs at one 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 - (Optional) 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 - (Optional) Specifies to delete ports from the VLAN.

<portlist> - (Optional) Enter the list of ports used for the configuration here.

advertisement - (Optional) Specifies the GVRP state of this VLAN.

enable - Specifies to enable advertisement for this VLAN.

disable - Specifies to disable advertisement for this VLAN.

name - (Optional) 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 4 through 8 as tagged ports to the VLAN ID from 10-20:

```
DGS-3000-26TC:admin#config vlan vlanid 10-20 add tagged 4-8
```

```
Command: config vlan vlanid 10-20 add tagged 4-8
```

```
Success.
```

```
DGS-3000-26TC: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> - 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) are specified. The beginning and end of the

port list range are separated by a dash.

all - Specifies all ports for ingress checking.

gvrp_state - (Optional) Enables or disables the 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 - (Optional) Enables or disables ingress checking for the specified portlist.

- enable** - Specifies that ingress checking will be enabled for the specified portlist.
- disable** - Specifies that ingress checking will be disabled for the specified portlist.

acceptable_frame - (Optional) The type of frame will be accepted by the port. There are two types:

- tagged_only** - Only tagged packets can be accepted by this port.
- admit_all** - All packets can be accepted.

pvid - (Optional) Specifies the 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 sets the ingress checking status, the sending and receiving GVRP information:

```
DGS-3000-26TC:admin#config port_vlan 1-5 gvrp_state enable ingress_checking
enabl
e acceptable_frame tagged_only pvid 2
Command: config port_vlan 1-5 gvrp_state enable ingress_checking enable acceptab
le_frame tagged_only pvid 2

Success.

DGS-3000-26TC:admin#
```

3-8 show vlan

Description

This command is used to display the vlan information including of parameters setting and operational value.

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-3000-26TC:admin#show vlan
Command: show vlan

VLAN Trunk State      : Disabled
VLAN Trunk Member Ports :

VID      : 1          VLAN Name      : default
VLAN Type : Static    Advertisement : Enabled
Member Ports : 1-26
Static Ports : 1-26
Current Tagged Ports :
Current Untagged Ports: 1-26
Static Tagged Ports :
Static Untagged Ports : 1-26
Forbidden Ports      :

Total Static VLAN Entries: 1
Total GVRP VLAN Entries: 0

DGS-3000-26TC:admin#
```

3-9 show vlan ports

Description

This command is used to display the vlan information per ports.

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-3000-26TC:admin#show vlan ports 6
Command: show vlan ports 6

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

DGS-3000-26TC: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-3000-26TC:admin#show vlan vlanid 1
Command: show vlan vlanid 1

VID           : 1                VLAN Name      : default
VLAN Type     : Static           Advertisement  : Enabled
Member Ports  : 1-26
Static Ports  : 1-26
Current Tagged Ports :
Current Untagged Ports: 1-26
Static Tagged Ports  :
Static Untagged Ports : 1-26
Forbidden Ports      :

Total Entries : 1

DGS-3000-26TC:admin#
```

3-11 show port_vlan

Description

This command is used to display the ports' VLAN attributes on the Switch.

Format

show port_vlan {<portlist>}

Parameters

<portlist> - (Optional) Specifies a range of ports to be displayed.
 If no parameter specified, system will display all ports gvrp information.

Restrictions

None.

Example

To display 802.1Q port setting:

```
DGS-3000-26TC: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  c  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 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 last item of VLAN list. When 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 the auto-assign PVID:

```
DGS-3000-26TC:admin#enable pvid auto_assign
Command: enable pvid auto_assign

Success.

DGS-3000-26TC: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-3000-26TC:admin#disable pvid auto_assign
Command: disable pvid auto_assign

Success.

DGS-3000-26TC: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-3000-26TC:admin#show pvid auto_assign
Command: show pvid auto_assign

PVID Auto-assignment: Enabled

DGS-3000-26TC:admin#
```

3-15 config gvrp

Description

The config gvrp timer command set the GVRP timer's value. The default value for Join time is 200 milliseconds; for Leave time is 600 milliseconds; for LeaveAll time is 10000 milliseconds.

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 the Join time will be set.

<value 100-100000> - Enter the time used here. This value must be between 100 and 100000.

leave - (Optional) Specifies the Leave time will be set.

<value 100-100000> - Enter the time used here. This value must be between 100 and 100000.

leaveall - (Optional) Specifies the LeaveAll time will be set.

<value 100-100000> - Enter the time used here. This value must be between 100 and 100000.

nni_bpdu_addr - Determines the BPDU protocol address for GVRP in service provide 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-3000-26TC:admin#config gvrp timer join 200
Command: config gvrp timer join 200

Success.

DGS-3000-26TC: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-3000-26TC: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-3000-26TC:admin#
```

3-17 enable gvrp

Description

This commands 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-3000-26TC:admin#enable gvrp
Command: enable gvrp

Success.

DGS-3000-26TC: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-3000-26TC:admin#disable gvrp
Command: disable gvrp

Success.

DGS-3000-26TC:admin#
```

3-19 config private_vlan**Description**

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

Format

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

Parameters

<vlan_name 32> - Specifies the name of the private VLAN.

vid - Specifies the VLAN ID of the private VLAN.

<vlanid 2-4094> - Enter the VLAN ID used here. 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 isolated VLAN.

community - Specifies the secondary VLAN as community VLAN.

remove - Specifies that a secondary VLAN will be removed from the private VLAN.

<vlan_name 32> - Specifies the secondary VLAN name used. This name can be up to 32 characters long.

vlanid - A range of secondary VLAN 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-3000-26TC:admin#config private_vlan p1 add community vlanid 3
Command: config private_vlan p1 add community vlanid 3

Success.

DGS-3000-26TC: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) Specifies 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 and Operators can issue this command.

Example

To display private VLAN settings:

```
DGS-3000-26TC:admin#show private_vlan
Command: show private_vlan

Primary VLAN      3
-----
Promiscuous Ports :
Trunk Ports      :

Total Entries: 1

DGS-3000-26TC: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 |
| show auth_statistics {ports <portlist>} |
| show auth_diagnostics {ports <portlist>} |
| show auth_session_statistics {ports <portlist>} |

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

Used to enable the 802.1X function:

```
DGS-3000-26TC:admin#enable 802.1x
Command: enable 802.1x

Success.

DGS-3000-26TC: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-3000-26TC:admin#disable 802.1x
Command: disable 802.1x

Success.

DGS-3000-26TC: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 a 802.1x user "test":

```
DGS-3000-26TC: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-3000-26TC: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-3000-26TC:admin#delete 802.1x user test
Command: delete 802.1x user test

Success.

DGS-3000-26TC: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-3000-26TC:admin#show 802.1x user
Command: show 802.1x user

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

Total Entries:1

DGS-3000-26TC:admin#
```

4-6 config 802.1x auth_protocol

Description

This command is used to configure the 802.1X auth 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-3000-26TC:admin#config 802.1x auth_protocol radius_eap
Command: config 802.1x auth_protocol radius_eap

Success.

DGS-3000-26TC: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 - Enables the forwarding of EAPOL PDU.

disable - Disables 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-3000-26TC:admin#config 802.1x fwd_pdu system enable
Command: config 802.1x fwd_pdu system enable

Success.

DGS-3000-26TC: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 - Enables forwarding EAPOL PDU receive on the ports.

disable - Disables 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-3000-26TC:admin#config 802.1x fwd_pdu ports 1-2 enable
Command: config 802.1x fwd_pdu ports 1-2 enable

Success.

DGS-3000-26TC:admin#
```

4-9 config 802.1x authorization attributes

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 RADIUS server will be accepted.

Format

config 802.1x authorization attributes radius [enable | disable]

Parameters

radius - If specified to enable, the authorization attributes (for example VLAN, 802.1p default

priority, and ACL) assigned by the RADIUS server will be accepted. The default state is enabled.

enable - Specifies to enable the authorization attributes.

disable - Specifies to disable the authorization attributes.

Restrictions

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

Example

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

```
DGS-3000-26TC:admin#config 802.1x authorization attributes radius disable
Command: config 802.1x authorization attributes radius disable

Success.

DGS-3000-26TC:admin#
```

4-10 show 802.1x

Description

This command is used to display the 802.1X state or configurations.

Format

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

Parameters

auth_state - (Optional) Displays 802.1X authentication state machine of some or all ports.

auth_configuration - (Optional) Used 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.

If no parameter is specified, the 802.1X system configurations will be displayed.

Restrictions

None.

Example

To display the 802.1X port level configurations:

```

DGS-3000-26TC: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

Description

This command is used to configure the port capability.

Format

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

Parameters

ports - Specifies a range of ports to be configured.

<portlist> - Enter the list of ports used for the configuration here.

all - Specifies all ports to be configured.

authenticator - Specifies the port that will enforce authentication before allowing access to services that are accessible from that port. This port will adopt the authenticator role.

none - Disables authentication on the specified ports.

Restrictions

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

Example

To configure the port capability:

```
DGS-3000-26TC:admin#config 802.1x capability ports 1-10 authenticator
Command: config 802.1x capability ports 1-10 authenticator

Success.

DGS-3000-26TC: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, maximum user for per port is also limited. It is specified by 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 maximum user limit will be set to 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-3000-26TC:admin#config 802.1x max_users 200
Command: config 802.1x max_users 200

Success.

DGS-3000-26TC:admin#
```

4-13 config 802.1x auth_parameter

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

| | |
|-----------------------|--|
| ports | - Specifies a range of ports to be configured. <portlist> - Enter the list of ports used for the configuration here. all - Specifies that all the ports will be used. |
| default | - Sets all parameter to be default value. |
| direction | - (Optional) Sets the direction of access control. both - For bidirectional access control. in - For unidirectional access control. |
| port_control | - (Optional) You can force a specific port to be unconditionally authorized or unauthorized by setting the parameter of port_control to be force_auth or force_unauth. Besides, the controlled port will reflect the outcome of authentication if port_control is auto. force_unauth - Forces a specific port to be unconditionally unauthorized. auto - The controlled port will reflect the outcome of authentication. force_auth - Forces a specific port to be unconditionally authorized. |
| quiet_period | - (Optional) It is the initialization value of the quietWhile timer. The default value is 60 seconds and can be any value among 0 to 65535. <sec 0-65535> - Enter the quiet period value here. This value must be between 0 and 65535 seconds. |
| tx_period | - (Optional) It is the initialization value of the transmit timer period. The default value is 30 seconds and can be any integer value among 1 to 65535. <sec 1-65535> - Enter the tx period value here. This value must be between 1 and 65535 seconds. |
| supp_timeout | - (Optional) The initialization value of the aWhile timer when timing out the supplicant. Its default value is 30 seconds and can be any integer value among 1 to 65535. <sec 1-65535> - Enter the supplicant timeout value here. This value must be between 1 and 65535 seconds. |
| server_timeout | - (Optional) The initialization value of the aWhile timer when timing out the authentication server. Its default value is 30 seconds and can be any integer value among 1 to 65535. <sec 1-65535> - Enter the server timeout value here. This value must be between 1 and 65535 seconds. |
| max_req | - (Optional) The maximum number of times that the authentication PAE state machine will retransmit an EAP Request packet to the supplicant. Its default value is 2 and can be any integer number among 1 to 10. <value 1-10> - Enter the maximum required value here. This value must be between 1 and 10. |
| reauth_period | - (Optional) It's a nonzero number of seconds, which is used to be the re-authentication timer. The default value is 3600. <sec 1-65535> - Enter the re-authentication period value here. This value must be between 1 and 65535 seconds. |
| max_users | - (Optional) Specifies per port maximum number of users. 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 used. |
| enable_reauth | - (Optional) You can 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-3000-26TC:admin#config 802.1x auth_parameter ports 1-20 direction both
Command: config 802.1x auth_parameter ports 1-20 direction both

Success.

DGS-3000-26TC:admin#
```

4-14 config 802.1x auth_mode

Description

This command is used to configure 802.1X authentication mode.

Format

config 802.1x auth_mode [port_based | mac_based]

Parameters

port_based - Specifies the authentication as the port-based mode.

mac_based - Specifies the authentication as the MAC-based mode.

Restrictions

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

Example

To configure the authentication mode:

```
DGS-3000-26TC:admin#config 802.1x auth_mode port_based
Command: config 802.1x auth_mode port_based

Success.

DGS-3000-26TC:admin#
```

4-15 config 802.1x init

Description

This command is used to initialize the authentication state machine 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 the authentication as the port-based mode.
<portlist> - Enter the list of ports used for the configuration here.
all - Specifies that all ports will be used.

mac_based ports - Specifies the authentication as the MAC-based mode.
<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 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 machine of some or all:

```
DGS-3000-26TC:admin#config 802.1x init port_based ports all
Command: config 802.1x init port_based ports all

Success.

DGS-3000-26TC:admin#
```

4-16 config 802.1x reauth

Description

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

Format

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

Parameters

port_based ports - Specifies the authentication as the port-based mode.
<portlist> - Enter the list of ports used for the configuration here.
all - Specifies that all ports will be used.

mac_based ports - Specifies the authentication as the MAC-based mode.
<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 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-3000-26TC:admin#config 802.1x reauth port_based ports all
Command: config 802.1x reauth port_based ports all

Success.

DGS-3000-26TC:admin#
```

4-17 create 802.1x guest_vlan

Description

This command is used to assign a static VLAN to be guest VLAN. The specific VLAN which assigned to guest VLAN must be existed. The specific VLAN which assigned to guest VLAN can't be deleting.

Format

create 802.1x guest_vlan <vlan_name 32>

Parameters

<vlan_name 32> - Specifies the VLAN to be 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 802.1X guest VLAN:

```
DGS-3000-26TC:admin#create 802.1x guest_vlan guestVLAN
Command: create 802.1x guest_vlan guestVLAN

Success.

DGS-3000-26TC:admin#
```

4-18 delete 802.1x guest_vlan

Description

This command is used to delete guest VLAN setting, but not delete the static VLAN. All ports which enabled guest VLAN will remove to original VLAN after deleted guest VLAN.

Format

delete 802.1x guest_vlan <vlan_name 32>

Parameters

<vlan_name 32> - Enter the 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-3000-26TC:admin#delete 802.1x guest_vlan guestVLAN
Command: delete 802.1x guest_vlan guestVLAN

Success.

DGS-3000-26TC:admin#
```

4-19 config 802.1x guest_vlan

Description

This command is used to configure guest VLAN setting. If the specific port state is changed from enabled state to disable state, this port will move to its original VLAN.

Format

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

Parameters

ports - A range of ports enable or disable guest VLAN function.
<portlist> - Enter the list of ports used for the configuration here.
all - Specifies that all the port 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

Enable on port 2 to 8 to configure 802.1X guest VLAN:

```
DGS-3000-26TC: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-3000-26TC: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-3000-26TC: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-3000-26TC:admin#
```

4-21 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-3000-26TC: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
```

4-22 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-3000-26TC: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
```

4-23 show auth_session_statistics

Description

This command is used to display information of 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 for port 1:

```
DGS-3000-26TC: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
```

Chapter 5 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> ipv6 <ipv6addr>] protocol [tacacs xtacacs tacacs+ radius] |
| delete authen server_group <string 15> |
| show authen server_group {<string 15>} |
| create authen server_host [<ipaddr> ipv6 <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> ipv6 <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> ipv6 <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>} |
| create accounting method_list_name <string 15> |
| config accounting [default method_list_name <string 15>] method {tacacs+ radius server_group <string 15> none} |
| delete accounting method_list_name <string 15> |
| show accounting [default method_list_name <string 15> all] |
| config accounting service command {administrator operator power_user user} [method_list_name <string> none] |
| config accounting service [network shell system] state [enable {[radius_only method_list_name <string 15> default_method_list]} disable] |
| show accounting service |
| show aaa |

5-1 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 the 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-3000-26TC:admin#enable password encryption
Command: enable password encryption

Success.

DGS-3000-26TC:admin#
```

5-2 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 plain text form, the password will be in plain text form. However, if the user specifies the password in encrypted form, or if the password has been converted to encrypted form by the last enable password encryption command, the password will still be in the encrypted form. It can not be reverted to the plaintext.

Format

disable password encryption

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To disable the password encryption:

```
DGS-3000-26TC:admin#disable password encryption
Command: disable password encryption

Success.

DGS-3000-26TC:admin#
```

5-3 enable authen_policy

Description

This command is used to enable system access authentication policy.

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-3000-26TC:admin#enable authen_policy
Command: enable authen_policy

Success.

DGS-3000-26TC:admin#
```

5-4 disable authen_policy

Description

This command is used to disable system access authentication policy.

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-3000-26TC:admin#disable authen_policy
Command: disable authen_policy

Success.

DGS-3000-26TC:admin#
```

5-5 show authen_policy

Description

This command is used to display that system access authentication policy is enabled or disabled.

Format

show authen_policy

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To display system access authentication policy:

```
DGS-3000-26TC:admin#show authen_policy
Command: show authen_policy

Authentication Policy : Enabled

DGS-3000-26TC:admin#
```

5-6 create authen_login

Description

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

Format

create authen_login method_list_name <string 15>

Parameters

<string 15> - 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-3000-26TC:admin#create authen_login method_list_name login_list_1
Command: create authen_login method_list_name login_list_1

Success.

DGS-3000-26TC:admin#
```

5-7 config authen_login

Description

Configure a user-defined or default method list of authentication methods for user login. The sequence of methods will effect the alteration result. For example, if the sequence is tacacs+ first, then tacacs and local, when user trys to login, 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...If all server hosts in tacacs group are missing, the local account database in the device is used to authenticate this user. When user logs in 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 only. If user wants to get admin privilege level, user must use the “enable admin” command to promote his privilege level. But when local method is used, the privilege level will depend on this 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 - The default method list of authentication methods.

method_list_name - The user-defined method list of authentication methods.

<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 to authenticate by using the built-in server group called “tacacs”.

xtacacs - (Optional) Specifies to authenticate by using the built-in server group called “xtacacs”.

tacacs+ - (Optional) Specifies to authenticate by using the built-in server group called “tacacs+”.

radius - (Optional) Specifies to authenticate by using the built-in server group called “radius”.

server_group - (Optional) Specifies to authenticate by using the user-defined server group.

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

local - (Optional) Specifies to authenticate by local user account database in device.

none - (Optional) No authentication.

Restrictions

Only Administrators can issue this command.

Example

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

```
DGS-3000-26TC: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-3000-26TC:admin#
```

5-8 delete authen_login

Description

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

Format

```
delete authen_login method_list_name <string 15>
```


Parameters

<string 15> - 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-3000-26TC:admin#delete authen_login method_list_name login_list_1
Command: delete authen_login method_list_name login_list_1

Success.

DGS-3000-26TC:admin#
```

5-9 show authen_login

Description

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

Format

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

Parameters

default - Displays default user-defined method list for user login.

method_list_name - Displays 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 - Displays 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-3000-26TC: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-3000-26TC:admin#
```

5-10 create authen_enable

Description

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

Format

create authen_enable method_list_name <string 15>

Parameters

<string 15> - 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-3000-26TC:admin#create authen_enable method_list_name enable_list_1
Command: create authen_enable method_list_name enable_list_1

Success.

DGS-3000-26TC:admin#
```

5-11 config authen_enable

Description

This command is used to configure a user-defined or default method list of authentication methods for promoting user's privilege to Admin level. The sequence of methods will affect the alteration result. For example, if the sequence is tacacs+ first, then tacacs and local_enable, when user try to promote user's 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...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 - The default method list of authentication methods.

method_list_name - The user-defined method list of authentication methods.

<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 to authenticate by using the built-in server group called "tacacs".

xtacacs - (Optional) Specifies to authenticate by using the built-in server group called "xtacacs".

tacacs+ - (Optional) Specifies to authenticate by using the built-in server group called "tacacs+".

radius - (Optional) Specifies to authenticate by using the built-in server group called "radius".

server_group - (Optional) Specifies to authenticate by 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 to authenticate by local enable password in device.

none - (Optional) No authentication.

Restrictions

Only Administrators can issue this command.

Example

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

```
DGS-3000-26TC: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-3000-26TC:admin#
```

5-12 delete authen_enable

Description

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

Format

delete authen_enable method_list_name <string 15>

Parameters

<string 15> - 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 user's privilege to Admin level:

```
DGS-3000-26TC:admin#delete authen_enable method_list_name enable_list_1
Command: delete authen_enable method_list_name enable_list_1

Success.

DGS-3000-26TC:admin#
```

5-13 show authen_enable

Description

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

Format

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

Parameters

default - Displays default user-defined method list for promoting user's privilege to Admin level.

method_list_name - Displays the specific user-defined method list for promoting user's privilege to Admin level.

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

all - Displays all method lists for promoting user's privilege to Admin level.

Restrictions

Only Administrators can issue this command.

Example

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

```
DGS-3000-26TC: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_enable     Keyword

DGS-3000-26TC:admin#
```

5-14 config authen application

Description

This command is used to configure 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 - Application: console.

telnet - Application: TELNET.

ssh - Application: SSH.

http - Application: web.

all - Application: console, TELNET, SSH, and web.

login - Selects the method list of authentication methods for user login.

enable - Selects the method list of authentication methods for promoting user's privilege to Admin level.

default - Default method list.

method_list_name - 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-3000-26TC: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-3000-26TC:admin#
```

5-15 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-3000-26TC: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-3000-26TC:admin#
```

5-16 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 group consists of 8 server hosts as maximum.

Format

create authen server_group <string 15>

Parameters

<string 15> - 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-3000-26TC:admin#create authen server_group mix_1
Command: create authen server_group mix_1

Success.

DGS-3000-26TC:admin#
```

5-17 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 server group "tacacs", "xtacacs", "tacacs+", "radius" accepts the server host with the same protocol only, but user-defined server group can accept server hosts with different protocols.

Format

```
config authen server_group [tacacs | xtacacs | tacacs+ | radius | <string 15>] [add | delete]
server_host [<ipaddr> | ipv6 <ipv6addr> ] protocol [tacacs | xtacacs | tacacs+ | radius]
```

Parameters

server_group - User-defined server group.
tacacs - Built-in server group "tacacs".
xtacacs - Built-in server group "xtacacs".
tacacs+ - Built-in server group "tacacs+".
radius - Built-in server group "radius".
<string 15> - Enter the server group name here. This value can be up to 15 characters long.

add - Adds a server host to a server group.
delete - Removes a server host from a server group.

server_host - Specifies the IP address of the server host.
<ipaddr> - Enter the server host IPv4 address.
ipv6 - Specifies the server host IPv6 address.
<ipv6addr> - Enter the server host IPv6 address.

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 an server group:

```
DGS-3000-26TC: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-3000-26TC:admin#
```

5-18 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> - 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-3000-26TC:admin#delete authen server_group mix_1
Command: delete authen server_group mix_1

Success.

DGS-3000-26TC:admin#
```

5-19 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) 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-3000-26TC: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-3000-26TC:admin#
```

5-20 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> | ipv6 <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.

ipv6 - Specifies the server host IPv6 address.

<ipv6addr> - Enter the server host IPv6 address.

protocol - Specifies the host's authentication protocol.

tacacs - Server host's authentication protocol.

xtacacs - Server host's authentication protocol.

tacacs+ - Server host's authentication protocol.

radius - Server host's authentication protocol.

port - (Optional) 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) 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 - No encryption for TACACS+ and RADIUS authentication. This value is meaningless for TACACS and XTACACS.

timeout - (Optional) 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) 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-3000-26TC: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-3000-26TC:admin#
```

5-21 config authen server_host

Description

This command is used to configure an authentication server host.

Format

```
config authen server_host [<ipaddr> | ipv6 <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.

ipv6 - Specifies the server host IPv6 address.

<ipv6addr> - Enter the server host IPv6 address.

protocol - Specifies the server host's authentication protocol.

tacacs - Server host's authentication protocol.

xtacacs - Server host's authentication protocol.

tacacs+ - Server host's authentication protocol.

radius - Server host's authentication protocol.

port - (Optional) 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 port number here. This value must be between 1 and 65535.

key - (Optional) 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 - No encryption for TACACS+ and RADIUS authentication. This value is meaningless for TACACS and XTACACS.

timeout - (Optional) 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) 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-3000-26TC: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-3000-26TC:admin#
```

5-22 delete authen server_host

Description

This command is used to delete an authentication server host.

Format

delete authen server_host [<ipaddr> | ipv6 <ipv6addr>] protocol [tacacs | xtacacs | tacacs+ | radius]

Parameters

<ipaddr> - Enter the server host's IP address.

ipv6 - Specifies the server host IPv6 address.

<ipv6addr> - Enter the server host IPv6 address.

protocol - Specifies that server host's authentication protocol.

tacacs - Server host's authentication protocol.

xtacacs - Server host's authentication protocol.

tacacs+ - Server host's authentication protocol.
radius - Server host's authentication protocol.

Restrictions

Only Administrators can issue this command.

Example

To delete an authentication server host:

```
DGS-3000-26TC:admin#delete authen server_host 10.1.1.222 protocol tacacs+
Command: delete authen server_host 10.1.1.222 protocol tacacs+

Success.

DGS-3000-26TC:admin#
```

5-23 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-3000-26TC: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-3000-26TC:admin#
```

5-24 config authen parameter response_timeout

Description

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

Format

config authen parameter response_timeout <int 0-255>

Parameters

<int 0-255> - 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 for user input to be 60 seconds:

```
DGS-3000-26TC:admin#config authen parameter response_timeout 60
Command: config authen parameter response_timeout 60

Success.

DGS-3000-26TC:admin#
```

5-25 config authen parameter attempt

Description

This command is used to configure the maximum attempts for user's 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> - The amount of attempts for user's 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 user's trying to login or promote the privilege to be 9:

```
DGS-3000-26TC:admin#config authen parameter attempt 9
Command: config authen parameter attempt 9

Success.

DGS-3000-26TC:admin#
```

5-26 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-3000-26TC:admin#show authen parameter
Command: show authen parameter

Response Timeout : 60 seconds
User Attempts    : 9

DGS-3000-26TC:admin#
```

5-27 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 user wants to use either one of these 3 protocols to do enable authentication, 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 can not be used when authentication policy is disabled.

Format**enable admin****Parameters**

None.

Restrictions

None.

Example

To enable administrator level privilege:

```
DGS-3000-26TC:puser#enable admin
Command: enable admin

PassWord:*****
Success.

DGS-3000-26TC:admin#
```

5-28 config admin local_enable**Description**

This command is used to config 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 local device is needed. When the password information is not specified in the command, the system will prompt the user to input the password interactively. For this case, the user can only input the plain text password. If the password is present in the command, the user can select to input the password in the plain text form or in the encrypted form. The encryption algorithm is based on SHA-1.

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

encrypt - (Optional) Specifies the password form.

plain_text - Specifies the password in plain text form.

sha_1 - Specifies the password in SHA-1 encrypted form.

<password> - (Optional) 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-3000-26TC: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-3000-26TC:admin#
```

5-29 create accounting method_list_name

Description

This command is used to create a user-defined list of accounting methods for accounting services on the Switch. The maximum supported number of accounting method lists is 8.

Format

create accounting method_list_name <string 15>

Parameters

<string 15> - Specifies the built-in or user-defined method list.

Restrictions

Only Administrators can issue this command.

Example

To create a user-defined accounting method list called "shell_acct":

```
DGS-3000-26TC:admin#create accounting method_list_name shell_acct
Command: create accounting method_list_name shell_acct

Success.

DGS-3000-26TC:admin#
```

5-30 config accounting

Description

This command is used to configure a user-defined or default method list of accounting methods.

Format

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

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 protocol.

tacacs+ - Specifies the built-in TACACS+ server group.

radius - Specifies the built-in RADIUS server group.

server_group - Specifies the user-defined server group. If the group contains TACACS and XTACACS server, it will be skipped in accounting.

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

none - Specifies no accounting.

Restrictions

Only Administrators can issue this command.

Example

To configure a user-defined method list called "shell_acct", that specifies a sequence of the built-in TACACS+ server group, followed by the RADIUS server group for accounting service on the Switch:

```
DGS-3000-26TC:admin#config accounting method_list_name shell_acct method
tacacs+ radius
Command: config accounting method_list_name shell_acct method tacacs+ radius

Success.

DGS-3000-26TC:admin#
```

5-31 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> - Specifies the built-in or user-defined method list.

Restrictions

Only Administrators can issue this command.

Example

To delete the user-defined accounting method list called "shell_acct" from the Switch:

```
DGS-3000-26TC:admin#delete accounting method_list_name shell_acct
Command: delete accounting method_list_name shell_acct

Success.

DGS-3000-26TC:admin#
```

5-32 show accounting**Description**

This command is used to display the list of accounting methods on the Switch.

Format

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

Parameters

default - Displays the user-defined list of default accounting methods.

method_list_name - Specifies the user-defined list of specific accounting methods.

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

all - Displays all accounting method lists on the Switch.

Restrictions

Only Administrators can issue this command.

Example

To display the user-defined accounting method list called "shell_acct":

```
DGS-3000-26TC: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-3000-26TC:admin#
```

5-33 config accounting service command

Description

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

Format

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

Parameters

| |
|--|
| administrator - Accounting service for all administrator level commands. |
| operator - Accounting service for all operator level commands. |
| power_user - Accounting service for all power-user level commands. |
| user - Accounting service for all user level commands. |
| method_list_name - Specifies accounting service by the AAA user-defined method list specified by the create accounting method_list_name <string 15> command. |
| <string> - Enter the name of the method list. |
| none - Disables AAA command accounting services by specified command level. |

Restrictions

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

Example

To enable AAA accounting methodlist "shell_acct" to configure accounting shell state:

```
DGS-3000-26TC:admin#config accounting service command method_list_name
shell_acct
Command: config accounting service command method_list_name shell_acct

Success.

DGS-3000-26TC:admin#
```

5-34 config accounting service

Description

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

Format

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

Parameters

| |
|--|
| network - Accounting service for 802.1X, JWAC and WAC port access control. By default, the service is disabled. |
|--|

shell - Accounting service for shell events: When user logs on or out the Switch (via the console, Telnet, or SSH) and timeout occurs, accounting information will be collected and sent to RADIUS server. By default, the service is disabled.

system - Accounting service for system events: reset, 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 accounting service to only use radius group specified by the **config radius add** command.

method_list_name - (Optional) Specifies accounting service by the AAA user-defined method list specified by the "create accounting method_list_name <string 15>" command.

<string 15> - Enter the method list name.

default_method_list - (Optional) Specifies accounting service by the AAA default method list.

disable - Specifies to disable the specified accounting service.

Restrictions

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

Example

Enable it to configure accounting shell state:

```
DGS-3000-26TC:admin#config accounting service shell state enable
Command: config accounting service shell state enable

Success.

DGS-3000-26TC:admin#
```

5-35 show accounting service

Description

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

Format

show accounting service

Parameters

None.

Restrictions

None.

Example

To show information of RADIUS accounting services:

```
DGS-3000-26TC:admin#show accounting service
Command: show accounting service

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

DGS-3000-26TC:admin#
```

5-36 show aaa

Description

This command is used to display AAA global configuration

Format

show aaa

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To display AAA global configuration:

```
DGS-3000-26TC:admin#show aaa
Command: show aaa

Authentication Policy: Enabled
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-3000-26TC:admin#
```

Chapter 6 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-ffffffff> | destination_mac <macmask 000000000000-ffffffff> | 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 <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff> | flag_mask [all | {urg | ack | psh | rst | syn | fin}]} | udp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | protocol_id_mask <hex 0x0-0xff> {user_define_mask <hex 0x0-0xffffffff>}}] | packet_content_mask { offset_chunk_1 <value 0-31> <hex 0x0-0xffffffff> | offset_chunk_2 <value 0-31> <hex 0x0-0xffffffff> | offset_chunk_3 <value 0-31> <hex 0x0-0xffffffff> | offset_chunk_4 <value 0-31> <hex 0x0-0xffffffff>} | ipv6 {class | flowlabel | source_ipv6_mask <ipv6mask> | destination_ipv6_mask <ipv6mask> | [tcp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | udp { src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | 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 1-256>][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 0x0-0xffff> | 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 <hex 0x0-0xffff>}} | 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 1-256>]

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 1-256> [rate [<value 1-1048576>] {burst_size [<value 1-262144>]} rate_exceed [drop_packet | remark_dscp <value 0-63>] | tr_tcm cir <value 1-1048576> {cbs <value 1-262144>} pir <value 1-1048576> {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 1-1048576> 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 1-256>}]

```
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
```

6-1 create access_profile

Description

This command is used to create access control list profiles.

When creating ACL, each profile can have 256 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 194 rules are available to configure. You can use the **show access_profile** command to see the available rules.

Support for field selections can have additional limitations that are project dependent.

For example, for some hardware, it may be invalid to specify a destination and source IPv6 address at the same time. The user will be prompted with these limitations.

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

Note: Profile Types 7 and 8 are not user configurable. Only system applications are allowed to create this type of profiles.

Format

```
create access_profile profile_id <value 1-512> {profile_name <name 32>} [ethernet {vlan
<hex 0x0-0x0fff>} | source_mac <macmask 000000000000-ffffffff> | destination_mac
<macmask 000000000000-ffffffff> | 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

-
- profile_id** - Specifies the index of the access list profile.
 <value 1-512> - Enter the profile ID here. This value must be between 1 and 512.
-
- profile_name** - The name of the profile must be specified. 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-3000-26TC: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-3000-26TC: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-3000-26TC: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-3000-26TC:admin#

```

6-2 delete access_profile

Description

This command is used to delete access list profiles. This command can only delete profiles that were created using the ACL module.

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-3000-26TC:admin#delete access_profile profile_id 1
Command: delete access_profile profile_id 1

Success.

DGS-3000-26TC:admin#
```

6-3 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 1-256>][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 0x0-0xffff> | 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 1-256>]
```

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. The value range is 1-256, but the supported maximum number of entries depends on the project. If the auto_assign option is selected, the access ID is automatically assigned, when adding multiple ports.
-

- auto_assign** - Specifies that the access ID will automatically be assigned.
<value 1-256> - Enter the access ID used here. This value must be between 1 and 256.
-
- 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** - A maximum of 4 offsets can be specified. 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. The value range is 1-256, but the supported maximum number of entries depends on the project.

<value 1-256> - Enter the access ID used here. This value must be between 1 and 256.

Restrictions

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

Example

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

```
DGS-3000-26TC:admin#config access_profile profile_id 3 add access_id
auto_assign packet_content offset_chunk_3 0xF0 port all deny
Command: config access_profile profile_id 3 add access_id auto_assign
packet_content offset_chunk_3 0xF0 port all deny
```

Success.

```
DGS-3000-26TC:admin#
```

6-4 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-3000-26TC:admin#show access_profile
Command: show access_profile
```

```
Access Profile Table
```

```
Total User Set Rule Entries : 4
```

```
Total Used HW Entries      : 128
Total Available HW Entries : 896

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

MASK on
  VLAN              : 0xFFF
  802.1p
  Ethernet Type

Available HW Entries : 193
-----
Rule ID : 1      Ports: 1

Match on
  VLAN ID          : 1
  802.1p           : 0
  Ethernet Type   : 0xFFFE

Action:
  Permit

=====

=====
Profile ID: 2      Profile name: IPv4ACL  Type: IPv4

MASK on
  VLAN              : 0xFFF
  DSCP
  ICMP

Available HW Entries : 193
-----
Rule ID : 1      Ports: 2

Match on
  VLAN ID          : 1
  DSCP             : 0

Action:
  Permit

=====

=====
Profile ID: 3      Profile name: IPv6ACL  Type: IPv6

MASK on
  Class
  TCP
```



```

Available HW Entries : 255
-----
Rule ID : 1          Ports: 3

Match on
  Class              : 0

Action:
  Permit

=====

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

MASK on
  offset_chunk_1 : 0      value : 0x00000000
  offset_chunk_2 : 1      value : 0x00000000
  offset_chunk_3 : 2      value : 0x00000000
  offset_chunk_4 : 3      value : 0x00000000

Available HW Entries : 255
-----
Rule ID : 1          Ports: 4

Match on
  offset_chunk_1 : 0      value : 0x0000FFEE      Mask : 0x0000FFEE

Action:
  Permit
  Priority              : 1
  Replace DSCP         : 1

=====

DGS-3000-26TC:admin#

```

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

```

DGS-3000-26TC:admin#show access_profile profile_id 2
Command: show access_profile profile_id 2

Access Profile Table

Profile ID: 2      Profile Name: 2                          Type : Ethernet
Mask on
  VLAN              : 0xF
  Source MAC        : FF-FF-FF-00-00-00
  Destination MAC   : 00-00-00-FF-FF-FF
Available HW Entries: 255
-----
Rule ID : 22      Ports: 1-7
Match on
  VLAN ID           : 8                               Mask : 0xFFF
  Source MAC        : 00-01-02-03-04-05             Mask : FF-FF-FF-FF-FF-FF
  Destination MAC   : 00-05-04-03-02-00             Mask : FF-FF-FF-FF-FF-00
Action:
Deny

DGS-3000-26TC:admin#
    
```

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

```

DGS-3000-26TC: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 : 255
-----
Rule ID : 1      Ports: 1-2
Match on
  offset_chunk_1 : 3      value : 0x000086DD
  offset_chunk_2 : 5      value : 0x00003A00
  offset_chunk_3 : 14     value : 0x86000000

Action:
  Deny

DGS-3000-26TC:admin#
    
```

6-5 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 1-256> [rate <value 1-1048576>] {burst_size <value 1-262144>} rate_exceed [drop_packet | remark_dscp <value 0-63>] | tr_tcm cir <value 1-1048576> {cbs <value 1-262144>} pir <value 1-1048576> {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 1-1048576> 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 1-256> - Enter the access ID used here. This value must be between 1 and 256.

rate - Specifies the rate for single rate two color mode. Specifies the committed bandwidth in Kbps for the flow.

<value 1-1048576> - Enter the rate for single rate two color mode here. This value must be

between 1 and 1048576.

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 - Drops the packet immediately.

remark_dscp - Marks 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 1-1048576> - Enter the committed information rate value here. This value must be between 1 and 1048576.

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 committed burst size 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 1-1048576> - Enter the peak information rate value here. This value must be between 1 and 1048576.

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 - Permits the packet.

replace_dscp - Changes the DSCP 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 - Permits the packet.

replace_dscp - (Optional) Changes the DSCP of the packet.

<value 0-63> - Enter the replace DSCP value here. This value must be between 0 and 63.

drop - Drops 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 - Enables the ACL counter option.

disable - Disables the ACL counter option.

violate - Specifies the action when a packet is mapped to the "red" color.

permit - Permits the packet.

replace_dscp - (Optional) Changes the DSCP of the packet.

<value 0-63> - Enter the replace DSCP value here. This value must be between 0 and 63.

drop - Drops 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 ommitted Information Rate. The unit is Kbps.
 - <value 0-1048576>** - Enter the comitted information rate value here. This value must be between 0 and 1048576.
 - cbs** - Specifies the "Committed Burst Size" The unit is Kbytes.
 - <value 0-131072>** - Enter the committed burst size value here. This value must be between 0 and 131072.
 - ebs** - Specifies the "Excess Burst Size". The unit is Kbytes.
 - <value 0-131072>** - Enter the excess burst size value here. This value must be between 0 and 131072.
 - 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** - Changes the DSCP 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** - Enables the ACL counter option.
 - disable** - Disables the ACL counter option.
 - exceed** - Specifies the action when a packet is mapped to the "yellow" color.
 - permit** - Permits the packet.
 - replace_dscp** - (Optional) Changes the DSCP of the packet.
 - <value 0-63>** - Enter the replace DSCP value here. This value must be between 0 and 63.
 - drop** - Drops 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** - Enables the ACL counter option.
 - disable** - Disables the ACL counter option.
 - violate** - Specifies the action when a packet is mapped to the "red" color.
 - permit** - Permits the packet.
 - replace_dscp** - (Optional) Changes the DSCP of the packet.
 - <value 0-63>** - Enter the replace DSCP value here. This value must be between 0 and 63.
 - drop** - Drops 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** - Enables the ACL counter option.
 - disable** - Disables the ACL counter option.

 - delete** - Deletes 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-3000-26TC: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-3000-26TC:admin#
```

6-6 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 1-256>}}

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 1-256> - Enter the access ID used here. This value must be between 1 and 256. |

Restrictions

None.

Example

To display the flow metering configuration:

```

DGS-3000-26TC: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-3000-26TC:admin#

```

6-7 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. Note that 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

-
- time_range** - Specifies the name of the time range settings.
- <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-3000-26TC: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-3000-26TC:admin#config time_range 1 delete
Command: config time_range 1 delete

Success.

DGS-3000-26TC:admin#
```

6-8 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-3000-26TC: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-3000-26TC:admin#
```

6-9 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** 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-3000-26TC: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-3000-26TC:admin#
```

Chapter 7 Address Resolution Protocol (ARP) Command List

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

7-1 create arprentry

Description

This command is used to enter a static ARP entry into the Switch's ARP table.

Format

create arprentry <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-3000-26TC:admin#create arprentry 10.48.74.121 00-50-BA-00-07-36
Command: create arprentry 10.48.74.121 00-50-BA-00-07-36

Success.

DGS-3000-26TC:admin#
```

7-2 delete arprentry

Description

This command is used to delete an ARP entry, by specifying either the IP address of the entry or all. Specifies 'all' clears the Switch's ARP table.

Format

delete arpentry [<ipaddr> | all]

Parameters

<ipaddr> - The IP address of the end node or station.

all - Specifies to 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-3000-26TC:admin#delete arpentry 10.48.74.121
Command: delete arpentry 10.48.74.121

Success.

DGS-3000-26TC:admin#
```

7-3 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-3000-26TC: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-3000-26TC:admin#
```

7-4 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-3000-26TC:admin#config arp_aging time 30
Command: config arp_aging time 30

Success.

DGS-3000-26TC:admin#
```

7-5 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-3000-26TC:admin#clear arptable
Command: clear arptable

Success.

DGS-3000-26TC:admin#
```

7-6 show arpentry

Description

This command is used to displays 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) 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) The IP address of the end node or station.

<ipaddr> - Enter the IP address here.

static - (Optional) Displays the static entries in the ARP table.

mac_address - (Optional) Displays the ARP entry by MAC address.

<macaddr> - Enter the MAC address here.

Restrictions

None.

Example

To display the ARP table:

```
DGS-3000-26TC: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-3000-26TC:admin#
```

Chapter 8 ARP Spoofing Prevention Command List

```
config arp_spoofing_prevention [add gateway_ip <ipaddr> gateway_mac <macaddr> ports  
[<portlist> | all] | delete gateway_ip <ipaddr>]  
show arp_spoofing_prevention
```

8-1 config arp_spoofing_prevention

Description

This command is used to configure the spoofing prevention entry to prevent spoofing of MAC for the protected gateway. When an entry is created, those ARP packets whose sender IP matches the gateway IP of an entry, but 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 of 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 and Operators can issue this command.

Example

To configure the ARP spoofing prevention entry:


```
DGS-3000-26TC: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-3000-26TC:admin#
```

8-2 show arp_spoofing_prevention

Description

This command is used to show the ARP spoofing prevention entry.

Format

show arp_spoofing_prevention

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To display the ARP spoofing prevention entries:

```
DGS-3000-26TC:admin#show arp_spoofing_prevention
Command: show arp_spoofing_prevention

Gateway IP          Gateway MAC          Ports
-----
10.254.254.251     00-00-00-11-11-11  1-2

Total Entries: 1

DGS-3000-26TC:admin#
```

Chapter 9 Auto-Configuration Command List

| |
|--|
| enable autoconfig |
| disable autoconfig |
| show autoconfig |
| config autoconfig timeout <value 1-65535> |

9-1 enable autoconfig

Description

This command is used to enable auto configuration. When enabled, during power on initialization, the Switch will get configure file path name 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 autoconfig:

```
DGS-3000-26TC:admin#enable autoconfig
Command: enable autoconfig

Success.

DGS-3000-26TC:admin#
```

9-2 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 autoconfig:

```
DGS-3000-26TC:admin#disable autoconfig
Command: disable autoconfig

Success.

DGS-3000-26TC:admin#
```

9-3 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 autoconfig status:

```
DGS-3000-26TC:admin#show autoconfig
Command: show autoconfig

Autoconfig State: Disabled
Timeout           : 50 sec

DGS-3000-26TC:admin#
```

9-4 config autoconfig timeout

Description

This command is used to configure the timeout value. This timer is used to limit the length of time in 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 Administrator, and Operator level users can issue this command.

Example

To configure auto configuration timeout:

```
DGS-3000-26TC:admin#config autoconfig timeout 60
Command: config autoconfig timeout 60

Success.

DGS-3000-26TC:admin#
```

Chapter 10 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]] ipv4 state [enable disable] dhcp_option12 [hostname <hostname63> 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>} |

10-1 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 number of account (include admin and user) is up to 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 a operator user account. |
| power_user - Specifies the name for a 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 plain text form. |

sha_1 - Specifies the password in the SHA-1 encrypted form.

<password> - The password for the user account. The length for of password in plain-text form and in encrypted form are different. For the plain-text form, passwords must have a minimum of 0 character and can have a maximum of 15 characters. For the encrypted form password, the length is fixed to 35 bytes long. The password is case-sensitive.

Restrictions

Only Administrators can issue this command.

Example

To create the admin-level user “dlink”:

```
DGS-3000-26TC: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-3000-26TC:admin#
```

To create the user-level user “Remote-Manager”:

```
DGS-3000-26TC: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-3000-26TC:admin#
```

10-2 config account

Description

This command is used to configure user account. When the password information is not specified in the command, the system will prompt the user to input the password interactively. For this case, the user can only input the plain text password.

If the password is present in the command, the user can select to input the password in the plain text form or in the encrypted form. The encryption algorithm is based on SHA-1.

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 plain text form.

sha_1 - Specifies the password in the SHA-1 encrypted form.

<password> - The password for the user account. The length for of password in plain-text form and in encrypted form are different. For the plain-text form, passwords must have a minimum of 0 character and can have a maximum of 15 characters. For the encrypted form password, the length is fixed to 35 bytes long. The assword is case-sensitive.

Restrictions

Only Administrators can issue this command.

Example

To configure the user password of “dlink” account:

```
DGS-3000-26TC: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-3000-26TC:admin#
```

To configure the user password of “administrator” account:

```
DGS-3000-26TC:admin#config account administrator encrypt sha_1
*~&cRDtpNCeBiq15KOQsKVYrA0sAiCIZQwq
Command: config account administrator encrypt sha_1
*~&cRDtpNCeBiq15KOQsKVYrA0sAiCIZQwq

Success.

DGS-3000-26TC:admin#
```

10-3 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-3000-26TC:admin#show account
Command: show account

Current Accounts:
Username           Access Level
-----
admin              Admin
oper               Operator
power              Power_user
user               User

Total Entries : 4

DGS-3000-26TC:admin#
```

10-4 delete account

Description

This command is used to delete an existing account.

Format

delete account <username>

Parameters

<username> - Specifies to delete the name of the user.

Restrictions

Only Administrators can issue this command.

Example

To delete the user account "System":

```
DGS-3000-26TC:admin#delete account System
Command: delete account System

Success.

DGS-3000-26TC:admin#
```


10-5 show switch

Description

This command is used to display the Switch information.

Format

show switch

Parameters

None.

Restrictions

None.

Example

The following is an example for display of the Switch information.

```
DGS-3000-26TC:admin#show sw
Command: show switch

Device Type           : DGS-3000-26TC Gigabit Ethernet Switch
MAC Address           : 00-01-02-03-04-00
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 1.00.001
Firmware Version      : Build 1.00.015
Hardware Version      : A1
System Name           :
System Location        :
System Uptime          : 0 days, 2 hours, 2 minutes, 52 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
SSL Status             : Disabled
CTRL+C  ESC  c Quit  SPACE  n Next Page  ENTER  Next Entry  a All
```

10-6 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-3000-26TC:admin#enable telnet 23
Command: enable telnet 23

Success.

DGS-3000-26TC:admin#
```

10-7 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-3000-26TC:admin#disable telnet
Command: disable telnet

Success.

DGS-3000-26TC:admin#
```

10-8 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) The TCP port number. TCP ports are numbered between 1 and 65535. The “well-known” TCP port for the WEB protocol is 80.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable HTTP and configure port number:

```
DGS-3000-26TC:admin#enable web 80
Command: enable web 80

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

DGS-3000-26TC:admin#
```

10-9 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-3000-26TC:admin#disable web
Command: disable web

Success.

DGS-3000-26TC:admin#
```

10-10 reboot

Description

This command is used to restart the Switch.

Format

reboot {force_agree}

Parameters

force_agree - (Optional) The **reboot** command will be executed immediately without further confirmation.

Restrictions

Only Administrators can issue this command.

Example

To reboot the Switch:

```
DGS-3000-26TC:admin#reboot
Command: reboot

Are you sure to proceed with the system reboot?(y/n)
Please wait, the switch is rebooting...
```

10-11 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 IP address, log, user accounts and banner configured on the system.

Format

reset {[config | system]} {force_agree}

Parameters

config - (Optional) All parameters are reset to default settings. However, the device will neither save or reboot.

system - (Optional) All parameters are reset to default settings, and the Switch will reset to factory default settings, save and reboot.

force_agree - (Optional) The **reset** command will be executed immediately without further confirmation.

Restrictions

Only Administrators can issue this command.

Example

To reset the Switch:

```
DGS-3000-26TC: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...
```

10-12 config firmware image

Description

This command is used to select a firmware file as a boot up file. This command is required to be supported when multiple firmware images are supported.

Format

config firmware image <path_filename64>boot_up

Parameters

<path_filename64> - Specifies 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:/ DGS3000_Run_1_00_010.had as the boot up image:

```
DGS-3000-26TC:admin#config firmware image c:/DGS3000_Run_1_00_010.had boot_up
Command: config firmware image c:/DGS3000_Run_1_00_010.had boot_up

Success.

DGS-3000-26TC:admin#
```

10-13 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 - Specifies the name of the IP interface.

<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 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-3000-26TC: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-3000-26TC:admin#
```

10-14 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]] | ipv4 state [enable | disable] | dhcp_option12 [hostname <hostname63> |
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) Configures a network on an ipif. The address should specify a host address and length of network mask. Since an ipif can have only one IPv4 address, the new 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 the state of the interface. |
| enable | - Enables the state of the interface. |
| disable | - Disables the state of the interface. |
| bootp | - Uses BOOTP to obtain the IPv4 address. |
| dhcp | - Uses 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 state will be enabled. |
| disable | - Specifies that the IPv6 interface state will be disabled. |
| 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 state will be enabled. |
| disable | - Specifies that the IPv4 interface state 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 have only letters, digits, and hyphen as interior characters; the maximal length is 63. |
| clear_hostname | - Clears the host name setting. If host name is empty, system name will be used to encode option 12. The length of system is more than 63, the superfluous chars will be truncated. If system name is also empty, then product model name will be used to encode option 12. |
| state | - Enables or disables insertion of option 12 in the DHCPDISCOVER and DHCPREQUEST message. The state is disable by default. |
| enable | - Enables insertion of option 12 in the DHCPDISCOVER and DHCPREQUEST message. |
| disable | - Disables 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-3000-26TC: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-3000-26TC:admin#
```

10-15 delete ipif

Description

This command is used to delete an IP interface.

Format

delete ipif [*<ipif_name 12>* {*ipv6address <ipv6networkaddr>*} | *all*]

Parameters

ipif - Specifies the name of the IP interface.

<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-3000-26TC:admin#delete ipif newone
Command: delete ipif newone

Success.

DGS-3000-26TC:admin#
```

10-16 enable ipif

Description

This commands is used to enable the IP interface.

Format

enable ipif [<ipif_name 12> | all]

Parameters

ipif_name - Specifies the name of the IP interface.
<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-3000-26TC:admin#enable ipif newone
Command: enable ipif newone

Success.

DGS-3000-26TC:admin#
```

10-17 disable ipif

Description

This command is used to disable an IP interface.

Format

disable ipif [<ipif_name 12> | all]

Parameters

ipif_name - Specifies the name of the IP interface.
<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-3000-26TC:admin#disable ipif newone
Command: disable ipif newone

Success.

DGS-3000-26TC:admin#
```

10-18 show ipif

Description

This command is used to display an IP interface.

Format

show ipif {<ipif_name 12>}

Parameters

ipif_name - Specifies the name of the IP interface.
<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-3000-26TC:admin#show ipif
Command: show ipif

IP Interface           : System
VLAN Name              : default
Interface Admin State  : Enabled
Link Status            : LinkUp
IPv4 Address           : 10.90.90.90/8 (Manual)
IPv4 State             : Enabled
IPv6 State             : Enabled
DHCP Option12 State    : Disabled
DHCP Option12 Host Name :

Total Entries: 1

DGS-3000-26TC:admin#
```

10-19 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 enable 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-3000-26TC:admin#enable ipif_ipv6_link_local_auto newone
Command: enable ipif_ipv6_link_local_auto newone

Success.

DGS-3000-26TC:admin#
```

10-20 disable ipif_ipv6_link_local_auto

Description

This command is used to disable the auto configuration of 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-3000-26TC:admin#disable ipif_ipv6_link_local_auto newone
Command: disable ipif_ipv6_link_local_auto newone

Success.

DGS-3000-26TC:admin#
```

10-21 show ipif_ipv6_link_local_auto

Description

This commands 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

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

Example

To display the link local address automatic configuration state.

```
DGS-3000-26TC:admin#show ipif_ipv6_link_local_auto
Command: show ipif_ipv6_link_local_auto

  IPIF: System           Automatic Link Local Address: Disabled

DGS-3000-26TC:admin#
```

Chapter 11 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>}}

```

11-1 config bpdu_protection ports

Description

This command is used to configure the BPD protection function for the ports on the Switch. In generally, there are two states in BPD protection function. One is normal state, and another is under attack state. The under attack state have three modes: drop, block, and shutdown. A BPD protection enabled port will enter under attack state when it receives one STP BPD packet. And it will take action based on the configuration. Thus, BPD protection can only be enabled on STP-disabled port.

BPD protection has high priority than fbpd setting configured by configure STP command in determination of BPD handling. That is, when fbpd is configured to forward STP BPD but BPD protection is enabled, then the port will not forward STP BPD.

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 the port will be configured.

state – (Optional) Specifies the BPD protection state. The default state is disable

enable – Specifies to enable BPD protection.

disable – Specifies to disable BPD protection.

mode – (Optional) Specifies the BPD protection mode. The default mode is shutdown

drop - Drops all received BPD packets when the port enters under_attack state.

block - Drops all packets including BPD and normal packets when the port enters under_attack state.

shutdown - Shuts 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-3000-26TC:admin#config bpdu_protection ports 1 state enable mode drop
Commands: config bpdu_protection ports 1 state enable mode drop

Success.

DGS-3000-26TC:admin#
```

11-2 config bpdu_protection recovery_interval

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

recovery_timer - Specifies the bpdu_protection Auto-Recovery recovery_timer. The default value of recovery_timer is 60.
<sec 60 –1000000> - The timer (in seconds) used by the Auto-Recovery mechanism to recover the port. The valid range is 60 to 1000000.
infinite - The port will not be auto recovered.

Restrictions

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

Example

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

```
DGS-3000-26TC:admin#config bpdu_protection recovery_timer 120
Commands: config bpdu_protection recovery_timer 120

Success.

DGS-3000-26TC:admin#
```

11-3 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 - Neither attack_detected nor attack_cleared is trapped or logged.

attack_detected - Events will be logged or trapped when the BPDU attacks is detected.

attack_cleared - Events will be logged or trapped when the BPDU attacks is cleared.

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

```
DGS-3000-26TC:admin#config bpdu_protection trap both
Commands: config bpdu_protection trap both

Success.

DGS-3000-26TC:admin#
```

11-4 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 for the entire switch:

```
DGS-3000-26TC:admin#enable bpdu_protection
Commands: enable bpdu_protection

Success.

DGS-3000-26TC:admin#
```

11-5 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 for the entire switch:

```
DGS-3000-26TC:admin#disable bpdu_protection
Commands: disable bpdu_protection

Success.

DGS-3000-26TC:admin#
```

11-6 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 - Specifies a range of ports to be configured.
<portlist> - Enter the portlist here.

Restrictions

None.

Example

To show the bpdu_protection for the entire switch:

```
DGS-3000-26TC: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-3000-26TC:admin#
```

To show the bpdu_protection status ports 1-12:

```
DGS-3000-26TC: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-3000-26TC:admin#
```

Chapter 12 Cable Diagnostics

Command List

cable_diag ports [<portlist> | all]

12-1 cable_diag ports

Description

This command is used to configure cable diagnostics on ports. For FE port, two pairs of cable will be diagnosed. For GE port, 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 **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

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-3000-26TC: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-3000-26TC:admin#
```

Chapter 13 Command Logging

Command List

enable command logging
disable command logging
show command logging

13-1 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 be 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-3000-26TC:admin#enable command logging
Command: enable command logging

Success.

DGS-3000-26TC:admin#
```

13-2 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-3000-26TC:admin#disable command logging
Command: disable command logging

Success.

DGS-3000-26TC:admin#
```

13-3 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-3000-26TC:admin#show command logging
Command: show command logging

Command Logging State : Disabled

DGS-3000-26TC:admin#
```

Chapter 14 Compound Authentication Command List

| |
|---|
| enable authorization attributes |
| disable authorization attributes |
| show authorization |
| config authentication server failover [local permit block] |
| show authentication |

14-1 enable authorization

Description

This command is used to enable authorization. When authorization for attributes is enabled, the authorized attributes (for example VLAN, 802.1p default priority, and ACL) assigned by the RADIUS server or local database, will be accepted depending on the individual module's settings. Authorization for attributes is enabled by default.

Format

enable authorization attributes

Parameters

None.

Restrictions

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

Example

This example sets authorization global state enabled:

```
DGS-3000-26TC:admin#enable authorization attributes
Command: enable authorization attributes

Success.

DGS-3000-26TC:admin#
```

14-2 disable authorization

Description

This command is used to disable authorization. When authorization for attributes is disabled, the authorized attributes (for example VLAN, 802.1p default priority, and ACL) assigned by the

RADIUS server or local database, will be ignored even if the individual module's setting is enabled. Authorization for attributes is enabled by default.

Format

disable authorization attributes

Parameters

None.

Restrictions

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

Example

This example sets authorization global state disabled:

```
DGS-3000-26TC:admin#disable authorization attributes
Command: disable authorization attributes

Success.

DGS-3000-26TC:admin#
```

14-3 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-3000-26TC:admin#show authorization
Command: show authorization

Authorization for Attributes: Enabled.

DGS-3000-26TC:admin#
```

14-4 config authentication server failover

Description

This command is used to configure authentication server failover function.

Format

config authentication server failover [local | permit | block]

Parameters

local - Uses local DB to authenticate the client.
permit - The client is always regarded as authenticated.
block - Blocks the client. This is the default.

Restrictions

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

Example

Set authentication server auth fail over state:

```
DGS-3000-26TC:admin#config authentication server failover local
Command: config authentication server failover local

Success.

DGS-3000-26TC:admin#
```

14-5 show authentication

Description

This command is used to display the authentication server failover configuration.

Format

show authentication

Parameters

None.

Restrictions

None.

Example

To show authentication global configuration:

```
DGS-3000-26TC:admin#show authentication
Command: show authentication

Authentication Server Failover: Local.

DGS-3000-26TC:admin#
```

Chapter 15 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
```

15-1 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 - Shows commands which only affects the behavior of the device. For example, if STP is disabled, only "STP is disabled" is displayed for STP configuration. All other lower level

setting regarding STP is not displayed. The lower level setting will only be displayed when the higher level setting is enabled.

Note: This parameter is only for the current configuration.

modified - Shows only the commands which are not default setting.

Note: 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> - Specifies an absolute pathname on the device file system. If pathname is not specified, the boot up configuration is implied. This name can be up to 64 characters long.

include - (Optional) Includes lines that contain the specified filter string.

exclude - (Optional) Excludes lines that contain the specified filter string.

begin - (Optional) The first line that contains the specified filter string will be the first line of the output.

<filter_string 80> - A filter string is enclosed by 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) A filter string is enclosed by 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) A filter string is enclosed by 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) Includes lines that contain the specified filter string.

exclude - (Optional) Excludes lines that contain the specified filter string.

begin - (Optional) The first line that contains the specified filter string will be the first line of the output.

<filter_string 80> - A filter string is enclosed by 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) A filter string is enclosed by 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) A filter string is enclosed by 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) Includes lines that contain the specified filter string.

exclude - (Optional) Excludes lines that contain the specified filter string.

begin - (Optional) The first line that contains the specified filter string will be the first line of the output.

<filter_string 80> - A filter string is enclosed by 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) A filter string is enclosed by 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) A filter string is enclosed by 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.

Restrictions

Only Administrators can issue this command.

Example

The following example illustrates how the special filters, 'modified', affect the configuration display:

```

DGS-3000-26TC:admin#show config modified
Command: show config modified

#-----
#
#           DGS-3000-26TC Gigabit Ethernet Switch
#           Configuration
#
#           Firmware: Build 1.00.015
#           Copyright(C) 2013 D-Link Corporation. All rights reserved.
#-----

# DEVICE

# BASIC

# ACCOUNT LIST
create account admin admin
admin
admin

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

```

15-2 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-3000-26TC:admin#config configuration config.cfg boot_up
Command: config configuration config.cfg boot_up

Success.
DGS-3000-26TC:admin#
```

15-3 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> - Specifies 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-3000-26TC:admin#save config c:/3000.cfg
Command: save config c:/3000.cfg

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

DGS-3000-26TC:admin#
```

15-4 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-3000-26TC:admin#show boot_file
Command: show boot_file

  Bootup Firmware      : /c:/runtime.had
  Bootup Configuration : /c:/config.cfg

DGS-3000-26TC:admin#
```

Chapter 16 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]}
```

16-1 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-3000-26TC:admin#create cfm md op_domain level 2
Command: create cfm md op_domain level 2

Success.

DGS-3000-26TC:admin#
```

16-2 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 to configure MIPs. |
| none - Specifies not to create MIPs. This is the default value. |
| auto - 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 - 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 - Transmits the sender ID TLV with the chassis ID information. |
| manage - Transmits the sender ID TLV with the managed address information. |
| chassis_manage - Transmits 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-3000-26TC:admin#config cfm md op_domain mip explicit
Command: config cfm md op_domain mip explicit

Success.

DGS-3000-26TC:admin#
```

16-3 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-3000-26TC:admin#create cfm ma op1 md op_domain
Command: create cfm ma op1 md op_domain

Success.

DGS-3000-26TC:admin#
```

16-4 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 to configure MIPs.

none - Specifies not to create MIPs.

auto - MIPs can always be created on any ports in this MA, if that port is not configured with an MEP of that MA.

explicit - 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 - Inherit the setting configured for the maintenance domain that this MA is associated with. This is the default value.

sender_id - (Optional) This is the control transmission of the sender ID TLV.

none - Specifies not to transmit the sender ID TLV. This is the default value.

chassis - Transmits the sender ID TLV with the chassis ID information.

manage - Transmits the sender ID TLV with the manage address information.

chassis_manage - Transmits the sender ID TLV with the chassis ID information and the manage address information.

defer - Inherits 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-3000-26TC: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-3000-26TC:admin#
```

16-5 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 that together identify a 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-3000-26TC:admin#create cfm mep mep1 mepid 1 md op_domain ma opl direction
inward port 2
Command: create cfm mep mep1 mepid 1 md op_domain ma opl direction inward port
2
Success.
DGS-3000-26TC:admin#
```

16-6 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) The 802.1p priority is set in the CCMs and the 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 - All types of fault alarms will be sent.

mac_status - Only the fault alarms whose priority is equal to or higher than "Some Remote MEP MAC Status Errors" are sent.

remote_ccm - Only the fault alarms whose priority is equal to or higher than "Some Remote MEPs Down" are sent.

error_ccm - Only the fault alarms whose priority is equal to or higher than "Error CCM Received" are sent.

xcon_ccm - Only the fault alarms whose priority is equal to or higher than "Cross-connect CCM Received" are sent.

none - 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 range is 250-1000. 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 range is 250-1000. 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-3000-26TC:admin#config cfm mep mepname mep1 state enable ccm enable
Command: config cfm mep mepname mep1 state enable ccm enable

Success.

DGS-3000-26TC:admin#
```

16-7 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-3000-26TC:admin#delete cfm mep mepname mep1
Command: delete cfm mep mepname mep1

Success.

DGS-3000-26TC:admin#
```

16-8 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-3000-26TC:admin#delete cfm ma op1 md op_domain
Command: delete cfm ma op1 md op_domain

Success.

DGS-3000-26TC:admin#
```


16-9 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-3000-26TC:admin#delete cfm md op_domain
Command: delete cfm md op_domain

Success.

DGS-3000-26TC:admin#
```

16-10 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-3000-26TC:admin#enable cfm
Command: enable cfm

Success.

DGS-3000-26TC:admin#
```

16-11 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-3000-26TC:admin#disable cfm
Command: disable cfm

Success.

DGS-3000-26TC:admin#
```

16-12 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 Link trace 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 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-3000-26TC:admin#config cfm ports 2-5 state enable
Command: config cfm ports 2-5 state enable

Success.

DGS-3000-26TC:admin#
```

16-13 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-3000-26TC:admin#show cfm ports 3-6
Command: show cfm ports 3-6

Port   State
-----  -----
3      Enabled
4      Enabled
5      Enabled
6      Disabled

DGS-3000-26TC:admin#
```

16-14 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 - (Optional) 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 - (Optional) 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-3000-26TC:admin#show cfm
Command: show cfm
```

CFM State: Enabled

| MD Index | MD Name | Level |
|----------|-----------|-------|
| 1 | op_domain | 2 |

DGS-3000-26TC: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-3000-26TC: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-3000-26TC: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-3000-26TC:admin#

```

16-15 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** - (Optional) 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** - (Optional) 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-3000-26TC:admin#show cfm fault
Command: show cfm fault

MD Name      MA Name      MEPID  Status
-----
op_domain    op1          1      Cross-connect CCM Received

DGS-3000-26TC:admin#
```

16-16 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.
inward - Specifies that the MEP direction will be inward facing.
outward - Specifies that the MEP direction will be outward facing.
 If not specified, both directions and the MIP are shown.

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-3000-26TC: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-3000-26TC:admin#
```

16-17 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 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-3000-26TC: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-3000-26TC:admin#

```

16-18 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 her. 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 her. 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 link trace message TTL value. The default value is 64. |
| <int 2-255> | - Enter the link trace message TTL value here. This value must be between 2 and 255. |
| pdu_priority | - (Optional) 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-3000-26TC: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-3000-26TC:admin#
```

16-19 show cfm linktrace

Description

This command is used to show the link trace responses. The maximum link trace responses a device can hold 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 her. 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 her. 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 show the link trace reply when the "all MPs reply LTRs" function is enabled:

```
DGS-3000-26TC:admin#show cfm linktrace mepid 5 md md6 ma ma1 trans_id 30
Command: show cfm linktrace mepid 5 md md6 ma ma1 trans_id 30

Transaction ID: 30
From MEP mep5 to 30-00-26-81-34-A2
Start Time      : 2013-01-31 14:47:36

Hop  MEPID  MAC Address          Forwarded  Relay Action
---  -      -                  -          -
1    -      30-00-26-81-34-19  Yes        FDB
2    -      30-00-26-81-34-B8  No         Hit

DGS-3000-26TC:admin#"
```

To show the link trace reply when the "all MPs reply LTRs" function is disabled:

```
DGS-3000-26TC: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-3000-26TC:admin#"
```

16-20 delete cfm linktrace

Description

This command is used to delete the stored link trace response 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 link trace reply:

```
DGS-3000-26TC:admin#delete cfm linktrace mepname mep1
Command: delete cfm linktrace mepname mep1

Success.

DGS-3000-26TC:admin#
```

16-21 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-3000-26TC: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-3000-26TC:admin#
```

16-22 config cfm mp_ltr_all

Description

This command is used to enable or disable the "all MPs reply LTRs" function.

Format

config cfm mp_ltr_all [enable | disable]

Parameters

enable - Specifies that the MP's reply to the LTR function will be set to all.

disable - Disables sending the all MPs replay LTRs function.

Restrictions

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

Example

To enable the "all MPs reply LTRs" function:

```
DGS-3000-26TC:admin#config cfm mp_ltr_all enable
Command: config cfm mp_ltr_all enable

Success.

DGS-3000-26TC:admin#
```

16-23 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-3000-26TC:admin#show cfm mp_ltr_all
Command: show cfm mp_ltr_all

All MPs reply LTRs: Disabled

DGS-3000-26TC:admin#
```

16-24 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 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.**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-3000-26TC: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
Port Status Defect     : Blocked
Interface Status       : Down
Interface Status Defect : No
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-3000-26TC:admin#

```

16-25 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-3000-26TC:admin#show cfm pkt_cnt
Command: show cfm pkt_cnt

```

| CFM RX Statistics | | | | | | | | |
|-------------------|--------|-----|-----|-----|-----|-----|---------|----------|
| Port | AllPkt | CCM | LBR | LBM | LTR | LTM | VidDrop | OpcoDrop |
| all | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 0 | 0 | 0 | 0 | 0 | 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 |

| CFM TX Statistics | | | | | | |
|-------------------|--------|-----|-----|-----|-----|-----|
| Port | AllPkt | CCM | LBR | LBM | LTR | LTM |
| all | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 0 | 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

DGS-3000-26TC: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
-----
DGS-3000-26TC:admin#

```

16-26 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-3000-26TC:admin#clear cfm pkt_cnt
Command: clear cfm pkt_cnt

Success.

DGS-3000-26TC:admin#clear cfm pkt_cnt ccm
Command: clear cfm pkt_cnt ccm

Success.

DGS-3000-26TC:admin#
```

Chapter 17 CPU Interface Filtering Command List

```
create cpu access_profile profile_id <value 1-5> [ethernet {vlan | source_mac <macmask 000000000000-ffffffff> | destination_mac <macmask 000000000000-ffffffff> | 802.1p | ethernet_type} | ip {vlan | source_ip_mask <netmask> | destination_ip_mask <netmask> | dscp | [icmp {type | code} | igmp {type} | tcp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff> | flag_mask [all | {urg | ack | psh | rst | syn | fin}]} | udp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff> | protocol_id_mask <hex 0x0-0xff> {user_define_mask <hex 0x0-0xffffffff>}}] | packet_content_mask {offset_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 0x0-0xffff> | 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>}
```

17-1 create cpu access_profile

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-ffffffff> | destination_mac <macmask 000000000000-ffffffff> | 802.1p | ethernet_type} | ip {vlan | source_ip_mask <netmask> | destination_ip_mask <netmask> | dscp | [icmp {type | code} | igmp {type} | tcp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff> | flag_mask [all | {urg | ack | psh | rst | syn | fin}]} | udp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | protocol_id_mask <hex 0x0-0xff> {user_define_mask <hex 0x0-0xffffffff>}}] | packet_content_mask {offset_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

-
- profile_id** - Specifies the profile ID used here.
<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 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 eighty bytes of 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 flowlabel.

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-3000-26TC: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-3000-26TC: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-3000-26TC:admin#
```

17-2 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-3000-26TC:admin#delete cpu access_profile profile_id 1
Command: delete cpu access_profile profile_id 1

Success.

DGS-3000-26TC:admin#
```

17-3 config cpu access_profile

Description

This command is used to configure 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 0x0-0xffff> | source_ipv6 <ipv6addr> | destination_ipv6 <ipv6addr>}] port [<portlist> | all] [permit | deny] {time_range <range_name 32>} | delete access_id <value 1-100>]
```

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.

add - Specifies that a profile or a rule will be added.

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.
- 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 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 eighty bytes of 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 flowlabel.

<hex 0x0-0xffff> - Enter the IPv6 flowlabel 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 the packets that match the access profile are permit by the Switch.

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

time_range - (Optional) Specifies 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-3000-26TC: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-3000-26TC:admin#
```

17-4 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-3000-26TC:admin#enable cpu_interface_filtering
Command: enable cpu_interface_filtering

Success.

DGS-3000-26TC:admin#
```

17-5 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-3000-26TC:admin#disable cpu_interface_filtering
Command: disable cpu_interface_filtering

Success.

DGS-3000-26TC:admin#
```

17-6 show cpu access_profile

Description

This command is used to display current access list table.

Format

show cpu access_profile {profile_id <value 1-5>}

Parameters

profile_id - (Optional) Specifies the index of 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-3000-26TC: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-3000-26TC:admin#
```

Chapter 18 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]

debug config error_reboot [enable | disable]

debug config state [enable | disable]

debug show error_reboot state

debug show status {module <module_list>}

18-1 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 - Displays the debug message of the debug log.

clear - Clears the debug log.

upload_toTFTP - Specifies to upload the debug log to a TFTP server specified by IP address.

<ipaddr> - (Optional) Specifies the IPv4 address of the TFTP server.

<path_filename 64> - (Optional) Specifies 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-3000-26TC:admin#debug error_log dump
Command: debug error_log dump

*****
# debug log: 1
# level: fatal
# clock: 1000ms
# 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-3000-26TC:admin#debug error_log clear
Command: debug error_log clear

Success.

DGS-3000-26TC:admin#
```

To upload the error log to TFTP server:

```
DGS-3000-26TC: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-3000-26TC:admin#
```

18-2 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 - Displays the debug buffer's state.

dump - Displays the debug message in the debug buffer.

clear - Clears the debug buffer.

upload_toTFTP - Specifies to upload the debug buffer to a TFTP server specified by IP address.

<ipaddr> - Specifies the IPv4 address of the TFTP server.

<path_filename 64> - Specifies 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 Administrator users can issue this command.

Example

To show the debug buffer's state:

```
DGS-3000-26TC:admin#debug buffer utilization
Command: debug buffer utilization

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

DGS-3000-26TC:admin#
```

To clear the debug buffer:

```
DGS-3000-26TC:admin#debug buffer clear
Command: debug buffer clear

Success.

DGS-3000-26TC:admin#
```

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

```
DGS-3000-26TC: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-3000-26TC:admin#
```

18-3 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]

Parameters

module - Specifies the module list.

<module_list> - Enter the module list here.

all - Controls output method of all modules.

buffer - Directs the debug message of the module output to debug buffer. This is the default.

console - Directs the debug message of the module output to local console.

Restrictions

Only Administrators can issue this command.

Example

To set all module debug message outputs to local console:

```
DGS-3000-26TC:admin#debug output all console
```

```
Command: debug output all console
```

```
Success.
```

```
DGS-3000-26TC:admin#
```

18-4 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 - If enabled, the Switch will reboot when a fatal error happens.

disable - If disabled 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 need a reboot when a fatal error occurs:

```
DGS-3000-26TC:admin#debug config error_reboot disable
Command: debug config error_reboot disable

Success.

DGS-3000-26TC:admin#
```

18-5 debug config state

Description

This command is used to set the state of the debug.

Format

debug config state [enable | disable]

Parameters

enable - Enables the debug state.
disable - Disables the debug state.

Restrictions

Only Administrators can issue this command.

Example

To set the debug state to disabled:

```
DGS-3000-26TC:admin#debug config state disable
Command: debug config state disable

Success.

DGS-3000-26TC:admin#
```

18-6 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-3000-26TC:admin#debug show error_reboot state
Command: debug show error_reboot state

Error Reboot: Enabled

DGS-3000-26TC:admin#
```

18-7 debug show status

Description

This command is used to display the debug handler state and 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-3000-26TC:admin#debug show status module MSTP
Command: debug show status module MSTP

Debug Global State   : Enabled

MSTP                  : Disabled

DGS-3000-26TC:admin#
```

To show the debug state:

```
DGS-3000-26TC:admin#debug show status
Command: debug show status

Debug Global State   : Enabled

MSTP                  : Disabled
IMPB                  : Disabled
ERPS                  : Disabled

DGS-3000-26TC:admin#
```

Chapter 19 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>}

```

19-1 config dhcp_local_relay vlan

Description

This command is used to enable or disable DHCP local relay function for specified VLAN name.

When DHCP local relay is enabled for the VLAN, the DHCP packet will be relayed in broadcast way without change of the source MAC address and gateway address. DHCP option 82 will be automatically added.

Format

```
config dhcp_local_relay vlan <vlan_name 32> state [enable | disable]
```

Parameters

```

<vlan_name 32> - Specifies the VLAN name. This name can be up to 32 characters long.
state - Enables or disables DHCP local relay for specified vlan.
  enable - Specifies to enable the DHCP local relay function.
  disable - Specifies to disable the DHCP local relay function.

```

Restrictions

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

Example

To enable DHCP local relay for default VLAN:

```

DGS-3000-26TC:admin#config dhcp_local_relay vlan default state enable
Command: config dhcp_local_relay vlan default state enable

Success.

DGS-3000-26TC:admin#

```

19-2 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.

<vlan_id> - Enter the VLAN ID used here.

state - Enables or disables 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 default VLAN:

```
DGS-3000-26TC:admin#config dhcp_local_relay vlan vlanid 1 state enable
Command: config dhcp_local_relay vlan vlanid 1 state enable

Success.

DGS-3000-26TC:admin#
```

19-3 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 DHCP relay agent to default.

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 of DHCP relay agent as default:

```
DGS-3000-26TC:admin#config dhcp_local_relay option_82 circuit_id default
Command: config dhcp_local_relay option_82 circuit_id default

Success.

DGS-3000-26TC:admin#
```

19-4 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> - Specifies 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-3000-26TC: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-3000-26TC:admin#
```

19-5 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 - Uses the Switch's system MAC address as the remote ID.

user_define - Uses user-defined string as the remote ID.

<desc 32> - Enter the maximum of 32 characters. Space is allowed in the string.

Restrictions

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

Example

To configure the remote ID:

```
DGS-3000-26TC:admin#config dhcp_local_relay option_82 remote_id user_define D-Link L2Switch
Command: config dhcp_local_relay option_82 remote_id user_define D-Link L2Switch

Success.

DGS-3000-26TC:admin#
```

19-6 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-3000-26TC:admin#enable dhcp_local_relay
Command: enable dhcp_local_relay

Success.

DGS-3000-26TC:admin#
```

19-7 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-3000-26TC:admin#disable dhcp_local_relay
Command: disable dhcp_local_relay

Success.

DGS-3000-26TC:admin#
```

19-8 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 local dhcp relay status:

```
DGS-3000-26TC: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-3000-26TC:admin#
```

19-9 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) Specifies a list of ports to be displayed.

Restrictions

None.

Example

To display DHCP local relay option 82 configuration of port 1 to 5:

```
DGS-3000-26TC: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-3000-26TC:admin#
```


Chapter 20 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>]}
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
config dhcp_relay ports [<portlist> | all] state [enable | disable]
show dhcp_relay ports {<portlist>}

```

20-1 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-3000-26TC:admin#config dhcp_relay hops 4 time 2
Command: config dhcp_relay hops 4 time 2

Success.

DGS-3000-26TC:admin#
```

20-2 config dhcp_relay add

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 - The name of the IP interface which contains the IP address below.
<ipif_name 12> - Enter the IP interface name used here. This name can be up to 12 characters long.
<ipaddr> - 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-3000-26TC:admin#config dhcp_relay add ipif System 10.43.21.12
Command: config dhcp_relay add ipif System 10.43.21.12

Success.

DGS-3000-26TC:admin#
```

20-3 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

vlanid - Specifies the VLAN ID list used for this configuration.
<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-3000-26TC: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-3000-26TC:admin#
```

To display the DHCP relay status:

```
DGS-3000-26TC:admin#show dhcp_relay
Command: show dhcp_relay

DHCP/BOOTP Relay Status      : Disabled
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 : Disabled
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 : 00-01-02-03-04-00

Interface      Server 1      Server 2      Server 3      Server 4
-----
Server          VLAN ID List
-----
10.43.21.12    1-10

DGS-3000-26TC:admin#
```

20-4 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 - The name of the IP interface which contains the IP address below.
<ipif_name 12> - Enter the IP interface name used here. This name can be up to 12 characters long.
<ipaddr> - 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-3000-26TC:admin#config dhcp_relay delete ipif System 10.43.21.12
Command: config dhcp_relay delete ipif System 10.43.21.12

Success.

DGS-3000-26TC:admin#
```

20-5 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

vlanid - Specifies the VLAN ID list used for this configuration.
<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-3000-26TC: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-3000-26TC:admin#
```

20-6 config dhcp_relay option_82

Description

This command is used to configure the processing of DHCP 82 option 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>]}

Parameters

state - (Optional) When the state is enabled, the DHCP packet will be inserted with the option 82 field before being relayed to server. The DHCP packet will be processed based on the behaviour defined in check and policy setting. When the state is disabled, the DHCP packet will be relayed directly to server without further check and processing on the packet. The default setting is disabled.

enable - Specifies that the option 82 processing will be enabled.

disable - Specifies that the option 82 processing will be disabled.

check - (Optional) When the state is enabled, For packet come from client side, the packet should not have the option 82's field. If the packet has this option field, it will be dropped. The default setting is disabled.

enable - Specifies that checking will be enabled.

disable - Specifies that checking will be disabled.

policy - (Optional) 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 it's 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 and Option 82 value, then the packet will be dropped. If the packet, that comes from the client side doesn't contain an Option 82 value, then insert it's 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 and Option 82 value, then keep the old Option 82 value. If the packet, that comes from the client side, doesn't contain an Option 82 value, then insert it's own Option 82 value into the packet.

remote_id - (Optional) Specifies the content in Remote ID suboption.

default - Uses switch's system MAC address as remote ID.

user_define - Uses user-defined string as remote ID. The space character is 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-3000-26TC:admin#config dhcp_relay option_82 state enable
Command: config dhcp_relay option_82 state enable

Success.

DGS-3000-26TC:admin#config dhcp_relay option_82 check disable
Command: config dhcp_relay option_82 check disable

Success.

DGS-3000-26TC:admin#config dhcp_relay option_82 policy replace
Command: config dhcp_relay option_82 policy replace

Success.

DGS-3000-26TC: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-3000-26TC:admin#
```

20-7 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.

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-3000-26TC:admin#config dhcp_relay option_82 circuit_id default
Command: config dhcp_relay option_82 circuit_id default

Success.

DGS-3000-26TC:admin#
```

20-8 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-3000-26TC:admin#enable dhcp_relay
Command: enable dhcp_relay

Success.

DGS-3000-26TC:admin#
```

20-9 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-3000-26TC:admin#disable dhcp_relay
Command: disable dhcp_relay

Success.

DGS-3000-26TC:admin#
```

20-10 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 system will display all DHCP relay configuration.

Restrictions

None.

Example

To display DHCP relay configuration:


```
DGS-3000-26TC:admin#show dhcp_relay ipif System
Command: show dhcp_relay ipif System

DHCP/BOOTP Relay Status      : Enabled
DHCP/BOOTP Hops Count Limit  : 4
DHCP/BOOTP Relay Time Threshold : 2
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 : "D-Link L2 Switch"

Interface      Server 1      Server 2      Server 3      Server 4
-----
System         10.43.21.12

DGS-3000-26TC:admin#
```

20-11 config dhcp_relay option_60

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 per IPIF configured servers will be ignored.

If the relay servers are not determined either by option 60 or option 61, then per IPIF configured servers will be used to determine the relay servers.

Format

config dhcp_relay option_60 state [enable | disable]

Parameters

-
- state** - Specifies that the DHCP relay function should use the option 60 rule to relay the DHCP packets.
 - 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-3000-26TC:admin#config dhcp_relay option_60 state enable
Command: config dhcp_relay option_60 state enable

Success

DGS-3000-26TC:admin#
```

20-12 config dhcp_relay option_60 add

Description

This command is used to configure the option 60 relay rules. Note that different string can be specified with the same relay server, and the same string can be specified with multiple relay servers.

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

string - Specifies the string used.

<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 - The option 60 string in the packet must full match with the specified string.

partial-match - The option 60 string in the packet only need 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-3000-26TC: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-3000-26TC:admin#
```

20-13 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 there is no matching found for the packet, the relay servers will be determined based on the default relay servers.

When drop is specified, the packet with no matching rules found will be dropped without further process.

If the setting is no- drop, then the packet will be processed further based on option 61. The final relay servers will be the union of option 60 default relay servers and the relay servers determined by option 61.

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 to relay the packet 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-3000-26TC:admin#config dhcp_relay option_60 default mode drop
Command: config dhcp_relay option_60 default mode drop

Success.

DGS-3000-26TC:admin#
```

20-14 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 - Deletes all the entries, of which the string is equal to the specified string, 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) Deletes one entry, of which the string and the 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 - Deletes all the entry of which the IP address is equal to the specified IP address.

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

all - Deletes all the entry. Default relay servers are excluded.

default - Deletes 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-3000-26TC: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-3000-26TC:admin#
```

20-15 show dhcp_relay option_60

Description

This command is used to show DHCP relay Option 60 entry specified by the user.

Format

```
show dhcp_relay option_60 {[string <multiword 255> | ipaddress <ipaddr> | default]}
```

Parameters

string - (Optional) Displays the DHCP relay Option 60 string specified by the user.

<multiword 255> - Enter the entry's string value here. This value can be up to 255 characters long.

ipaddress - (Optional) Displays the IP address specified by the user.

<ipaddr> - Enter the IP address here.

default - (Optional) Displays the default DHCP relay Option 60 information.

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-3000-26TC: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-3000-26TC:admin#
```

20-16 config dhcp_relay option_61

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 per IPIF configured servers will be ignored.

If the relay servers are not determined either by option 60 or option 61, then per IPIF configured servers will be used to determine the relay servers.

Format

config dhcp_relay option_61 state [enable | disable]

Parameters

state - Specifies whether the DHCP relay option 61 is enabled or disabled.

enable - Enables the function DHCP relay use option 61 ruler to relay DHCP packet.

disable - Disables the function DHCP relay use option 61 ruler to relay DHCP packet.

Restrictions

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

Example

To configure the state of dhcp_relay option 61:

```
DGS-3000-26TC:admin#config dhcp_relay option_61 state enable
Command: config dhcp_relay option_61 state enable

Success

DGS-3000-26TC:admin#
```

20-17 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 base on either MAC address or a user-specified string. Only one relay server can be specified for a MAC-address or a string.

If relay servers are determined based on option 60, and one relay server is determined based on option 61, the final relay servers will be the union of these two sets of the servers.

Format

config dhcp_relay option_61 add [mac_address <macaddr> | string <multiword 255>] [relay <ipaddr> | drop]

Parameters

mac_address - The client's client-ID which is the hardware address of client.

<macaddr> - Enter the client's MAC address here.

string - The client's client-ID, which is specified by 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 a 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-3000-26TC: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-3000-26TC:admin#
```

20-18 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 matching 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-3000-26TC:admin#config dhcp_relay option_61 default drop
Command: config dhcp_relay option_61 default drop

Success

DGS-3000-26TC:admin#
```

20-19 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 - The entry with the specified MAC address will be deleted.

<macaddr> - Enter the MAC address here.

string - 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 - 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-3000-26TC: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-3000-26TC:admin#
```

20-20 show dhcp_relay option_61

Description

This command is used to show all rulers for option 61.

Format

show dhcp_relay option_61

Parameters

None.

Restrictions

None.

Example

To display DHCP relay rulers for option 61:


```

DGS-3000-26TC: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-3000-26TC:admin#

```

20-21 config dhcp_relay ports

Description

This command is used to configure the DHCP relay of the ports.

Format

config dhcp_relay ports [<portlist> | all] state [enable | disable]

Parameters

<portlist> - Specifies a list of ports to be configured.

all - Specifies all ports to be configured.

state - Specifies the DHCP relay state of the ports.

enable - Enables the DHCP relay.

disable - Disables the DHCP relay.

Restrictions

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

Example

To enable the DCHP relay on port 1-3:

```

DGS-3000-26TC:admin#config dhcp_relay ports 1-3 state enable
Command: config dhcp_relay ports 1-3 state enable

Success.

DGS-3000-26TC:admin#

```

20-22 show dhcp_relay ports

Description

This command is used to display the DHCP relay of each port.

Format

show dhcp_relay ports {<portlist>}

Parameters

<portlist> - (Optional) Specifies a list of ports to be displayed.

Restrictions

None.

Example

To display the DHCP relay state of port 1-10:

```
DGS-3000-26TC:admin#show dhcp_relay ports 1-10
Command: show dhcp_relay ports 1-10

Port  State
-----
1     Enabled
2     Enabled
3     Enabled
4     Enabled
5     Enabled
6     Enabled
7     Enabled
8     Enabled
9     Enabled
10    Enabled

DGS-3000-26TC:admin#
```

Chapter 21 DHCP Server Screening Command List

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

```
show filter dhcp_server
```

21-1 config filter dhcp_server

Description

This command is used to configure DHCP server screening.

With DHCP server screening function, illegal DHCP server packet will be filtered. This command is used to configure the state of the function for filtering of DHCP server packet and to add/delete the DHCP server 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 three purposes: (1) To specify to filter all DHCP server packets on the specific port, (2) to specify to allow some DHCP server packets with pre-defined server IP addresses and (3) to deny all DHCP OFFER requests by using the default DHCP Server Screening method to specify explicit "permit" rules for the 3-tuple (DHCP server IP, client's MAC address, and port list from the DHCP server). 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] state [enable | disable] | illegal_server_log_suppress_duration
  [1min | 5min | 30min] | trap_log [enable | disable]]
```

Parameters

```
add permit - Specifies to add a DHCP permit.
server_ip - The IP address of the DHCP server to be filtered.
  <ipaddr> - Enter the DHCP server IP address here.
client_mac - (Optional) The MAC address of the DHCP client.
  <macaddr> - Enter the DHCP client MAC address here.
ports - 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 permit - Specifies to delete a DHCP permit. |
| server_ip - The IP address of the DHCP server to be filtered. |
| <ipaddr> - Enter the DHCP server IP address here. |
| client_mac - (Optional) The MAC address of the DHCP client. |
| <macaddr> - Enter the DHCP client MAC address here. |
| ports - 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. |
| 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_log - Specifies to enable or disable the trap and log function. |
| enable - Enables the trap and log function. |
| disable - Disables the trap and 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-3000-26TC:admin#config filter dhcp_server add permit server_ip 10.90.90.20
ports 1-20
Command: config filter dhcp_server add permit server_ip 10.90.90.20 ports 1-20

Success.

DGS-3000-26TC:admin#
```

```
DGS-3000-26TC:admin#config filter dhcp_server ports 1-10 state enable
Command: config filter dhcp_server ports 1-10 state enable

Success.

DGS-3000-26TC:admin#
```

```
DGS-3000-26TC: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 port 1-26

Success.

DGS-3000-26TC:admin#
```

21-2 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

Parameters

None.

Restrictions

None.

Example

To display the DHCP server/client filter list created on the Switch:

```
DGS-3000-26TC:admin#show filter dhcp_server
Command: show filter dhcp_server

Enabled Ports: 1-10
Trap & Log State: Disabled
Illegal Server Log Suppress Duration:5 minutes

Permit DHCP Server/Client Table:
Server IP Address Client MAC Address  Port
-----
10.90.90.20      All Client MAC      1-20

Total Entries: 1

DGS-3000-26TC:admin#
```

Chapter 22 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]

22-1 config ddm

Description

The command configures the DDM log and trap action 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-3000-26TC:admin#config ddm log enable
Command: config ddm log enable

Success.

DGS-3000-26TC:admin#
```

To configure DDM trap state to enable:

```
DGS-3000-26TC:admin#config ddm trap enable
Command: config ddm trap enable

Success.

DGS-3000-26TC:admin#
```

22-2 config ddm ports

Description

The 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. At least one parameter shall be specified for this threshold. |
| 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 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 shutdown the port when the operating parameter exceeds the corresponding alarm threshold or warning threshold. The default value is none. alarm - Shuts down the port when the configured alarm threshold range is exceeded. warning - Shuts 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 the port 25's temperature threshold:

```
DGS-3000-26TC: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-3000-26TC:admin#
```

To configure the port 25's voltage threshold:

```
DGS-3000-26TC: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-3000-26TC:admin#
```

To configure the port 25's bias current threshold:

```
DGS-3000-26TC: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-3000-26TC:admin#
```

To configure the port 25's transmit power threshold:

```
DGS-3000-26TC: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-3000-26TC:admin#
```

To configure the port 25's receive power threshold:


```
DGS-3000-26TC: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-3000-26TC:admin#
```

To configure the port 25's actions associate with the alarm:

```
DGS-3000-26TC:admin#config ddm ports 25 state enable shutdown alarm
Command: config ddm ports 25 state enable shutdown alarm

Success.

DGS-3000-26TC:admin#
```

22-3 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-3000-26TC:admin#show ddm
Command: show ddm

DDM Log           :Enabled
DDM Trap          :Disabled

DGS-3000-26TC:admin#
```

22-4 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-3000-26TC:admin#show ddm ports 25-26 status
```

```
Command: show ddm ports 25-26 status
```

| Port | Temperature (in Celsius) | Voltage (V) | Bias Current (mA) | TX Power (mW) | RX Power (mW) |
|------|-----------------------------|----------------|----------------------|------------------|------------------|
| 25 | - | - | - | - | - |
| 26 | - | - | - | - | - |

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

Chapter 23 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)
show duld ports {<portlist>}
```

23-1 config duld ports

Description

The command is used to configure unidirectional link detection on ports. Unidirectional link detection provides discovery mechanism based on 802.3ah to discover its neighbor. If the OAM discovery can complete in configured discovery time, it concludes the link is bidirectional. Otherwise, it starts detecting task to detect the link status.

Format

```
config duld ports [<portlist> | all] {state [enable | disable] | mode [shutdown | normal] |
  discovery_time <sec 5-65535>}(1)
```

Parameters

<portlist> - Specifies a range of ports.

all - Specifies to select all ports.

state - Specifies these ports unidirectional link detection status.

- enable** - Enables unidirectional link detection status.
- disable** - Disables unidirectional link detection status.

mode - Specifies the mode when detecting unidirectional link.

- shutdown** - If any unidirectional link is detected, disables the port and logs an event.
- normal** - Only logs 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, Operators and Power-Users can issue this command.

Example

To enable unidirectional link detection on port 1:

```
DGS-3000-26TC:admin#config duld ports 1 state enable
Command: config duld ports 1 state enable

Success.

DGS-3000-26TC:admin#
```

23-2 show duld ports

Description

This command is used to show unidirectional link detection information.

Format

show duld ports {<portlist>}

Parameters

<portlist> - (Optional) Specifies a range of ports.

Restrictions

None.

Example

To show ports 1-4 unidirectional link detection information:

```
DGS-3000-26TC: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-3000-26TC:admin#
```

Chapter 24 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 <second 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

```

24-1 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-3000-26TC:admin#config name_server add 10.10.10.10 primary
Command: config name_server add 10.10.10.10 primary

Success.

DGS-3000-26TC:admin#

```

24-2 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-3000-26TC:admin#config name_server delete 10.10.10.1
Command: config name_server delete 10.10.10.1

Success.

DGS-3000-26TC:admin#
```

24-3 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

<second 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-3000-26TC:admin#config name_server timeout 10
Command: config name_server timeout 10

Success.

DGS-3000-26TC:admin#
```

24-4 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:

```
Static Name Server Table:
  Server IP Address                Priority
  -----
  10.10.10.10                      Primary
  10.1.1.1                          Secondary

Dynamic Name Server Table:
  Server IP Address                Priority
  -----
  10.48.74.122                     Primary

DGS-3000-26TC:admin#
```

24-5 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-3000-26TC:admin#create host_name www.example.com 10.10.10.10
Command: create host_name www.example.com 10.10.10.10

Success.

DGS-3000-26TC:admin#
```

24-6 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-3000-26TC:admin#delete host_name www.example.com
Command: delete host_name www.example.com

Success.

DGS-3000-26TC:admin#
```


24-7 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-3000-26TC: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-3000-26TC:admin#
```

24-8 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-3000-26TC:admin#enable dns_resolver
Command: enable dns_resolver

Success.

DGS-3000-26TC:admin#
```

24-9 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-3000-26TC:admin#disable dns_resolver
Command: disable dns_resolver

Success.

DGS-3000-26TC:admin#
```

Chapter 25 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]
```

25-1 config dos_prevention dos_type

Description

This command is used to configure the prevention of each Denial-of-Service (DoS) attack, 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) Checks whether the source address is equal to destination address of a received IP packet.

blat_attack - (Optional) Checks whether the source port is equal to destination port of a received TCP packet.

tcp_null_scan - (Optional) Checks whether a received TCP packet contains a sequence number of 0 and no flags

tcp_xmasscan - (Optional) Checks whether a received TCP packet contains URG, Push and FIN flags.

tcp_synfin - (Optional) Checks whether a received TCP packet contains FIN and SYN flags.

tcp_syn_srcport_less_1024 - (Optional) Checks whether the TCP packets source ports are less than 1024 packets.

ping_death_attack - (Optional) Detects whether received packets are fragmented ICMP packets.

tcp_tiny_frag_attack - (Optional) Checks whether the packets are TCP tiny fragment packets.

all - Specifies all DoS attack type.

action - (Optional) When enabling DoS prevention, the following actions can be taken.

drop - Drops DoS attack packets.

state - (Optional) Specifies the DoS attack prevention state.

enable - Enables DoS attack prevention.

disable - Disables 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-3000-26TC: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-3000-26TC:admin#
```

25-2 show dos_prevention

Description

This command is used to display DoS prevention information, including the Trap/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) Checks whether the source address is equal to destination address of a received IP packet. |
| blat_attack - (Optional) Checks whether the source port is equal to destination port of a received TCP packet. |
| tcp_null_scan - (Optional) Checks whether a received TCP packet contains a sequence number of 0 and no flags |
| tcp_xmasscan - (Optional) Checks whether a received TCP packet contains URG, Push and FIN flags. |
| tcp_synfin - (Optional) Checks whether a received TCP packet contains FIN and SYN flags. |
| tcp_syn_srcport_less_1024 - (Optional) Checks whether the TCP packets source ports are less than 1024 packets. |
| ping_death_attack - (Optional) Detects whether received packets are fragmented ICMP packets. |
| tcp_tiny_frag_attack - (Optional) Checks whether the packets are TCP tiny fragment packets. |

Restrictions

None.

Example

To display DoS prevention information:

```

DGS-3000-26TC: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

```

25-3 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 - Enables DoS prevention trap state.

disable - Disables DoS prevention trap state.

Restrictions

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

Example

To disable DoS prevention trap:

```

DGS-3000-26TC:admin#config dos_prevention trap disable
Command: config dos_prevention trap disable

Success.

DGS-3000-26TC:admin#

```

25-4 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 - Enables DoS prevention log state.

disable - Disables DoS prevention log state.

Restrictions

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

Example

To enable DoS prevention log:

```
DGS-3000-26TC:admin#config dos_prevention log enable
Command: config dos_prevention log enable

Success.

DGS-3000-26TC:admin#
```

Chapter 26 Energy Efficient Ethernet (EEE) Commands

config eee ports [<portlist> | all] state [enable | disable]
show eee ports {<portlist>}

26-1 config eee ports

Description

This command is used to enable or disable the EEE function on the specified port(s) on the Switch.

Note: The two functions, EEE and ERPS, are mutually exclusive.

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 - Enable the EEE function for the specified port(s).

disable - 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-3000-26TC:admin#config eee ports 2-5 state enable
Command: config eee ports 2-5 state enable

Success.

DGS-3000-26TC:admin#
```

26-2 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) Specify a list of ports to be displayed.

Restrictions

None.

Example

To display the EEE state:

```
DGS-3000-26TC: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-3000-26TC:admin#
```


Chapter 27 Ethernet Ring Protection Switching (ERPS) Command List

| |
|---|
| enable erps |
| disable erps |
| create erps raps_vlan <vlanid> |
| delete erps raps_vlan <vlanid> |
| config erps raps_vlan <vlanid> [state [enable disable] ring_mel <value 0-7> ring_port [west <port> east <port>] rpl_port [west east none] rpl_owner [enable disable] protected_vlan [add delete] vlanid <vidlist> revertive [enable disable] timer {holdoff_time <millisecond 0 - 10000> guard_time <millisecond 10 - 2000> wtr_time <min 5 - 12>}] |
| config erps log [enable disable] |
| config erps trap [enable disable] |
| show erps |

27-1 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: The two functions, EEE and ERPS, are mutually exclusive.

Format

enable erps

Parameters

None.

Restrictions

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

Example

To enable ERPS:

```
DGS-3000-26TC:admin#enable erps
Command: enable erps

Success.

DGS-3000-26TC:admin#
```

27-2 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-3000-26TC:admin#disable erps
Command: disable erps

Success.

DGS-3000-26TC:admin#
```

27-3 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 that the R-APS VLAN must already have been created by the create vlan command.

Format

create erps raps_vlan <vlanid>

Parameters

raps_vlan - Specifies the VLAN which will be the R-APS VLAN.
<vlanid> - Enter the VLAN ID used here.

Restrictions

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

Example

To create an R-APS VLAN:

```
DGS-3000-26TC:admin#create erps raps_vlan 4094
Command: create erps raps_vlan 4094

Success.

DGS-3000-26TC:admin#
```

27-4 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>

Parameters

raps_vlan - Specifies the VLAN which will be the R-APS VLAN.
<vlanid> - Enter the VLAN ID used here.

Restrictions

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

Example

To delete an R-APS VLAN:

```
DGS-3000-26TC:admin#delete erps raps_vlan 4094
Command: delete erps raps_vlan 4094

Success.

DGS-3000-26TC:admin#
```

27-5 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. Note that if CFM (Connectivity Fault Management) and ERPS are used at the same time, the R-APS PDU is one of a suite of Ethernet OAM PDU. The behavior for forwarding of R-APS PDU should follow the Ethernet OAM. If the MEL of R-APS PDU is not higher than the level of the MEP with the same VLAN on the ring ports, the R-APS PDU cannot be forwarded on the ring.

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. Note that the ring ports cannot be modified when ERPS is enabled.

RPL port - Specifies one of the R-APS VLAN ring ports as the RPL port. To remove an RPL port from an R-APS VLAN, use the none designation for rpl_port.

RPL owner - Specifies the node as the RPL owner.

Note that the RPL port and RPL owner cannot be modified when ERPS is enabled; and the virtual channel cannot be configured as RPL. For example, if a ring port is configured on the virtual channel and the ring port is configured as an RPL port, an error message will be display and the configuration will fail.

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.

Holdoff timer - The Holdoff timer is used to filter out intermittent link faults when link failures occur during the protection switching process. When a ring node detects a link failure, it will start the holdoff timer and report the link failure event (R-APS BPDU with SF flag) after the link failure is confirmed within period of time specified.

Guard timer - Guard timer is used to prevent ring nodes from receiving outdated R-APS messages. This timer is used during the protection switching process after the link failure recovers. When the link node detects the recovery of the link, it will report the link failure recovery event (R-APS PDU with NR flag) and start the guard timer. Before the guard timer expires, all received R-APS messages are ignored by this ring node, except in the case where a burst of three R-APS event messages that indicates the topology of a sub-ring has changed and the node needs to flush FDB are received on the node. In this case the recovered link does not go into a blocking state. The Guard Timer should be greater than the maximum expected forwarding delay for which one R-APS message circles around the ring.

WTR timer - WTR timer is used to prevent frequent operation of the protection switch due to an intermittent defect. This timer is used during the protection switching process when a link failure recovers. It is only used by the RPL owner. When the RPL owner in protection state receives R-APS PDU with an NR flag, it will start the WTR timer. The RPL owner will block 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. EEE, 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, RPL owner, are configured. Note that 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.

Format

```
config erps raps_vlan <vlanid> [state [enable | disable] | ring_mel <value 0-7> | ring_port
[west <port> | east <port> ] | rpl_port [west | east | none] | rpl_owner [enable | disable] |
protected_vlan [add | delete] vlanid <vidlist> | revertive [enable | disable] | timer
{holdoff_time <millisecond 0 - 10000> | guard_time <millisecond 10 - 2000> | wtr_time <min
5 - 12>}]
```

Parameters

| |
|--|
| <vlanid> - Enter the R-APS VLAN ID used. |
| state - Specifies to enable or disable the specified ring. enable - Enable the state of the specified ring. disable - Disable the state of the specified ring. The default value is disabled. |
| 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 the port as the west ring port. <port> - Enter the port number here. east - Specifies the port as the east ring port. <port> - Enter the port number here. |
| 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 - This node is not an RPL owner. By default, the RPS owner is disabled. |
| protected_vlan - Specifies to add or delete the protected VLAN group. add - Adds VLANs to the protected VLAN group. delete - Deletes VLANs from the protected VLAN group. vlanid - Specifies the VLAN ID to be removed or added. <vidlist> - Enter the VLAN ID list 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 - (Optional) Specifies the holdoff time of the R-APS function. The default holdoff time is 0 milliseconds.

<millisecond 0-10000> - Enter the hold off time value here. This value must be in the range of 0 to 10000 milliseconds.

guard_time - (Optional) 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 0 to 2000 milliseconds.

wtr_time - (Optional) Specifies the WTR time of the R-APS function.

<min 5-12> - Enter the WTR time range value here. The range is from 5 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-3000-26TC:admin#config erps raps_vlan 4094 ring_mel 2
Command: config erps raps_vlan 4094 ring_mel 2

Success.

DGS-3000-26TC:admin#
```

To configure the ports of the ERPS ring for a specific R-APS VLAN:

```
DGS-3000-26TC:admin#config erps raps_vlan 4094 ring_port west 5
Command: config erps raps_vlan 4094 ring_port west 5

Success.

DGS-3000-26TC:admin#
```

To configure the RPL owner for a specific R-APS VLAN:

```
DGS-3000-26TC:admin#config erps raps_vlan 4094 rpl_owner enable
Command: config erps raps_vlan 4094 rpl_owner enable

Success.

DGS-3000-26TC:admin#
```

To configure the protected VLAN for a specific R-APS VLAN:

```
DGS-3000-26TC: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-3000-26TC:admin#
```

To configure the ERPS timers for a specific R-APS VLAN:

```
DGS-3000-26TC: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-3000-26TC:admin#
```

To configure the ring state of the ERPS:

```
DGS-3000-26TC:admin#config erps raps_vlan 4094 state enable
Command: config erps raps_vlan 4094 state enable

Success.

DGS-3000-26TC:admin#
```

27-6 config erps log

Description

This command is used to configure the log state of ERPS events.

Format

config erps log [enable | disable]

Parameters

log - Specifies to enable or disable the ERPS log state.
enable - Enter enable to enable the log state.
disable - Enter disable to disable the log state. The default value is disabled.

Restrictions

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

Example

To configure the ERPS log state:

```
DGS-3000-26TC:admin#config erps log enable
Command: config erps log enable

Success.

DGS-3000-26TC:admin#
```

27-7 config erps trap

Description

This command is used to configure trap state of ERPS events.

Format

config erps trap [enable | disable]

Parameters

trap - Specifies to enable or disable the ERPS trap state.
enable - Enter enable to enable the trap state.
disable - Enter disable to disable the trap state. The default value is disabled.

Restrictions

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

Example

To configure the trap state of the ERPS:

```
DGS-3000-26TC:admin#config erps trap enable
Command: config erps trap enable

Success.

DGS-3000-26TC:admin#
```

27-8 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", "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 owner administrative state could be configured to "Enabled" or "Disabled". But the RPL owner operational state may be different from the RPL owner administrative state, for example, the RPL owner conflict occurs. "Active" is used to indicate that the RPL owner administrative state is enabled and the device is operated as the active RPL owner. "Inactive" is used to indicate that the RPL owner administrative state is enabled, but the device is operated as the inactive RPL owner.

Format

show erps

Parameters

None.

Restrictions

None.

Example

To display ERPS information:

```
DGS-3000-26TC:admin#show erps
Command: show erps

Global Status          : Disabled
Log Status             : Disabled
Trap Status           : Disabled
-----
R-APS VLAN             : 4094
ERPS Status           : Disabled
Admin West Port       : 5
Operational West Port : 5    (Forwarding)
Admin East Port       :
Operational East Port :
Admin RPL Port        : None
Operational RPL Port  : None
Admin Owner           : Enabled
Operational Owner     : Enabled
Protected VLANs       : 10-20
Ring MEL              : 2
Holdoff Time          : 100 milliseconds
Guard Time           : 1000 milliseconds
WTR Time              : 10 minutes
Revertive mode        : Enabled
Current Ring State    : -

-----
Total Rings: 1

DGS-3000-26TC:admin#
```

Chapter 28 External Alarm Command List

config external_alarm channel <value 1-2> message <sentence 1-128>
show external_alarm

28-1 config external_alarm channel

Description

This command is used to configure external alarm message for a channel.

Format

config external_alarm channel <value 1-2> message <sentence 1-128>

Parameters

<value 1-2> - Specifies the value of channel to be configured.

message - Specifies the message to be displayed on console, log and trap.

<sentence 1-128> - Enter the message to be displayed on console, log and trap.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure alarm message for channel 1:

```
DGS-3000-26TC:admin#config external_alarm channel 1 message External Alarm: UPS
is Exhausted.
Command: config external_alarm channel 1 message External Alarm: UPS is
Exhausted.

Success.

DGS-3000-26TC:admin#
```

28-2 show external_alarm

Description

This command is used to display the status of external alarm.

Format

show external_alarm

Parameters

None.

Restrictions

None.

Example

To display the real-time status of external alarm:

```
DGS-3000-26TC:admin#show external_alarm  
Command: show external_alarm
```

| Channel | Status | Alarm Message |
|---------|--------|-----------------------------------|
| 1 | Normal | External Alarm: UPS is Exhausted. |
| 2 | Normal | External Alarm 2 |

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

Chapter 29 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**

29-1 config filter netbios

Description

This command is used to configure the Switch to deny the 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 filter to block the NETBIOS packet.**enable** - Specifies that the state will be enabled.**disable** - Specifies that the state will be disabled.

Restrictions

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

Example

To configure filter netbios state:

```
DGS-3000-26TC:admin#config filter netbios 1-10 state enable
Command: config filter netbios 1-10 state enable

Success.

DGS-3000-26TC:admin#
```

29-2 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-3000-26TC:admin#show filter netbios
Command: show filter netbios

Enabled ports: 1-3

DGS-3000-26TC:admin#
```

29-3 config filter extensive_netbios

Description

This command is used to configure the Switch to filter NETBIOS packets over 802.3 frame 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 filter to block the NETBIOS packet over 802.3 frame.

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-3000-26TC:admin#config filter extensive_netbios 1-10 state enable
Command: config filter extensive_netbios 1-10 state enable

Success.

DGS-3000-26TC:admin#
```

29-4 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-3000-26TC:admin#show filter extensive_netbios
Command: show filter extensive_netbios

Enabled ports: 1-3

DGS-3000-26TC:admin#
```

Chapter 30 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>]}

```

30-1 create fdb

Description

This command is used to create a static entry in the unicast MAC address forwarding table (database).

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> - The MAC address to be added to the static forwarding table.
port - 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 action drop to be taken.

```

Restrictions

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

Example

To create a unicast MAC forwarding entry:

```
DGS-3000-26TC: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-3000-26TC:admin#
```

To filter a unicast MAC:

```
DGS-3000-26TC:admin#create fdb default 00-00-00-00-01-02 drop
Command: create fdb default 00-00-00-00-01-02 drop

Success.

DGS-3000-26TC:admin#
```

30-2 create fdb vlanid

Description

This command is used to create a static entry in the unicast MAC address forwarding table (database).

Format

create fdb vlanid <vidlist> <macaddr> [port <port> | drop]

Parameters

<vidlist> - Specifies a VLAN ID associated with a MAC address.

<macaddr> - The MAC address to be added to the static forwarding table.

port - 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 action drop to be taken.

Restrictions

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

Example

To create a unicast MAC forwarding entry:

```
DGS-3000-26TC: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-3000-26TC:admin#
```

To filter a unicast MAC:


```
DGS-3000-26TC: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-3000-26TC:admin#
```

30-3 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> - The name of the VLAN on which the MAC address resides. The maximum name length is 32.

<macaddr> - 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-3000-26TC:admin#create multicast_fdb default 01-00-5E-00-00-00
Command: create multicast_fdb default 01-00-5E-00-00-00

Success.

DGS-3000-26TC:admin#
```

30-4 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> - The name of the VLAN on which the MAC address resides. The maximum

name length is 32.

<macaddr> - 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> - Specifies 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-3000-26TC: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-3000-26TC:admin#
```

30-5 config fdb aging_time

Description

This command is used to configure the MAC address table aging time.

Format

config fdb aging_time <sec 10-1000000>

Parameters

aging_time - Specifies the FDB age out time in seconds. The aging time affects the learning process of the Switch. Dynamic forwarding table entries, which are made up of the source MAC addresses and their associated port numbers, are deleted from the table if they are not accessed within the aging time. The aging time can be from 10 to 1000000 seconds with a default value of 300 seconds. 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..

<sec 10-1000000> - Enter the FDB age out time between 10 to 1000000 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-3000-26TC:admin#config fdb aging_time 600
Command: config fdb aging_time 600

Success.

DGS-3000-26TC:admin#
```

30-6 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> - The VLAN name can be up to 32 characters long.

all - Specifies all configured VLANs.

forward_all_groups - 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 - The unregistered group will be forwarded to all member ports of the VLAN where the multicast traffic comes in.

filter_unregistered_groups - 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-3000-26TC: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-3000-26TC:admin#
```

30-7 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> - The name of the VLAN on which the MAC address resides. The maximum name length is 32.

<macaddr> - 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-3000-26TC:admin#delete fdb default 00-00-00-00-01-02
Command: delete fdb default 00-00-00-00-01-02

Success.

DGS-3000-26TC:admin#
```

30-8 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 - Clears the FDB entry by specifying the VLAN name.

<vlan_name 32> - The name of the VLAN on which the MAC address resides. The maximum name length is 32.

port - Clears the FDB entry by specifying the port number.

<port> - The port number corresponding to the MAC destination address. The switch will always forward traffic to the specified device through this port.

all - Clears 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-3000-26TC:admin#clear fdb all
Command: clear fdb all

Success.

DGS-3000-26TC:admin#
```

30-9 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) 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) Displays 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-3000-26TC: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-3000-26TC:admin#

```

30-10 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) Displays the entries for a specified port. <port> - Enter the port number here. |
| vlan - (Optional) Displays 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) Displays the entries for the VLANs indicated by VID list. <vidlist> - Enter the VLAN ID list here. |
| mac_address - (Optional) Displays a specific MAC address. <macaddr> - Enter the MAC address here. |
| static - (Optional) Displays all permanent entries. |
| aging_time - (Optional) Displays the unicast MAC address aging time. |
| security - (Optional) Displays 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-3000-26TC: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-3000-26TC:admin#
```

To display the security FDB table:

```
DGS-3000-26TC: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-3000-26TC:admin#
```

30-11 show multicast vlan_filtering_mode

Description

This command is used to show the multicast packet filtering mode for VLANs.

Note: A product supports the multicast VLAN filtering mode could not 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-3000-26TC: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-3000-26TC:admin#
```


Chapter 31 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>

```

31-1 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, the media identification.

Format

show storage_media_info

Parameters

None.

Restrictions

None.

Example

To display the storage media's information:

```

DGS-3000-26TC:admin#show storage_media_info
Command: show storage_media_info

Drive  Media Type      Size  Label      FS Type
-----  -----  -
c:/    Flash           28 MB             FFS

DGS-3000-26TC:admin#

```

31-2 md

Description

This command is used to create a directory.

Format

md {<drive_id>} <pathname>

Parameters

<drive_id> - (Optional) Enter the drive ID used, for example, C:.

<pathname> - Specifies the directory. The path name can be specified either as a full path name or partial name. For partial path name, it indicates the file is in the current directory. The drive ID also included in this parameter, for example, c:/config/bootup.cfg.

Restrictions

Only Administrators and Operators can issue this command.

Example

To make a directory:

```
DGS-3000-26TC:admin#md c:/abc
Command: md c:/abc

Success.

DGS-3000-26TC:admin#
```

31-3 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 error message.

Format

rd {<drive_id>} <pathname>

Parameters

<drive_id> - (Optional) Enter the drive ID used, for example, C:.

<pathname> - Specifies the directory to be removed. The path name can be specified either as a full path name or partial name. For partial path name, it indicates the file is in the current directory.

Restrictions

Only Administrators and Operators can issue this command.

Example

To remove a directory:

```
DGS-3000-26TC:admin#rd c:/abc
Command: rd c:/abc

Success.

DGS-3000-26TC:admin#
```

31-4 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. The current drive and current directory will be displayed if the <pathname> is not specified.

Format

cd {<pathname>}

Parameters

<pathname> - (Optional) Specifies the directory to be navigated to. The path name can be specified either as a full path name or partial name. For partial path name, it indicates the file is in the current directory.

Restrictions

None.

Example

To change to other directory or display current directory path:

```
DGS-3000-26TC:admin#cd
Command: cd

Current work directory: "/c:".

DGS-3000-26TC:admin#
```

31-5 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 used, for example, C:.**<pathname>** - (Optional) Specifies the directory to be displayed. The path name can be specified either as a full path name or partial name. For partial path name, it indicates the file is in the current directory.**Restrictions**

None.

Example

List the files:

```

DGS-3000-26TC:admin#dir
Command: dir

Directory of /c:

Idx Info      Attr Size      Update Time      Name
-----
  1 RUN(*)    -rw- 5491536   2000/01/01 00:41:03 DGS3000_Run_1_00_010.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-3000-26TC:admin#

```

31-6 rename**Description**

This command is used to rename a file. Note that for standalone device, the unit argument is not needed. 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 used, for example, C:.

<pathname> - Specifies the file (in path form) to be renamed.

<filename> - Specifies the new name of the file.

Restrictions

Only Administrators and Operators can issue this command.

Example

To rename a file:

```
DGS-3000-26TC:admin#rename run.had run1.had
Command: rename run.had run1.had

Success.

DGS-3000-26TC:admin#
```

31-7 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 acceptable.

System will prompt if the target file is a firmware or configuration file of which the type is bootup.

Format

del {<drive_id>} <pathname> {recursive}

Parameters

<drive_id> - (Optional) Enter the drive ID used, for example, C:.

<pathname>- Specifies the file or directory to be deleted. If it is specified in the associated form, then it is related to the current directory.

recursive - (Optional) Specifies to delete a directory and its contents, even if it's not empty.

Restrictions

Only Administrators and Operators can issue this command.

Example

Delete a directory with parameter "recursive":

```

DGS-3000-26TC: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-3000-26TC:admin#del 12 recursive
Command: del 12 recursive

Success.

DGS-3000-26TC: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-3000-26TC:admin#

```

31-8 erase

Description

This command is used to delete a file stored in the file system.

System will prompt if the target file is a FW or configuration whose type is boot up.

Format

erase {<drive_id>} <pathname>

Parameters

<drive_id> - (Optional) Enter the drive ID used, for example, C:.

<pathname> - Specifies the file to be deleted. If it is specified in the associated form, then it is

related to the current directory.

Restrictions

Only Administrators and Operators can issue this command.

Example

To erase a file:

```
DGS-3000-26TC: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-3000-26TC:admin#erase config2.cfg
Command: erase config2.cfg

Success.

DGS-3000-26TC: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-3000-26TC:admin#
```

31-9 move

Description

This command is used to move a file around the file system. Note that when a file is moved, it can be specified whether to rename at the same time.

Format

move {<drive_id>} <pathname> {<drive_id>} <pathname>

Parameters

<drive_id> - (Optional) Enter the drive ID, for example, C:.

<pathname> - Specifies the file to be moved. The path name can be specified either as a full path name or partial name. Specifies either as a full path name or partial name. For partial path name, it indicates the file is in the current directory.

<drive_id> - (Optional) Enter the drive ID, for example, C:.

<pathname> - Specifies the new path where the file will be moved. The path name can be. For partial path name, it indicates the file is in the current directory.

Restrictions

Only Administrators and Operators can issue this command.

Example

To move a file from one location to another location:

```
DGS-3000-26TC:admin#move c:/log.txt c:/log1.txt
```

```
Command: move c:/log.txt c:/log1.txt
```

```
Success.
```

```
DGS-3000-26TC:admin#
```

31-10 copy**Description**

This command is used to copy a file to another file in the file system.

Format

copy {<drive_id>} <pathname> {<drive_id>} <pathname>

Parameters

<drive_id> - (Optional) Enter the drive ID, for example, C:.

<pathname> - Specifies the file to be copied. The path name can be specified either as a full path name or partial name. For partial path name, it indicates the file is in the current directory.

<drive_id> - (Optional) Enter the drive ID, for example, C:.

<pathname> - Specifies the file to copy to. The path name can be specified either as a full path name or partial name. For partial path name, it indicates the file is in the current directory.

Restrictions

Only Administrators and Operators can issue this command.

Example

To copy a file:

```
DGS-3000-26TC:admin#copy c:/log.txt c:/log1.txt
```

```
Command: copy c:/log.txt c:/log1.txt
```

```
Success.
```

```
DGS-3000-26TC:admin#
```

Chapter 32 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>}

```

32-1 config gratuitous_arp send ipif_status_up

Description

The command is used to enable or disable the sending of gratuitous ARP packets when the IP interface's status is up. This is used to automatically announce the interface's IP address to other nodes. Only one gratuitous ARP packet will be broadcasted.

Format

```
config gratuitous_arp send ipif_status_up [enable | disable]
```

Parameters

enable - Enables the sending of gratuitous ARP packets when the IP interface's status is up. This is the default value.

disable - Disables the sending of gratuitous ARP packets when the IP interface's status is up.

Restrictions

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

Example

To enable send gratuitous ARP request in normal situation:

```

DGS-3000-26TC:admin#config gratuitous_arp send ipif_status_up enable
Command: config gratuitous_arp send ipif_status_up enable

Success.

DGS-3000-26TC:admin#

```

32-2 config gratuitous_arp send dup_ip_detected

Description

The command is used to enable or disable the sending of gratuitous ARP request packets while the duplicate IP is detected. 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 some body out there uses an IP address that is conflict with the system. In order to reclaim the correct host of this IP address, the system can send out the gratuitous ARP request packet for this duplicate IP address.

Format

config gratuitous_arp send dup_ip_detected [enable | disable]

Parameters

enable - Enables the sending of gratuitous ARP request packet when duplicate IP is detected. This is the default value.

disable - Disables the sending of gratuitous ARP request packet when duplicate IP is detected.

Restrictions

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

Example

To enable send gratuitous ARP request when duplicate IP is detected:

```
DGS-3000-26TC:admin#config gratuitous_arp send dup_ip_detected enable
Command: config gratuitous_arp send dup_ip_detected enable

Success.

DGS-3000-26TC:admin#
```

32-3 config gratuitous_arp learning

Description

This command is used to configure gratuitous ARP learning. Normally, the system only learns the ARP reply packet or a normal ARP request packet that asks for the MAC address that corresponds to the system's IP address. The command is used to enable or disable the learning of ARP entry in the ARP cache based on the received gratuitous ARP packet. The gratuitous ARP packet is sent by a source IP address that is identical to the IP that the packet is queried for. Note that, with the gratuitous ARP learning, the system will not learn new entry but only do the update on the ARP table based on the received gratuitous ARP packet.

Format

config gratuitous_arp learning [enable | disable]

Parameters

enable - Enables the learning of ARP entry based on the received gratuitous ARP packet. This is the default value.

disable - Disables the learning of ARP entry based on the received gratuitous ARP packet.

Restrictions

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

Example

To show the global GratuitousARP state:

```
DGS-3000-26TC:admin#config gratuitous_arp learning enable
Command: config gratuitous_arp learning enable

Success.

DGS-3000-26TC:admin#
```

32-4 config gratuitous_arp send periodically

Description

The command is used to configure the interval for the periodical sending of gratuitous ARP request packet. By default, the interval is 0.

Format

config gratuitous_arp send periodically ipif <ipif_name 12> interval <value 0-65535>

Parameters

ipif - Specifies the interface name of L3 interface.

<ipif_name 12> - Enter the IP interface name here. This name can be up to 12 characters long.

interval - Specifies the periodically sending gratuitous ARP interval time in seconds. 0 means not to send gratuitous ARP periodically.

<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-3000-26TC:admin#config gratuitous_arp send periodically ipif System
interval 5
Command: config gratuitous_arp send periodically ipif System interval 5

Success.

DGS-3000-26TC:admin#
```

32-5 enable gratuitous_arp

Description

The command is used to enable gratuitous ARP trap and log state. The switch can trap and log the IP conflict event to inform the administrator. By default, trap is disabled and event log is enabled.

Format

enable gratuitous_arp {ipif <ipif_name 12>} {trap | log}(1)

Parameters

ipif - (Optional) Specifies the interface name of L3 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-3000-26TC:admin#enable gratuitous_arp ipif System trap log
Command: enable gratuitous_arp ipif System trap log

Success.

DGS-3000-26TC:admin#
```

32-6 disable gratuitous_arp

Description

The command is used to disable 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 interface name of L3 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-3000-26TC:admin#disable gratuitous_arp ipif System trap log
Command: disable gratuitous_arp ipif System trap log

Success.

DGS-3000-26TC:admin#
```

32-7 show gratuitous_arp

Description

This command is used to display gratuitous ARP configuration.

Format

show gratuitous_arp {ipif <ipif_name 12>}

Parameters

-
- ipif** - (Optional) Specifies the interface name of L3 interface.
<ipif_name> - Enter the IP interface name here.
-

Restrictions

None.

Example

To display gratuitous ARP log and trap state:

```
DGS-3000-26TC: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-3000-26TC:admin#
```

Chapter 33 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>] |

```
clear igmp_snooping statistics counter
```

```
show igmp_snooping host {[vlan <vlan_name 32> | vlanid <vlanid_list> | ports <portlist> | group <ipaddr>]}
```

33-1 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** - (Optional) 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 whether to use IGMP report suppression to forward only one IGMP report per multicast router query to multicast devices.
 - enable** - Specifies to use IGMP report suppression to forward only one IGMP report per multicast router query to multicast devices.
 - disable** - Disables IGMP report suppression to forward only one IGMP report per multicast router query to multicast devices.
-
- 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-3000-26TC:admin#config igmp_snooping vlan_name default state enable
Command: config igmp_snooping vlan_name default state enable

Success.

DGS-3000-26TC:admin#
```

33-2 config igmp_snooping rate_limit

Description

This command is used to configure the rate of IGMP control packet that is 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 packet 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 packet 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-3000-26TC:admin#config igmp_snooping rate_limit ports 1 100
Command: config igmp_snooping rate_limit ports 1 100

Success.

DGS-3000-26TC:admin#
```

33-3 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 - (Optional) 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 - (Optional) 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 - (Optional) Provides fine-tuning to allow for expected packet loss on a subnet. The value of the robustness variable is used in calculating the following IGMP message intervals:

<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 - (Optional) 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 - (Optional) If the state is enabled, it allows the Switch to be selected as an IGMP Querier (sends IGMP query packets). If the state is disabled, then the Switch cannot play the role as a querier. Note that if the Layer 3 router connected to the Switch provide only the IGMP proxy function but does not provide the multicast routing function, then this state must be configured as disabled. Otherwise, if the 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 packet, the port will be timed out as a router port.

enable - Specifies to enable this state.

disable - Specifies to disable this state.

version - (Optional) Specifies the version of IGMP packet 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-3000-26TC: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-3000-26TC:admin#
```

33-4 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 - Enables the RADIUS authentication function on the specified ports.

disable - Disables 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-3000-26TC:admin#config igmp access_authentication ports all state enable
Command: config igmp access_authentication ports all state enable

Success.

DGS-3000-26TC:admin#
```

33-5 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-3000-26TC:admin#config router_ports default add 1-10
Command: config router_ports default add 1-10

Success.

DGS-3000-26TC:admin#
```

33-6 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 to forbidden router ports of default VLAN:

```
DGS-3000-26TC:admin#config router_ports_forbidden default add 11-12
```

```
Command: config router_ports_forbidden default add 11-12
```

```
Success.
```

```
DGS-3000-26TC:admin#
```

33-7 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-3000-26TC:admin#enable igmp_snooping
Command: enable igmp_snooping

Success.

DGS-3000-26TC:admin#
```

33-8 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-3000-26TC:admin#disable igmp_snooping
Command: disable igmp_snooping

Success.

DGS-3000-26TC:admin#
```

33-9 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 port 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 to route 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> - Specifies 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-3000-26TC: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-3000-26TC:admin#
```

33-10 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 for 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> - Specifies 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-3000-26TC: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-3000-26TC:admin#
```

33-11 config igmp_snooping static_group

Description

This command is used to configure 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> - Specifies the multicast group IP address (for Layer 3 switch).
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 IGMP snooping static member ports for group 239.1.1.1 on default VLAN:

```
DGS-3000-26TC:admin#config igmp_snooping static_group vlan default 239.1.1.1
delete 9-10
Command: create igmp_snooping static_group vlan default 239.1.1.1 delete 9-10

Success.

DGS-3000-26TC:admin#
```

33-12 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 - 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> - Specifies the multicast group IP address.

Restrictions

None.

Example

To display all the IGMP snooping static groups:

```
DGS-3000-26TC:admin#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-3000-26TC:admin#
```

33-13 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, when the Switch receives the IP multicast traffic on this VLAN, an IGMP snooping group will be created. That is, the learning of an entry is not activated by IGMP membership registration, but activated by the traffic. For an ordinary IGMP snooping entry, the IGMP protocol will take care of the aging out of the entry. For a data-driven entry, the entry can be specified not to be aged out or to be aged out by the aged timer.

When data driven learning is enabled, and the data driven table is not full, the multicast filtering mode for all ports is ignored. That is, the multicast packets will be forwarded to router ports. If the data driven learning table is full, the multicast packets will be forwarded according to the multicast filtering mode.

Note that if a data-driven group is created and IGMP member ports are learned later, the entry will become an ordinary IGMP snooping entry. That is, the aging out mechanism will follow the ordinary IGMP snooping entry.

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 - (Optional) 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 - (Optional) 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 - (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 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-3000-26TC: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-3000-26TC:admin#
```

33-14 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.

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

max_learned_entry - Specifies the maximum number of groups that can be learned by data driven. The default setting is 128.
<value 1-1024> - Enter the maximum learning entry value here. This value must be between 1 and 1024.

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-3000-26TC:admin#config igmp_snooping data_driven_learning max_learned_entry
50
Command: config igmp_snooping data_driven_learning max_learned_entry 50

Success.

DGS-3000-26TC:admin#
```

33-15 clear igmp_snooping data_driven_group

Description

This command is used to delete the IGMP snooping group(s) learned by data driven.

Format

clear igmp_snooping data_driven_group [**all** | [**vlan_name** <vlan_name> | **vlanid** <vlanid_list>] [**<ipaddr>** | **all**]]

Parameters

| |
|---|
| all - Specifies all VLANs to 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 here. |
| <ipaddr> - Specifies the group's IP address learned by data driven. |
| all - Deletes all IGMP snooping groups of specified VLANs. |

Restrictions

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

Example

To delete all the groups learned by data-driven:

```
DGS-3000-26TC:admin#clear igmp_snooping data_driven_group all
Command: clear igmp_snooping data_driven_group all

Success.

DGS-3000-26TC:admin#
```

33-16 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 the VLAN is not specified, the system will display all current IGMP snooping configurations. |

Restrictions

None.

Example

To show IGMP snooping:

```
DGS-3000-26TC: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
Version                               : 3
Data Driven Learning State            : Enabled
Data Driven Learning Aged Out         : Disabled
Data Driven Group Expiry Time         : 260

Total Entries: 1

DGS-3000-26TC:admin#
```

33-17 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-3000-26TC: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
```

33-18 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) If data_driven is specified, only data driven groups will be displayed.

Restrictions

None.

Example

To show IGMP snooping groups when IGMP v3 is supported:

```
DGS-3000-26TC:admin#show igmp_snooping group
Command: show igmp_snooping group

Source/Group           : 10.0.0.1/225.0.0.1
VLAN Name/VID          : default/1
Member Ports           : 5
UP Time                : 6
Expiry Time            : 254
Filter Mode             : INCLUDE

Source/Group           : 10.0.0.10/225.0.0.1
VLAN Name/VID          : default/1
Member Ports           : 5
UP Time                : 6
Expiry Time            : 254
Filter Mode             : INCLUDE

Source/Group           : NULL/239.255.255.250
VLAN Name/VID          : default/1
Member Ports           : 5
UP Time                : 2
Expiry Time            : 258
Filter Mode             : EXCLUDE

Total Entries: 3

DGS-3000-26TC:admin#
```

```
DGS-3000-26TC:admin#show igmp_snooping group data_driven
Command: show igmp_snooping group data_driven
Source/Group           : NULL/225.0.0.5
VLAN Name/VID          : default/1
Reports                : 0
Member Ports           :
Router Ports           : 24
UP Time                : 3 days 50 mins
Expiry Time            : 120 secs
Filter Mode             : EXCLUDE

Total Entries : 1

DGS-3000-26TC: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-3000-26TC:admin#show igmp_snooping group
Command: show igmp_snooping group

Source/Group           : NULL/226.0.0.1
VLAN Name/VID          : default/1
Member Ports           : 5
UP Time                : 10
Expiry Time            : 258
Filter Mode            : EXCLUDE

Source/Group           : NULL/226.0.0.2
VLAN Name/VID          : default/1
Member Ports           : 5
UP Time                : 9
Expiry Time            : 259
Filter Mode            : EXCLUDE

Source/Group           : NULL/226.0.0.3
VLAN Name/VID          : default/1
Member Ports           :
Router Ports           :
UP Time                : 1
Expiry Time            : 259
Filter Mode            : EXCLUDE

Source/Group           : NULL/239.255.255.250
VLAN Name/VID          : default/1
Member Ports           : 5
UP Time                : 1
Expiry Time            : 259
Filter Mode            : EXCLUDE

Total Entries: 4

DGS-3000-26TC:admin#

```

33-19 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. The packet comes 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-3000-26TC: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-3000-26TC:admin#
```

33-20 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-3000-26TC: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-3000-26TC:admin#
```

33-21 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 port to be displayed here.

Restrictions

None.

Example

To display the IGMP snooping statistics counter:

```
DGS-3000-26TC: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-3000-26TC:admin#

```

To display the IGMP snooping statistics counter for a port:

```

DGS-3000-26TC: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-3000-26TC:admin#

```

33-22 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> - Specifies a range of ports to be displayed.

Restrictions

None.

Example

To display the IGMP Access Control status for ports 1-4:

```
DGS-3000-26TC: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-3000-26TC:admin#
```

To display the IGMP Access Control status for all ports:

```
DGS-3000-26TC: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
```

33-23 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-3000-26TC:admin#clear igmp_snooping statistic counter
Command: clear igmp_snooping statistic counter

Success.

DGS-3000-26TC:admin#
```

33-24 show igmp_snooping host

Description

This command is used to display the IGMP hosts that have joined groups on specific ports or specific VLANs.

Format

show igmp_snooping host {[vlan <vlan_name 32> | vlanid <vlanid_list> | ports <portlist> | group <ipaddr>]}

Parameters

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

vlanid - (Optional) Specifies the VLAN ID.
<vlanid_list> - Enter the VLAN ID here.

ports - (Optional) Specifies that list of port that will be displayed.
<portlist> - Enter the list of ports here.

group - (Optional) Specifies the group.
<ipaddr> - Enter the group IP address here.

If no parameter is specified, all joining hosts will be displayed.

Restrictions

None.

Example

To display the host IP information:

```
DGS-3000-26TC:admin#show igmp_snooping host vlan default
Command: show igmp_snooping host vlan default
```

| VLAN ID | Group | Port No | IGMP 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-3000-26TC:admin#
```

To display the host IP information for the group 225.0.1.0:

```
DGS-3000-26TC:admin#show igmp_snooping host group 225.0.1.0
Command: show igmp_snooping host group 225.0.1.0

VLAN ID      Group                Port No      IGMP 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-3000-26TC:admin#
```

Chapter 34 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] 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>} mac_address <macaddr>]] |
| 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 |

34-1 create address_binding ip_mac

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

-
- ipaddress** - Specifies the IP address used for the IMPB entry.
<ipaddr> - Enter the IP address used here.
-
- 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-3000-26TC: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-3000-26TC:admin#
```

34-2 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] | protocol [ipv4 | ipv6 | all] | allow_zeroip [enable | disable] | forward_dhcpkt [enable | disable] | stop_learning_threshold <int 0-500>}

Parameters

-
- ports** - Specifies the ports used for this configuration.
<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 packets are detected.
loose - In this mode, all packets are forwarded by default until an illegal ARP or broadcast IP packets are detected. If not specified strict or loose, default is strict.
disable - Disable ARP inspection function. The default value is disabled.
-
- ip_inspection** - (Optional) Specifies that the IP inspection option will be configured.
enable - Enables the IP inspection function. The legal IP packets will be forwarded, while the illegal IP packets will be dropped.
-

| | |
|--------------------------------|--|
| disable | - Disables the IP inspection function. The default value is disabled. |
| protocol | - (Optional) Specifies the version used. |
| ipv4 | - Specifies that 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 to enable the allow zero IP option. |
| disable | - Specifies to disable the allow zero IP option. |
| forward_dhcppt | - (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 to enable the forward DHCP packets option. |
| disable | - Specifies to disable the forward DHCP packets option. |
| 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-3000-26TC:admin#config address_binding ip_mac ports 1 arp_inspection strict
Command: config address_binding ip_mac ports 1 arp_inspection strict

Success.

DGS-3000-26TC:admin#
```

34-3 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> | - Specifies 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> - Specifies 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-3000-26TC: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-3000-26TC:admin#
```

34-4 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> - Specifies 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-3000-26TC: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-3000-26TC:admin#
```

34-5 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 that all the entries the address database that the system has automatically blocked to be deleted.

vlan_name - Specifies the name of the VLAN to which the blocked MAC address belongs.

<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-3000-26TC: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-3000-26TC:admin#
```

34-6 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 that all the MAC address will be used.

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 specified IMPB entry:

```
DGS-3000-26TC: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-3000-26TC:admin#
```

34-7 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

ipaddress - Specifies the IP address of the entry being updated.

<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 port 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-3000-26TC: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-3000-26TC:admin#
```

34-8 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-3000-26TC:admin#show address_binding
Command: show address_binding

Roaming state      : Enabled
Trap/Log           : Disabled
DHCP Snoop(IPv4)  : Disabled
DHCP Snoop(IPv6)  : Disabled
ND Snoop           : Disabled
Function Version   : 3.93

DGS-3000-26TC:admin#
```

To show the IMPB ports:

```
DGS-3000-26TC:admin#show address_binding ports
Command: show address_binding ports

ARP: ARP Inspection   IP: IP Inspection

Port   ARP       IP       Protocol Zero IP   DHCP Packet   Stop Learning
-----|-----|-----|-----|-----|-----|-----
1      Disabled Disabled All   Not Allow Forward   500/Normal
2      Disabled Disabled All   Not Allow Forward   500/Normal
3      Disabled Disabled All   Not Allow Forward   500/Normal
4      Disabled Disabled All   Not Allow Forward   500/Normal
5      Disabled Disabled All   Not Allow Forward   500/Normal
6      Disabled Disabled All   Not Allow Forward   500/Normal
7      Disabled Disabled All   Not Allow Forward   500/Normal
8      Disabled Disabled All   Not Allow Forward   500/Normal
9      Disabled Disabled All   Not Allow Forward   500/Normal
10     Disabled Disabled All   Not Allow Forward   500/Normal
11     Disabled Disabled All   Not Allow Forward   500/Normal
12     Disabled Disabled All   Not Allow Forward   500/Normal
13     Disabled Disabled All   Not Allow Forward   500/Normal
14     Disabled Disabled All   Not Allow Forward   500/Normal
15     Disabled Disabled All   Not Allow Forward   500/Normal
16     Disabled Disabled All   Not Allow Forward   500/Normal

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

34-9 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 that 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-3000-26TC: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-3000-26TC:admin#
```

34-10 show address_binding ip_mac

Description

This command is used to display the IMPB entries.

Format

```
show address_binding ip_mac [all | ipaddress <ipaddr> mac_address <macaddr>]
```

```
show address_binding ip_mac [all | [[ipaddress <ipaddr> | ipv6address <ipv6addr>]
{mac_address <macaddr>} | mac_address <macaddr>]]
```

Parameters

-
- all** - Specifies that 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** - (Optional) Specifies the MAC address of the entry in the database.
<macaddr> - Enter the MAC address here.

 - 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:

```

GS-3000-26TC:admin#show address_binding ip_mac all
Command: show address_binding ip_mac all

M(Mode) - D:DHCP, N:ND 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    1-26
FE80::240:5FF:FE00:28                    00-00-00-00-00-11 S  I    1-26

Total Entries : 2

DGS-3000-26TC:admin#

```

34-11 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).

Note that the DHCP discover packet cannot be passed thru 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 expires, the expired entry will be removed from the port. The auto-learned binding entry can be moved from one port to another port if the DHCP snooping function has learned that the MAC address has moved to a different port.

If a situation occurs where a binding entry learned by DHCP snooping conflicts with a statically configured entry. The binding relation has conflicted. For example, if IP A is binded to MAC X with a static configuration and suppose that the binding entry learned by DHCP snooping is that IP A is bound to MAC Y, and then it is conflict. When the DHCP snooping learned entry binds with the static configured entry, and the DHCP snooping learned entry will not be created.

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 enable the IPv6 entries.

all - (Optional) Specifies to enable all DHCP snooping mode.

Restrictions

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

Example

To enable DHCP IPv4 snooping mode:

```
DGS-3000-26TC:admin#enable address_binding dhcp_snoop
Command: enable address_binding dhcp_snoop

Success.

DGS-3000-26TC:admin#
```

34-12 disable address_binding dhcp_snoop

Description

This command is used to disable DHCP snooping mode. When the DHCP snooping function is disabled, all of the 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-3000-26TC:admin#disable address_binding dhcp_snoop
Command: disable address_binding dhcp_snoop

Success.

DGS-3000-26TC:admin#
```

34-13 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-3000-26TC:admin#clear address_binding dhcp_snoop binding_entry ports 1-3
Command: clear address_binding dhcp_snoop binding_entry ports 1-3

Success.

DGS-3000-26TC:admin#
```

34-14 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) Displays the maximum number of entries per port.

ports - Specifies the ports used for this configuration.

<portlist> - Enter a list of ports used here.

If no parameters are specified, show DHCP snooping displays the enable/disable state.

Restrictions

None.

Example

To show the DHCP snooping state:

```
DGS-3000-26TC:admin#show address_binding dhcp_snoop
Command: show address_binding dhcp_snoop

DHCP Snoop(IPv4) : Disabled
DHCP Snoop(IPv6) : Disabled

DGS-3000-26TC:admin#
```

To display DHCP snooping maximum entry configuration:

```
DGS-3000-26TC: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
```

34-15 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-3000-26TC: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  Time  Port
-----
10.62.58.35                00-0B-5D-05-34-0B         A 35964  1
10.33.53.82                00-20-c3-56-b2-ef         I  2590  2

Total entries : 2

DGS-3000-26TC:admin#
```

34-16 config address_binding dhcp_snoop max_entry

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

ports - Specifies the list of ports you would like to set the maximum number of entries that can be learned.

<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 learned to 10:

```
DGS-3000-26TC: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-3000-26TC:admin#
```

34-17 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-3000-26TC:admin#enable address_binding nd_snoop
Command: enable address_binding nd_snoop

Success.

DGS-3000-26TC:admin#
```

34-18 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-3000-26TC:admin#disable address_binding nd_snoop
Command: disable address_binding nd_snoop

Success.

DGS-3000-26TC:admin#
```

34-19 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-3000-26TC: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-3000-26TC:admin#
```

34-20 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-3000-26TC:admin#show address_binding nd_snoop
Command: show address_binding nd_snoop

ND Snoop           : Enabled

DGS-3000-26TC:admin#
```

To show the ND snooping maximum entry information for ports 1-5:

```
DGS-3000-26TC: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-3000-26TC:admin#
```

34-21 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-3000-26TC: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-3000-26TC:admin#
```

34-22 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-3000-26TC:admin#clear address_binding nd_snoop binding_entry ports 1-3
Command: clear address_binding nd_snoop binding_entry ports 1-3

Success.

DGS-3000-26TC:admin#
```

34-23 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-3000-26TC:admin#enable address_binding trap_log
Command: enable address_binding trap_log

Success.

DGS-3000-26TC:admin#
```

34-24 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-3000-26TC:admin#disable address_binding trap_log
Command: disable address_binding trap_log

Success.

DGS-3000-26TC:admin#
```

34-25 config address_binding recover_learning

Description

This command is used to recover IMPB checking.

Format

config address_binding recover_learning ports [<portlist> | all]

Parameters

ports - Specifies the list of ports that need to recover the IMPB check.
<portlist> - Enter the list of port used here.
all - Specifies that all the ports will be used.

Restrictions

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

Example

To recover IMPB checking for ports 6 to 7:

```
DGS-3000-26TC:admin#config address_binding recover_learning ports 6-7
Command: config address_binding recover_learning ports 6-7

Success.

DGS-3000-26TC:admin#
```

34-26 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 - Prints out the debug messages when IMPB module receives ARP/IP packets.
dhcp - Prints out the debug messages when the IMPB module receives the DHCP packets.
all - Prints out all debug messages.

state - Specifies the IMPB debug state to be enabled or disabled.
enable - Specifies to enable the state.
disable - Specifies to disable the state.

Restrictions

Only Administrator users can issue this command.

Example

To print out all debug IMPB messages:

```
DGS-3000-26TC:admin#debug address_binding all state enable
Command: debug address_binding all state enable

Success.

DGS-3000-26TC:admin#
```

34-27 no debug address_binding

Description

This command is used to stop the IMPB debug starting when the IMPB module receives an ARP/IP packet or a DHCP packet.

Format

no debug address_binding

Parameters

None.

Restrictions

Only Administrator users can issue this command.

Example

To stop IMPB debug: starting when the IMPB module receives an ARP/IP or DHCP packet:

```
DGS-3000-26TC:admin#no debug address_binding
Command: no debug address_binding

Success.

DGS-3000-26TC:admin#
```

34-28 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-3000-26TC:admin#enable address_binding roaming
Command: enable address_binding roaming

Success.

DGS-3000-26TC:admin#
```

34-29 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-3000-26TC:admin#disable address_binding roaming
Command: disable address_binding roaming

Success.

DGS-3000-26TC:admin#
```


Chapter 35 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>}

```

35-1 create ipv6 neighbor_cache

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 - Specifies the interface's name.

<ipif_name 12> - Enter the IP interface name here. This name can be up to 12 characters long.

<ipv6addr> - Specifies the IPv6 address of the neighbor.

<macaddr> - Specifies 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-3000-26TC: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-3000-26TC:admin#

```

35-2 delete ipv6 neighbor_cache

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 - Specifies the IPv6 interface name.

<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> - Specifies the neighbor's IPv6 address.

static - Deletes the static entry.

dynamic - Deletes those dynamic entries.

all - Deletes all entries include static and dynamic entries.

Restrictions

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

Example

Delete a neighbor cache entry on IP interface "System":

```
DGS-3000-26TC:admin#delete ipv6 neighbor_cache ipif System 3ffc::1
Command: delete ipv6 neighbor_cache ipif System 3FFC::1

Success.

DGS-3000-26TC:admin#
```

35-3 show ipv6 neighbor_cache

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 - Specifies the IPv6 interface name.

<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 address.

<ipv6addr> - Enter the IPv6 address here.

static - Static neighbor cache entry.

dynamic - Dynamic entries.

all - All entries include static and dynamic entries.

Restrictions

None

Example

Show all neighbor cache entries of IP interface "System":

```
DGS-3000-26TC: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-3000-26TC:admin#
```

35-4 config ipv6 nd ns retrans_time

Description

This command is used to configure the IPv6 ND neighbor solicitation retransmit time, which is 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 - The IPv6 interface name.

<ipif_name 12> - Enter the IP interface name here. This name can be up to 12 characters long.

retrans_time - Neighbor solicitation's re-transmit timer in millisecond.

<millisecond 0-4294967295> - Enter the re-transmit 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 retrans_time of IPv6 ND neighbor solicitation:

```
DGS-3000-26TC:admin#config ipv6 nd ns ipif Zira retrans_time 1000000
Command: config ipv6 nd ns ipif Zira retrans_time 1000000

Success.

DGS-3000-26TC:admin#
```

35-5 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 IP interface is specified, it will show the IPv6 ND related configuration of all interfaces.

Restrictions

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

Example

To show IPv6 ND related configuration:

```
DGS-3000-26TC:admin#show ipv6 nd ipif System
Command: show ipv6 nd ipif System

Interface Name           : System
NS Retransmit Time      : 0 (ms)

DGS-3000-26TC:admin#
```

Chapter 36 IPv6 Route Command List

```

create ipv6route [default] [<ipif_name 12> <ipv6addr> | <ipv6addr>] {<metric 1-65535>}
delete ipv6route [default] [<ipif_name 12> <ipv6addr> | <ipv6addr> | all]
show ipv6route

```

36-1 create ipv6route

Description

This command is used to create an IPv6 default 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

```
create ipv6route [default] [<ipif_name 12> <ipv6addr> | <ipv6addr>] {<metric 1-65535>}
```

Parameters

default - Specifies the default route.

<ipif_name 12> - Specifies the interface for the route. This name can be up to 12 characters long.

<ipv6addr> - Specifies the next hop address for this route.

<ipv6addr> - Specifies the next hop address for this route.

<metric 1-65535> - (Optional) Enter the metric value here. The default setting is 1. This value must be between 1 and 65535.

Restrictions

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

Example

To create and IPv6 route:

```

DGS-3000-26TC:admin#create ipv6route default System 3FFC::1
Command: create ipv6route default System 3FFC::1

Success.

DGS-3000-26TC:admin#

```

36-2 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] [<ipif_name 12> <ipv6addr> | <ipv6addr> | all]

Parameters

default - Specifies the default route.

<ipif_name 12> - Enter the IP interface name used here. This name can be up to 12 characters long.

<ipv6addr> - Specifies the next hop address for the default route.

<ipv6addr> - Specifies the next hop address for the default route.

all - Specifies that all static created routes will be deleted.

Restrictions

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

Example

Delete an IPv6 static route:

```
DGS-3000-26TC:admin#delete ipv6route default System 3FFC::1
Command: delete ipv6route default System 3FFC::1

Success.

DGS-3000-26TC:admin#
```

36-3 show ipv6route

Description

This command is used to display IPv6 routes.

Format

show ipv6route

Parameters

None.

Restrictions

None.

Example

Show all the IPv6 routes:

```
DGS-3000-26TC:admin#show ipv6route
```

```
Command: show ipv6route
```

```
IPv6 Prefix: ::/0
```

```
Protocol: Static Metric: 1
```

```
Next Hop   : 3001::254
```

```
IPIF      : System
```

```
Status     : Inactive
```

```
Total Entries: 1
```

```
DGS-3000-26TC:admin#
```

Chapter 37 Japanese Web-Based Access Control (JWAC) Command List

| |
|--|
| enable jwac |
| disable jwac |
| config jwac [quarantine_server_url <string 128> clear_quarantine_server_url] |
| show jwac |
| enable jwac redirect |
| disable jwac redirect |
| config jwac redirect {destination [quarantine_server jwac_login_page] delay_time <sec 0-10>}(1) |
| enable jwac forcible_logout |
| disable jwac forcible_logout |
| enable jwac udp_filtering |
| disable jwac udp_filtering |
| enable jwac quarantine_server_monitor |
| disable jwac quarantine_server_monitor |
| config jwac quarantine_server_error_timeout <sec 5-300> |
| config jwac virtual_ip <ipaddr> {url [<string 128> clear]} |
| config jwac update_server [add delete] ipaddress <network_address> {[tcp_port <port_number 1-65535> udp_port <port_number 1-65535>]} |
| config jwac switch_http_port <tcp_port_number 1-65535> {[http https]} |
| config jwac ports [<portlist> all] {state [enable disable] max_authenticating_host <value 0-50> aging_time [infinite <min 1-1440>] idle_time [infinite <min 1-1440>] block_time [<sec 0-300>] auth_mode [host_based port_based]}(1) |
| show jwac ports {<portlist>} |
| config jwac radius_protocol [local eap_md5 pap chap ms_chap ms_chapv2] |
| create jwac user <username 15> {vlan <vlanid 1-4094>} |
| config jwac user <username 15> {vlan <vlanid 1-4094>} |
| delete jwac [user <username 15> all_users] |
| show jwac user |
| clear jwac auth_state [ports [all <portlist>] {authenticated authenticating blocked} mac_addr <macaddr>] |
| show jwac auth_state ports {<portlist>} |
| config jwac authorization_attributes {radius [enable disable] local [enable disable]}(1) |
| show jwac update_server |
| config jwac authentication_page element [japanese english] [default page_title <desc 128> login_window_title <desc 32> user_name_title <desc 16> password_title <desc 16> logout_window_title <desc 32> notification_line <value 1-5> <desc 128>] |
| config jwac authenticate_page [japanese english] |
| show jwac authenticate_page |

37-1 enable jwac

Description

This command is used to enable the Japanese Web-based access control (JWAC) function.

Using the JWAC function, PC users need to pass two stages of authentication. The first stage is to do the authentication with the quarantine server and the second stage is the authentication with the Switch.

Format

enable jwac

Parameters

None.

Restrictions

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

Example

To enable JWAC:

```
DGS-3000-26TC:admin#enable jwac
Command: enable jwac

Success.

DGS-3000-26TC:admin#
```

37-2 disable jwac

Description

This command is used to disable JWAC.

Format

disable jwac

Parameters

None.

Restrictions

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

Example

To disable JWAC:

```
DGS-3000-26TC:admin#disable jwac
Command: disable jwac

Success.

DGS-3000-26TC:admin#
```

37-3 config jwac

Description

This command is used to configure the quarantine server URL. If the redirection is enabled and the redirection destination is a quarantine server, when a HTTP request from an unauthenticated host which is not headed to a quarantine server reaches the Switch, the Switch will handle this HTTP packet and send back a message to the host to make it access the quarantine server with the configured URL. When the PC connected to the specified URL, the quarantine server will request the PC user to input the user name and password to authenticate.

Note: If the quarantine server is linked to the JWAC enabled port on the Switch, it must be added to the static FDB correctly before it can work properly.

Format

config jwac [quarantine_server_url <string 128> | clear_quarantine_server_url]

Parameters

quarantine_server_url - Specifies the entire URL of the authentication page on the quarantine server.

<string 128> - Specifies the entire URL of the authentication page on the quarantine server. The quarantine server URL can be up to 128 characters long.

clear_quarantine_server_url - Specifies to clear the current quarantine server URL.

Restrictions

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

Example

To configure the quarantine server URL::

```
DGS-3000-26TC:admin#config jwac quarantine_server_url
http://10.90.90.88/authpage.html
Command: config jwac quarantine_server_url http://10.90.90.88/authpage.html

Success.

DGS-3000-26TC:admin#
```

37-4 show jwac

Description

This command is used to display the JWAC configuration settings.

Format**show jwac****Parameters**

None.

Restrictions

None.

Example

To display the current JWAC configuration:

```
DGS-3000-26TC:admin#show jwac
Command: show jwac

State                : Enabled
Enabled Ports        :
Virtual IP/URL        : 1.1.1.1/-
Switch HTTP Port     : 80 (HTTP)
UDP Filtering         : Enabled
Forcible Logout      : Enabled
Redirect State        : Enabled
Redirect Delay Time   : 1 Seconds
Redirect Destination  : Quarantine Server
Quarantine Server     : http://10.90.90.88/authpage.html
Q-Server Monitor     : Disabled
Q-Server Error Timeout : 30 Seconds
RADIUS Auth-Protocol  : PAP
RADIUS Authorization : Enabled
Local Authorization   : Enabled

DGS-3000-26TC:admin#
```

37-5 enable jwac redirect**Description**

This command is used to enable JWAC redirect. When **redirect quarantine_server** is enabled, the unauthenticated host will be redirected to a quarantine server when it tries to access a random URL. When redirect **jwac_login_page** is enabled, the unauthenticated host will be redirected to the **jwac_login_page** on the Switch to finish authentication.

When enable redirect to quarantine server is in effect, a quarantine server must be configured first.

Format**enable jwac redirect**

Parameters

None.

Restrictions

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

Example

To enable JWAC redirect:

```
DGS-3000-26TC:admin#enable jwac redirect
Command: enable jwac redirect

Success.

DGS-3000-26TC:admin#
```

37-6 disable jwac redirect

Description

This command is used to disable JWAC redirect. When redirect is disabled, only access to **quarantine_server** and the **jwac_login_page** from an unauthenticated host is allowed, all other Web access will be denied.

Format

disable jwac redirect

Parameters

None.

Restrictions

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

Example

To disable JWAC redirect:

```
DGS-3000-26TC:admin#disable jwac redirect
Command: disable jwac redirect

Success.

DGS-3000-26TC:admin#
```

37-7 config jwac redirect

Description

This command is used to configure redirect destination and delay time before an unauthenticated host is redirected to the quarantine server or the JWAC login web page. The unit of delay time is seconds. 0 means no delaying the redirect.

Format

config jwac redirect {destination [quarantine_server | jwac_login_page] | delay_time <sec 0-10>}(1)

Parameters

destination - Specifies the destination which the unauthenticated host will be redirected to.

quarantine_server - Specifies the unauthenticated host will be redirected to the quarantine_server.

jwac_login_page - Specifies the unauthenticated host will be redirected to the jwac_login_page.

delay_time - Specifies the time interval after which the unauthenticated host will be redirected.

<sec 0-10> - Specifies the time interval after which the unauthenticated host will be redirected. The delay time must be between 0 and 10 seconds.

Restrictions

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

Example

To configure JWAC redirect destination to JWAC login web page and a delay time of 5 seconds:

```
DGS-3000-26TC:admin#config jwac redirect destination jwac_login_page delay_time
5
Command: config jwac redirect destination jwac_login_page delay_time 5

Success.

DGS-3000-26TC:admin#
```

37-8 enable jwac forcible_logout

Description

This command is used to enable JWAC forcible logout. When enabled, a Ping packet from an authenticated host to the JWAC Switch with TTL=1 will be regarded as a logout request, and the host will be moved back to unauthenticated state.

Format

enable jwac forcible_logout

Parameters

None.

Restrictions

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

Example

To enable JWAC forcible logout:

```
DGS-3000-26TC:admin#enable jvac forcible_logout
Command: enable jvac forcible_logout

Success.

DGS-3000-26TC:admin#
```

37-9 disable jvac forcible_logout

Description

This command is used to disable JWAC forcible logout.

Format

disable jvac forcible_logout

Parameters

None.

Restrictions

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

Example

To disable JWAC forcible logout:

```
DGS-3000-26TC:admin#disable jvac forcible_logout
Command: disable jvac forcible_logout

Success.

DGS-3000-26TC:admin#
```

37-10 enable jwac udp_filtering

Description

This command is used to enable the JWAC UDP filtering function. When UDP filtering is enabled, all UDP and ICMP packets except DHCP and DNS packets from unauthenticated hosts will be dropped.

Format

enable jwac udp_filtering

Parameters

None.

Restrictions

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

Example

To enable JWAC UDP filtering:

```
DGS-3000-26TC:admin#enable jwac udp_filtering
Command: enable jwac udp_filtering

Success.

DGS-3000-26TC:admin#
```

37-11 disable jwac udp_filtering

Description

This command is used to disable JWAC UDP filtering.

Format

disable jwac udp_filtering

Parameters

None.

Restrictions

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

Example

To disable JWAC UDP filtering:

```
DGS-3000-26TC:admin#disable jwac udp_filtering
Command: disable jwac udp_filtering

Success.

DGS-3000-26TC:admin#
```

37-12 enable jwac quarantine_server_monitor

Description

This command is used to enable the JWAC quarantine server monitor. When enabled, the JWAC switch will monitor the quarantine server to ensure the server is okay. If the Switch detects no quarantine server, it will redirect all unauthenticated HTTP accesses to the JWAC Login Page forcibly if the redirect is enabled and the redirect destination is configured to be quarantine server.

Format

enable jwac quarantine_server_monitor

Parameters

None.

Restrictions

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

Example

To enable JWAC quarantine server monitoring:

```
DGS-3000-26TC:admin#enable jwac quarantine_server_monitor
Command: enable jwac quarantine_server_monitor

Success.

DGS-3000-26TC:admin#
```

37-13 disable jwac quarantine_server_monitor

Description

This command is used to disable JWAC quarantine server monitoring.

Format

disable jwac quarantine_server_monitor

Parameters

None.

Restrictions

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

Example

To disable JWAC quarantine server monitoring:

```
DGS-3000-26TC:admin#disable jwac quarantine_server_monitor
Command: disable jwac quarantine_server_monitor

Success.

DGS-3000-26TC:admin#
```

37-14 config jwac quarantine_server_error_timeout

Description

This command is used to set the quarantine server error timeout. When the quarantine server monitor is enabled, the JWAC switch will periodically check if the quarantine works okay. If the Switch does not receive any response from quarantine server during the configured error timeout, the Switch then regards it as not working properly.

Format

config jwac quarantine_server_error_timeout <sec 5-300>

Parameters

<sec 5-300> - Specifies the error timeout interval.

Restrictions

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

Example

To set the quarantine server error timeout:

```
DGS-3000-26TC:admin#config jwac quarantine_server_error_timeout 60
Command: config jwac quarantine_server_error_timeout 60

Success.

DGS-3000-26TC:admin#
```

37-15 config jwac virtual_ip

Description

This command is used to configure JWAC virtual IP addresses used to accept authentication requests from an unauthenticated host. The virtual IP of JWAC is used to accept authentication request from unauthenticated host. Only requests sent to this IP will get correct responses. This IP does not respond to ARP requests or ICMP packets.

Format

```
config jwac virtual_ip <ipaddr> {url [<string 128> | clear]}
```

Parameters

<ipaddr> - Specifies the IP address of the virtual IP.
url - (Optional) Specifies the URL of the virtual IP.
 <string 128> - Specifies the URL of the virtual IP.
 clear - Specifies to clear the URL of the virtual IP.

Restrictions

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

Example

To configure a JWAC virtual IP address of 1.1.1.1 to accept authentication requests from an unauthenticated host:

```
DGS-3000-26TC:admin#config jwac virtual_ip 1.1.1.1
Command: config jwac virtual_ip 1.1.1.1

Success.

DGS-3000-26TC:admin#
```

37-16 config jwac update_server

Description

This command is used to add or delete a server network address to which the traffic from an unauthenticated client host will not be blocked by the JWAC Switch. Any servers running ActiveX need to be able to have access to accomplish authentication. Before the client passes authentication, it should be added to the Switch with its IP address. For example, the client may need to access update.microsoft.com or some sites of the Anti-Virus software companies to check whether the OS or Anti-Virus software of the client are the latest; and so IP addresses of update.microsoft.com and of Anti-Virus software companies need to be added in the Switch.

Format

```
config jwac update_server [add | delete] ipaddress <network_address> {[tcp_port
<port_number 1-65535> | udp_port <port_number 1-65535>]}
```

Parameters

add - Specifies to add a network address to which the traffic will not be blocked. Up to 100 network addresses can be added.

delete - Specifies to delete a network address to which the traffic will not be blocked.

ipaddress - Specifies the network address to add or delete.

<network_address> - Enter the network address here.

tcp_port - (Optional) Specifies a TCP port number between 1 and 65535.

<port_number 1-65535> - Specifies a TCP port value between 1 and 65535.

udp_port - (Optional) Specifies a UDP port number between 1 and 65535.

<port_number 1-65535> - Specifies a UDP port value between 1 and 65535.

Restrictions

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

Example

To configure the update servers:

```
DGS-3000-26TC:admin#config jwac update_server add ipaddress 10.1.1.1/8
Command: config jwac update_server add ipaddress 10.1.1.1/8

Update Server 10.0.0.0/8 is added.

Success.

DGS-3000-26TC:admin#
```

37-17 config jwac switch_http_port

Description

This command is used to configure the TCP port which the JWAC switch listens to. This port number is used in the second stage of the authentication. PC users will connect to the page on the Switch to input the user name and password. If not specified, the default port number is 80. If no protocol is specified, the protocol is HTTP.

HTTP cannot run on TCP port 443, and HTTPS cannot run on TCP port 80.

Format

config jwac switch_http_port <tcp_port_number 1-65535> {[http | https]}

Parameters

<tcp_port_number 1-65535> - Specifies a TCP port which the JWAC switch listens to and uses to finish the authenticating process.

http - (Optional) Specifies the JWAC run HTTP protocol on this TCP port.

https - (Optional) Specifies the JWAC run HTTPS protocol on this TCP port.

Restrictions

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

Example

To configure the TCP port which the JWAC switch listens to:

```
DGS-3000-26TC:admin#config jwac switch_http_port 8888 http
Command: config jwac switch_http_port 8888 http

Success.

DGS-3000-26TC:admin#
```

37-18 config jwac ports

Description

This command is used to configure port state of JWAC.

Format

config jwac ports [**<portlist>** | **all**] {**state** [**enable** | **disable**] | **max_authenticating_host** **<value 0-50>** | **aging_time** [**infinite** | **<min 1-1440>**] | **idle_time** [**infinite** | **<min 1-1440>**] | **block_time** [**<sec 0-300>**] | **auth_mode** [**host_based** | **port_based**]}(1)

Parameters

<portlist> - Specifies a port range for setting the JWAC state.

all - Specifies to configure all switch ports' JWAC state.

state - Specifies the port state of JWAC.

enable - Specifies to enable the JWAC port state.

disable - Specifies to disable the JWAC port state.

max_authenticating_host - Specifies the maximum number of hosts that can process authentication on each port at the same time. The default value is 50.

<value 0-50> - Specifies the maximum number of authenticating hosts, between 0 and 50.

aging_time - Specifies a time period during which an authenticated host will keep in authenticated state.

infinite - Specifies to indicate the authenticated host on the port will never ageout.

<min 1-1440> - Specifies an aging time between 1 and 1440 minutes. The default value is 1440 minutes.

idle_time - If there is no traffic during idle time, the host will be moved back to unauthenticated state.

infinite - Specifies to indicate the idle state of the authenticated host on the port will never be checked. The default value is infinite.

<min 1-1440> - Specifies an idle time between 1 and 1440 minutes.

block_time - If a host fails to pass the authentication, it will be blocked for a period specified by the blocking time. The default value is 60 seconds.

<sec 0-300> - Specifies a blocking time value between 0 and 300.

auth_mode - Specifies the port authentication mode.

host_based - Specifies the port authentication mode as host-based.

port_based - Specifies the port authentication mode as port-based.

Restrictions

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

Example

To configure the JWAC port state:

```
DGS-3000-26TC:admin#config jwac ports 1-9 state enable
Command: config jwac ports 1-9 state enable

Success.

DGS-3000-26TC:admin#
```

37-19 show jwac ports**Description**

This command is used to display the port configuration of JWAC.

Format

show jwac ports {<portlist>}

Parameters

<portlist> - (Optional) Specifies a port range to show the configuration of JWAC.

Restrictions

None.

Example

To display JWAC ports 1 to 4:

```
DGS-3000-26TC:admin#show jwac ports 1-4
Command: show jwac ports 1-4

  Port   State      Aging Time   Idle Time   Block Time   Auth Mode   Max
        (min)      (min)       (sec)
-----
  1      Enabled    1440        Infinite    60           Host-Based  50
  2      Enabled    1440        Infinite    60           Host-Based  50
  3      Enabled    1440        Infinite    60           Host-Based  50
  4      Enabled    1440        Infinite    60           Host-Based  50

DGS-3000-26TC:admin#
```

37-20 config jwac radius_protocol**Description**

This command is used to specify the RADIUS protocol used by JWAC to complete RADIUS authentication.

JWAC shares other RADIUS configurations with 802.1X. When using this command to set the RADIUS protocol, make sure the RADIUS server added by the **config radius** command supports the protocol.

Format

config jwac radius_protocol [local | eap_md5 | pap | chap | ms_chap | ms_chapv2]

Parameters

| |
|--|
| local - Specifies the JWAC switch uses the local user DB to complete the authentication. |
| eap_md5 - Specifies the JWAC switch uses EAP MD5 to communicate with the RADIUS server. |
| pap - Specifies the JWAC switch uses PAP to communicate with the RADIUS server. |
| chap - Specifies the JWAC switch uses CHAP to communicate with the RADIUS server. |
| ms_chap - Specifies the JWAC switch uses MS-CHAP to communicate with the RADIUS server. |
| ms_chapv2 - Specifies the JWAC switch uses MS-CHAPv2 to communicate with the RADIUS server. |

Restrictions

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

Example

To configure the RADIUS protocol used by JWAC:

```
DGS-3000-26TC:admin#config jwac radius_protocol ms_chapv2
Command: config jwac radius_protocol ms_chapv2

Success.

DGS-3000-26TC:admin#
```

37-21 create jwac user

Description

This command is used to create JWAC users in the local database. When "local" is chosen while configuring the JWAC RADIUS protocol, the local database will be used.

Format

create jwac user <username 15> {vlan <vlanid 1-4094>}

Parameters

| |
|---|
| <username 15> - Specifies the user name to be created. |
| vlan - (Optional) Specifies the target VLAN ID for the authenticated host which uses this user account to pass authentication. |
| <vlanid 1-4094> - Specifies the target VLAN ID for the authenticated host which uses this user account to pass authentication. The VLAN ID value must be between 1 and 4094. |

Restrictions

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

Example

To create a JWAC user in the local database:

```
DGS-3000-26TC:admin#create jwac user 112233
Command: create jwac user 112233

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

DGS-3000-26TC:admin#
```

37-22 config jwac user

Description

This command is used to configure a JWAC user.

Format

config jwac user <username 15> {vlan <vlanid 1-4094>}

Parameters

<username 15> - Specifies the user name to be configured.

vlan - (Optional) Specifies the target VLAN ID for the authenticated host which uses this user account to pass authentication.

<vlanid 1-4094> - Specifies the target VLAN ID for the authenticated host which uses this user account to pass authentication. The VLAN ID value must be between 1 and 4094.

Restrictions

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

Example

To configure a JWAC user:

```
DGS-3000-26TC:admin#config jwac user 112233
Command: config jwac user 112233

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

DGS-3000-26TC:admin
```

37-23 delete jwac

Description

This command is used to delete JWAC users from the local database.

Format

delete jwac [user <username 15> | all_users]

Parameters

user - Specifies the user name to be deleted.

<username 15> - Specifies the user name to be deleted. The user name can be up to 15 characters long.

all_users - Specifies all user accounts in the local database will be deleted.

Restrictions

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

Example

To delete a JWAC user from the local database:

```
DGS-3000-26TC:admin#delete jwac user 112233
Command: delete jwac user 112233

Success.

DGS-3000-26TC:admin#
```

37-24 show jwac user

Description

This command is used to display JWAC users in the local database.

Format

show jwac user

Parameters

None.

Restrictions

None.

Example

To display the current JWAC local users:

```
DGS-3000-26TC:admin#show jwac user
Command: show jwac user

User Name          Password          VID
-----
112233             112233           -
123                123              1

Total Entries:2

DGS-3000-26TC:admin#
```

37-25 clear jwac auth_state**Description**

This command is used to clear authentication entries.

Format

```
clear jwac auth_state [ports [all | <portlist>] {authenticated | authenticating | blocked} |
mac_addr <macaddr>]
```

Parameters

ports - Specifies the port range to delete hosts on.
all - Specifies to delete all ports.
<portlist> - Specifies range of ports to delete.
authenticated - (Optional) Specifies the state of host to delete.
authenticating - (Optional) Specifies the state of host to delete.
blocked - (Optional) Specifies the state of host to delete.

mac_addr - Deletes a specified host with this MAC address.
<macaddr> - Enter the MAC address here.

Restrictions

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

Example

To delete authentication entries:

```
DGS-3000-26TC:admin#clear jwac auth_state ports all blocked
Command: clear jwac auth_state ports all blocked

Success.

DGS-3000-26TC:admin#
```

37-26 show jwac auth_state ports

Description

This command is used to display information for JWAC client hosts.

Format

show jwac auth_state ports {<portlist>}

Parameters

<portlist> - (Optional) Specifies a port range to show the JWAC authentication entries.

If no port is specified, the JWAC authentication state will be displayed for all ports.

Restrictions

None.

Example

To display JWAC authentication entries for ports 1 to 4:

```
DGS-3000-26TC:admin#show jwac auth_state ports 1-4
Command: show jwac auth_state ports 1-4
Pri - Priority. State - A:Authenticated, B:Blocked, -:Authenticating
Time - Aging Time/Idle Time for authenticated entries.
```

| Port | MAC Address | State | VID | Pri | Time | IP | User Name |
|------|----------------------|-------|------|-----|---------|---|-----------|
| 1 | 00-00-00-00-00-01 | A | 20 | 3 | 1440/30 | 192.168.101.239 | jack |
| 1 | 00-00-00-00-00-02 | A | 1234 | - | 1440/30 | 172.18.61.242 | tom |
| 1 | 00-00-00-00-00-03 | B | - | - | -/40 | 172.18.61.243 | user |
| 1 | 00-00-00-00-00-04 | - | - | - | 10 | - | - |
| 2 | 00-00-00-00-00-10(P) | A | 1234 | - | 1440/30 | 10.10.10.90 | admin |
| 3 | 00-00-00-00-00-20(P) | - | - | - | 1440/30 | 10.10.10.131 | - |
| 3 | 00-00-00-00-00-21(P) | B | - | - | -/29 | 172.18.61.133 | lina |
| 4 | 00-00-00-00-00-21(P) | A | 1234 | 5 | 1440/30 | 3000:2000:3000:aabb:bbcc:ccdd:d dee:eeff | name |

```
Total Authenticating Hosts      : 2
Total Authenticated Hosts       : 4
Total Blocked Hosts             : 2

DGS-3000-26TC:admin#
```

37-27 config jwac authorization attributes

Description

This command is used to enable or disable acceptance of authorized configuration. When the authorization is enabled for JWAC's RADIUS, the authorized data assigned by the RADIUS server will be accepted if the global authorization network is enabled. When the authorization is enabled for JWAC's local, the authorized data assigned by the local database will be accepted.

Format

config jwac authorization attributes {radius [enable | disable] | local [enable | disable]}(1)

Parameters

radius - If specifies 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 RADUIS server to be accepted.

disable - Specifies to disable authorized data assigned by the RADUIS server from being accepted.

local - If specifies 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 disable the configuration authorized from the local database:

```
DGS-3000-26TC:admin#config jwac authorization attributes local disable
Command: config jwac authorization attributes local disable

Success.

DGS-3000-26TC:admin#
```

37-28 show jwac update_server

Description

This command is used to display the JWAC update server.

Format

show jwac update_server

Parameters

None.

Restrictions

None.

Example

To display the JWAC update server:

```
DGS-3000-26TC:admin#show jwac update_server
Command: show jwac update_server

Index  IP                TCP/UDP  Port  State
-----  -----
1      172.18.0.0/21    TCP      1     Active
2      172.18.0.0/21    TCP      2     Active
3      172.18.0.0/21    TCP      3     Active

DGS-3000-26TC:admin#
```

37-29 config jwac authentication_page element

Description

This command is used by administrators to customize the JWAC authenticate page.

Format

```
config jwac authentication_page element [japanese | english] [default | page_title <desc 128> | login_window_title <desc 32> | user_name_title <desc 16> | password_title <desc 16> | logout_window_title <desc 32> | notification_line <value 1-5> <desc 128>]
```

Parameters

| | |
|----------------------------|--|
| japanese | - Specifies to change to the Japanese page. |
| english | - Specifies to change to the English page. |
| default | - Specifies to reset the page element to default. |
| page_title | - Specifies the title of the authenticate page. |
| <desc 128> | - Specifies the title of the authenticate page. The page title description can be up to 128 characters long. |
| login_window_title | - Specifies the login window title of the authenticate page. |
| <desc 32> | - Specifies the login window title of the authenticate page. The login window title description can be up to 32 characters long. |
| user_name_title | - Specifies the user name title of the authenticate page. |
| <desc 16> | - Specifies the user name title of the authenticate page. The user name title description can be up to 16 characters long. |
| password_title | - Specifies the password title of the authenticate page. |
| <desc 16> | - Specifies the password title of the authenticate page. The password title description can be up to 16 characters long. |
| logout_window_title | - Specifies the logout window title mapping of the authenticate page. |
| <desc 32> | - Specifies the logout window title mapping of the authenticate page. The logout window title description can be up to 32 characters long. |
| notification_line | - Specifies this parameter to set the notification information by line in authentication Web pages. |
| <value 1-5> | - Specifies a notification line value between 1 and 5. |
| <desc 128> | - Specifies a notification line description up to 128 characters long. |

Restrictions

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

Example

To customize the authenticate page:

```
DGS-3000-26TC:admin# config jwac authentication_page element japanese
page_title "ディーリンクジャパン株式会社" login_window_title "JWAC 認証"
user_name_title "ユーザ名" password_title "パスワード" logout_window_title "ログアウト"

Command: config jwac authentication_page element japanese page_title "ディーリンク
ジャパン株式会社" login_window_title "JWAC 認証" user_name_title "ユーザ名"
password_title "パスワード" logout_window_title "ログアウト"

Success.

DGS-3000-26TC:admin#
```

37-30 config jwac authenticate_page

Description

This command is used by administrators to decide which authenticate page to use.

Format

config jwac authenticate_page [japanese | english]

Parameters

japanese - Specifies to change to the Japanese page.

english - Specifies to change to the English page. This is the default page.

Restrictions

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

Example

To customize the authenticate page:

```
DGS-3000-26TC:admin#config jwac authenticate_page japanese
Command: config jwac authenticate_page japanese

Success.

DGS-3000-26TC:admin#
```

37-31 show jwac authenticate_page

Description

This command is used to display the element mapping of the customized authenticate page.

Format

show jwac authenticate_page

Parameters

None.

Restrictions

None.

Example

To display the element mapping of the customized authenticate page:

```
DGS-3000-26TC:admin#show jwac authenticate_page
Command: show jwac authenticate_page

  Current Page : English Version
English Page Element
-----
Page Title           :
Login Window Title   : Authentication Login
User Name Title      : User Name
Password Title       : Password
Logout Window Title  : Logout from the network
Notification         :

Japanese Page Element
-----
Page Title           :
Login Window Title   : 社内 LAN 認証ログイン
User Name Title      : ユーザ ID
Password Title       : パスワード
CTRL+C  ESC  c  Quit  SPACE  n  Next Page  ENTER  Next Entry  a  All
```

Chapter 38 Jumbo Frame Command List

enable jumbo_frame
disable jumbo_frame
show jumbo_frame

38-1 enable jumbo_frame

Description

This command is used to configure the jumbo frame setting as enable.

Format

enable jumbo_frame

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable the Jumbo frame:

```
DGS-3000-26TC:admin#enable jumbo_frame
Command: enable jumbo_frame

The maximum size of jumbo frame is 12288 bytes.
Success.

DGS-3000-26TC:admin#
```

38-2 disable jumbo_frame

Description

This command is used to configure the jumbo frame setting as disable.

Format

disable jumbo_frame

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To disable the Jumbo frame:

```
DGS-3000-26TC:admin#disable jumbo_frame
Command: disable jumbo_frame

Success.

DGS-3000-26TC:admin#
```

38-3 show jumbo_frame

Description

This command is used to display the current configuration of jumbo frame.

Format

show jumbo_frame

Parameters

None.

Restrictions

None.

Example

To show the Jumbo frame:

```
DGS-3000-26TC:admin#show jumbo_frame
Command: show jumbo_frame

Jumbo Frame State : Disabled
Maximum Frame Size : 1536 Bytes

DGS-3000-26TC:admin#
```


Chapter 39 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]}
```

39-1 enable l2protocol_tunnel

Description

This command is used to enable the Layer 2 protocol tunneling function.

Format

```
enable l2protocol_tunnel
```

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable the Layer 2 protocol tunneling function:

```
DGS-3000-26TC:admin#enable l2protocol_tunnel
Command: enable l2protocol_tunnel

Success.

DGS-3000-26TC:admin#
```

39-2 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 Layer 2 protocol tunneling function:

```
DGS-3000-26TC:admin#disable l2protocol_tunnel
Command: disable l2protocol_tunnel

Success.

DGS-3000-26TC:admin#
```

39-3 config l2protocol_tunnel ports

Description

This command is used to configure Layer 2 protocol tunneling on ports. Layer 2 protocol tunneling is used to tunnel Layer 2 protocol packet. If a Layer 2 protocol is tunnel-enabled on an UNI, once received the PDU on this port, the multicast destination address of the PDU will be replaced by Layer 2 protocol tunneling multicast address. The Layer 2 protocol tunneling 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 too. The S-TAG is assigned according 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 Layer 2 protocol tunneling to be configured.

all – Specifies to have all ports to be configured

type - Specifies the type of the ports.

uni - Specifies the ports as UNI ports.

tunneled_protocol - Specifies tunneled protocols 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 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 - 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> - The range of the threshold value is 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 - Disables tunnel on it.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the STP tunneling on ports 1-4:

```
DGS-3000-26TC: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-3000-26TC:admin#
```

39-4 show l2protocol_tunnel

Description

This command is used to display Layer 2 protocol tunneling information.

Format

show l2protocol_tunnel {[uni | nni]}

Parameters

uni - (Optional) Specifies to show UNI detail information, include tunneled and dropped PDU statistic.

nni - (Optional) Specifies to show NNI detail information, include de-capsulated Layer 2 PDU statistic.

Restrictions

None.

Example

To show Layer 2 protocol tunneling information summary:

```
DGS-3000-26TC:admin#show l2protocol_tunnel
Command: show l2protocol_tunnel

Global State : Enabled
UNI Ports    : 1-4
NNI Ports    :

DGS-3000-26TC:admin#
```

To show Layer 2 protocol tunneling information summary:

```
DGS-3000-26TC: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-3000-26TC:admin#
```

Chapter 40 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> |

40-1 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 is belong to 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-3000-26TC:admin#create link_aggregation group_id 1 type lacp
Command: create link_aggregation group_id 1 type lacp

Success.

DGS-3000-26TC:admin#
```

40-2 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

group_id - Specifies the group id. The number of link aggregation groups is project dependency. The group number identifies each of the groups.
<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-3000-26TC:admin#delete link_aggregation group_id 3
Command: delete link_aggregation group_id 3

Success.

DGS-3000-26TC:admin#
```

40-3 config link_aggregation group_id

Description

This command is used to configure a previously created link aggregation group.

Format

config link_aggregation group_id <value> {master_port <port> | ports <portlist> | state [enable | disable]}

Parameters

group_id - Specifies the group ID. The group number identifies each of the groups.
<value> - Enter the group ID value here. For the DGS-3000-10TCn this value must be between 1 and 5. For the DGS-3000-26TC, this value must be between 1 and 13.

master_port - (Optional) Master port ID. Specifies which port (by port number) of the link aggregation group will be the master port. All of the ports in a link aggregation group will share the port configuration with the master port.
<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 port 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, the default state is disabled. If configure LACP group, the ports' state machine will start.

enable - Enables the specified link aggregation group.

disable - Disables the specified link aggregation group.

Restrictions

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

Example

To define a load-sharing group of ports:

```
DGS-3000-26TC: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-3000-26TC:admin#
```

40-4 config link_aggregation algorithm

Description

This command is used to configure the part of the packet examined by the Switch when selecting the egress port for transmitting load-sharing data. 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 - Indicates that the Switch should examine the MAC source address.

mac_destination - Indicates that the Switch should examine the MAC destination address.

mac_source_dest - Indicates that the Switch should examine the MAC source and destination address.

ip_source - Indicates that the Switch should examine the IP source address.

ip_destination - Indicates that the Switch should examine the IP destination address.

ip_source_dest - Indicates that the Switch should examine the IP source 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-3000-26TC:admin#config link_aggregation algorithm mac_source_dest
Command: config link_aggregation algorithm mac_source_dest

Success.

DGS-3000-26TC:admin#
```

40-5 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) Allows you to specify the display of link aggregation by the algorithm in use by that group.

If no parameter specified, system will display all link aggregation information.

Restrictions

None.

Example

Link aggregation group enable:

```
DGS-3000-26TC: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-3000-26TC:admin#
```

Link aggregation group enable and no member linkup:


```
DGS-3000-26TC: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-3000-26TC:admin#
```

Link aggregation group disabled:

```
DGS-3000-26TC: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-3000-26TC:admin#
```

40-6 config lacp_port

Description

This command is used to configure per-port LACP mode.

Format

config lacp_port <portlist> mode [active | passive]

Parameters

lacp_port - Specifies a range of ports to be configured.
<portlist> - Enter the list of port 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 config port LACP mode:

```
DGS-3000-26TC:admin#config lacp_port 1-12 mode active
command: config lacp_port 1-12 mode active

Success.

DGS-3000-26TC:admin#
```

40-7 show lacp_port

Description

This command is used to display the current mode of LACP of the ports.

Format

show lacp_port <portlist>

Parameters

lacp_port - Specifies a range of ports to be configured.

<portlist> - Enter the list of ports used for this configuration here.

If no parameter specified, the system will display current LACP and all port status.

Restrictions

None.

Example

To show port lacp mode:

```
DGS-3000-26TC: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 |

```
DGS-3000-26TC:admin#
```

Chapter 41 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_mdix 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>} |
| 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}] state [enable disable] |
| show lldp med ports {<portlist>} |
| show lldp med |
| show lldp med local_ports {<portlist>} |
| show lldp med remote_ports {<portlist>} |

41-1 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-3000-26TC:admin#enable lldp
Command: enable lldp

Success.

DGS-3000-26TC:admin#
```

41-2 disable lldp

Description

This command is used to stop sending and receiving of LLDP advertisement packet.

Format

disable lldp

Parameters

None.

Restrictions

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

Example

To disable LLDP:

```
DGS-3000-26TC:admin#disable lldp
Command: disable lldp

Success.

DGS-3000-26TC:admin#
```

41-3 config lldp

Description

This command is used to change the 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 - Changes the interval between consecutive transmissions of LLDP advertisements on any given port. The default setting 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 setting 4.
<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 setting 2 seconds.
<sec 1-8192> - Enter the transmit delay value here. This value must be between 1 and 8192 seconds.

reinit_delay - Specifies the the minimum time of reinitialization delay interval. The default setting 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-3000-26TC:admin#config lldp message_tx_interval 30
Command: config lldp message_tx_interval 30

Success.

DGS-3000-26TC:admin#
```

41-4 config lldp notification_interval

Description

This command is used to configure the timer of notification interval for sending notification to configured SNMP trap receiver(s).

Format

config lldp notification_interval <sec 5-3600>

Parameters

notification_interval - Specifies the timer of notification interval for sending notification to configured SNMP trap receiver(s). The default setting is 5 seconds.
<sec 5-3600> - Enter the notification interval value here. This value must be between 5 and 3600 seconds.

Restrictions

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

Example

To changes the notification interval to 10 second:

```
DGS-3000-26TC:admin#config lldp notification_interval 10
Command: config lldp notification_interval 10

Success.

DGS-3000-26TC:admin#
```

41-5 config lldp ports

Description

This command is used to configure each port for sending a notification to configure 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 - Enables or disables the SNMP trap notification of LLDP data changes detected on advertisements received from neighbor devices. The default notification state is disabled.

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.

admin_status - Specifies the per-port transmit and receive modes.

tx_only - Configure the specified port(s) to transmit LLDP packets.

rx_only - Configures the specified port(s) to receive LLDP packets from neighbors.
tx_and_rx - Configures the specified port(s) to both transmit and receive LLDP packets.
disable - Disable LLDP packet transmit and receive 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) This TLV optional data type indicates that LLDP agent should transmit Port Description TLV on the port. The default state is disabled.

system_name - (Optional) This TLV optional data type includes indicates that LLDP agent should transmit System Name TLV. The default state is disabled.

system_description - (Optional) This TLV optional data type includes indicates that LLDP agent should transmit System Description TLV. The default state is disabled.

system_capabilities - (Optional) This TLV optional data type includes indicates that LLDP agent should transmit System Capabilities TLV. The system capability will indicate whether the device provides repeater, bridge, or router function, and whether the provided functions are currently enabled. The default state is disabled.

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 - This TLV optional data type determines 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 - This TLV optional data type determines whether the IEEE 802.1 organizationally defined port and protocol VLAN ID TLV transmission is allowed on a given LLDP transmission capable port. 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 - This TLV optional data type indicates whether the corresponding Local System's VLAN name instance will be transmitted on the port. If a port is associated with multiple VLANs, those enabled VLAN ID will be advertised. 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 VLAN name will be enabled.

disable - Specifies that the Dot1 TLV VLAN name will be disabled.

dot1_tlv_protocol_identity - This TLV optional data type indicates whether the corresponding Local System's Protocol Identity instance will be transmitted on the port. The Protocol Identity TLV provides a way for stations to advertise protocols that are important to the operation of the network. Such as Spanning Tree Protocol, the Link Aggregation Control Protocol, and numerous vendor proprietary variations 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) This TLV optional data type indicates that LLDP agent should transmit MAC/PHY configuration/status TLV. This type indicates it is possible for two ends of an IEEE 802.3 link to be configured with different 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) This TLV optional data type indicates that LLDP agent should transmit Link Aggregation TLV. This type indicates the current link aggregation status of IEEE 802.3 MACs. More precisely, the information should include whether the port is capable of doing link aggregation, whether the port is aggregated in a aggregated link, and the aggregated port ID. The default state is disabled.

power_via_mdi - (Optional) This TLV optional data type indicates that 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) This TLV optional data type indicates that 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-3000-26TC:admin#config lldp ports 1-5 notification enable
Command: config lldp ports 1-5 notification enable

Success.

DGS-3000-26TC:admin#
```

To configure port 1-5 to transmit and receive:

```
DGS-3000-26TC:admin#config lldp ports 1-5 admin_status tx_and_rx
Command: config lldp ports 1-5 admin_status tx_and_rx

Success.

DGS-3000-26TC:admin#
```

To enable ports 1-2 for manage address entry:

```
DGS-3000-26TC: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-3000-26TC:admin#
```

To configure exclude the system name TLV from the outbound LLDP advertisements for all ports:

```
DGS-3000-26TC:admin#config lldp ports all basic_tlvs system_name enable
Command: config lldp ports all basic_tlvs system_name enable

Success.

DGS-3000-26TC:admin#
```

To configure exclude the vlan name TLV from the outbound LLDP advertisements for all ports:

```
DGS-3000-26TC:admin#config lldp ports all dot1_tlv_pvid enable
Command: config lldp ports all dot1_tlv_pvid enable

Success.

DGS-3000-26TC:admin#
```

To configure exclude the port and protocol VLAN ID TLV from the outbound LLDP advertisements for all ports:

```
DGS-3000-26TC: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-3000-26TC:admin#
```

To configure exclude the VLAN name TLV from the outbound LLDP advertisements for all ports:

```
DGS-3000-26TC: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-3000-26TC:admin#
```

To configure exclude the protocol identity TLV from the outbound LLDP advertisements for all ports:

```
DGS-3000-26TC:admin#config lldp ports all dot1_tlv_protocol_identity all enable
Command: config lldp ports all dot1_tlv_protocol_identity all enable

Success.

DGS-3000-26TC:admin#
```

To configure exclude the MAC/PHY configuration/status TLV from the outbound LLDP advertisements for all ports:

```
DGS-3000-26TC: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-3000-26TC:admin#
```

41-6 config lldp forward_message

Description

This command is used to configure forwarding of LLDP PDU packet when LLDP is disabled.

Format

config lldp forward_message [enable | disable]

Parameters

None.

Restrictions

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

Example

To configure LLDP to forward LLDP PDUs:

```
DGS-3000-26TC:admin#config lldp forward_message enable
Command: config lldp forward_message enable

Success.

DGS-3000-26TC:admin#
```

41-7 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-3000-26TC:admin#show lldp
Command: show lldp

LLDP System Information
  Chassis ID Subtype      : MAC Address
  Chassis ID              : 00-01-02-03-04-00
  System Name             :
  System Description      : Gigabit Ethernet Switch
  System Capabilities     : Repeater, Bridge

LLDP Configurations
  LLDP Status             : Enabled
  LLDP Forward Status     : Enabled
  Message TX Interval    : 30
  Message TX Hold Multiplier: 4
  ReInit Delay           : 2
  TX Delay                : 2
  Notification Interval   : 5

DGS-3000-26TC:admin#
```

41-8 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 used for the display.

<ipaddr> - Enter the IPv4 address used for this configuration here.

ipv6 - (Optional) Specifies the IPv6 address used for the display.

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

Restrictions

None.

Example

To display management address information:

```
DGS-3000-26TC: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               : 1.3.6.1.4.1.171.10.133.2.1
Advertising Ports : 1-2,5

DGS-3000-26TC:admin#
```

41-9 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 the port list is not specified, information for all the ports will be displayed.

Restrictions

None.

Example

To display the LLDP port 1 TLV option configuration:

```

DGS-3000-26TC: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-3000-26TC:admin#

```

41-10 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. When port list is not specified, information for all ports will be displayed.

mode - (Optional) Specifies the display mode.

brief - Displays the information in brief mode.

normal - Displays the information in normal mode. This is the default display mode.

detailed - Displays 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-3000-26TC: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                        : 00-01-02-03-04-01
Port Description                : D-Link DGS-3000-26TC R1.00.015
                                Port 1
Port PVID                      : 1
Management Address Count      : 1
    Subtype                    : IPv4
    Address                    : 10.90.90.90
    IF Type                    : IfIndex
    OID                        : 1.3.6.1.4.1.171.10.133.2.1

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-3000-26TC: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                   : 00-01-02-03-04-01
Port Description          : D-Link DGS-3000-26TC R1.00.015
                           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)
Link Aggregation         : (See Detail)
Maximum Frame Size       : 1536

DGS-3000-26TC:admin#
```

To display outbound LLDP advertisements for port 1 in brief mode:

```
DGS-3000-26TC: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                   : 00-01-02-03-04-01
Port Description          : D-Link DGS-3000-26TC R1.00.015
                           Port 1

DGS-3000-26TC:admin#
```

41-11 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. When port list is not specified, information for all ports will be displayed.

mode – (Optional) Specifies to display the information in various modes.
brief - Displays the information in brief mode.
normal - Displays the information in normal mode. This is the default display mode.
detailed - Displays the information in detailed mode.

Restrictions

None.

Example

To display remote table in brief mode:

```
DGS-3000-26TC: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-3000-26TC R1.00.015
                        Port 3

DGS-3000-26TC:admin#
```

To display remote table in normal mode:

```
DGS-3000-26TC: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-3000-26TC R1.00.015
                          Port 3
  System Name             :
  System Description      : Fast 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-3000-26TC:admin#
```

To display remote table in detailed mode:

```

DGS-3000-26TC: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-3000-26TC R1.00.015
                        Port 3
  System Name            :
  System Description     : Fast 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-3000-26TC:admin#

```

41-12 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-3000-26TC: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-3000-26TC:admin#
```

41-13 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. When port list is not specified, information for all ports will be displayed.

Restrictions

None.

Example

To display statistics information of port 1:

```
DGS-3000-26TC: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-3000-26TC:admin#
```

41-14 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> - Specifies a fast start repeat count value between 1 and 10. The default value is 4.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure a LLDP-MED fast start repeat count of 5:

```
DGS-3000-26TC:admin#config lldp_med fast_start repeat_count 5
Command: config lldp_med fast_start repeat_count 5

Success.

DGS-3000-26TC:admin#
```

41-15 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 - Enables the log state for LLDP-MED events.

disable - Disables the log state for LLDP-MED events. The default is disabled.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable the log state of LLDP-MED events:

```
DGS-3000-26TC:admin#config lldp_med log state enable
Command: config lldp_med log state enable

Success.

DGS-3000-26TC:admin#
```

41-16 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> - Specifies 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 - Enables the SNMP trap notification of topology change detected.

disable - Disables the SNMP trap notification of topology change detected. The default notification state is disabled.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable topology change notification on ports 1-2:

```
DGS-3000-26TC: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-3000-26TC:admin#
```

41-17 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> - Specifies a range of ports to be configured.

all - Specifies to set all ports in the system.

med_transmit_capabilities - Specifies to send the LLDP-MED TLV capabilities.

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 - Enables the transmitting of LLDP-MED TLVs.

disable - Disables the transmitting of LLDP-MED TLVs.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable transmitting all capabilities on all ports:

```
DGS-3000-26TC: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-3000-26TC:admin#
```

41-18 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) Specifies 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-3000-26TC: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 Network Policy TLV             :Enabled
LLDP-MED Extended Power Via MDI PSE TLV  :Enabled
LLDP-MED Inventory TLV                  :Enabled

DGS-3000-26TC:admin#
```

41-19 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-3000-26TC:admin#show lldp_med
Command: show lldp_med

LLDP-MED System Information:
  Device Class           : Network Connectivity Device
  Hardware Revision      : A1
  Firmware Revision      : 1.00.001
  Software Revision      : 1.00.015
  Serial Number          :
  Manufacturer Name      : D-Link
  Model Name             : DGS-3000-26TC Gigabit Ethernet S
  Asset ID               :

LLDP-MED Configuration:
  Fast Start Repeat Count : 4

LLDP-MED Log State:Enabled

DGS-3000-26TC:admin#
```

41-20 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) Specifies 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-3000-26TC: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         :Support
  Location Identification :Not Support
  Extended Power Via MDI PSE :Not Support
  Extended Power Via MDI PD :Not Support
  Inventory              :Support

Network Policy:
  None

Extended Power Via MDI:
  None

DGS-3000-26TC:admin#
```

41-21 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) Specifies a range of ports to be displayed.

Restrictions

None.

Example

To display remote entry information:

```

DGS-3000-26TC: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-3000-26TC:admin#
```

Chapter 42 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]

```

42-1 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) 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. 0 is a special value that specifies that the auto-recovery mechanism should be disabled. When the auto-recovery mechanism is disabled, a user would need to manually recover a disabled port. The default value for the recover timer is 60 seconds.

<value 0> - 0 is a special value that specifies that the auto-recovery mechanism should be disabled. 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) 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 setting is 10 seconds. The valid range is from 1 to 32767 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-3000-26TC:admin#config loopdetect recover_timer 0 interval 20 mode vlan-
based
Command: config loopdetect recover_timer 0 interval 20 mode vlan-based

Success.

DGS-3000-26TC:admin#
```

42-2 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

ports - Specifies the range of ports that LBD will be configured on.
<portlist> - Enter a list of ports
all - Specifies to set all ports in the system.

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-3000-26TC:admin#config loopdetect ports 1-5 state enable
Command: config loopdetect ports 1-5 state enable

Success.

DGS-3000-26TC:admin#
```

42-3 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-3000-26TC:admin#enable loopdetect
Command: enable loopdetect

Success.

DGS-3000-26TC:admin#
```

42-4 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-3000-26TC:admin#disable loopdetect
Command: disable loopdetect

Success.

DGS-3000-26TC:admin#
```

42-5 show loopdetect

Description

This command is used to display the LBD global configuration.

Format

show loopdetect

Parameters

None.

Restrictions

None.

Example

To show the LBD global settings:

```
DGS-3000-26TC: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
Function Version : 4.04

DGS-3000-26TC:admin#
```

42-6 show loopdetect ports

Description

This command is used to display the LBD per-port configuration.

Format

show loopdetect ports {<portlist>}

Parameters

ports - Specifies the range of member ports that will display the LBD settings.

<portlist> - Enter the list of port to be configured here.

If no port is specified, the configuration for all ports will be displayed.

Restrictions

None.

Example

To show the LBD settings on ports 1-9:

```
DGS-3000-26TC: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-3000-26TC:admin#
```

42-7 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 - There is no trap in the LBD function.

loop_detected - Trap will only be sent when the loop condition is detected.

loop_cleared - Trap will only be sent when the loop condition is cleared.

both - 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-3000-26TC:admin#config loopdetect trap both
Command: config loopdetect trap both

Success.

DGS-3000-26TC:admin#
```

42-8 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

state - Specifies the state of the LBD log feature.
enable - Enables the LBD log feature.
disable - Disables 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-3000-26TC:admin#config loopdetect log state enable
Command: config loopdetect log state enable

Success.

DGS-3000-26TC:admin#
```

Chapter 43 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>}
```

43-1 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-3000-26TC:admin#enable mac_notification
Command: enable mac_notification

Success.

DGS-3000-26TC:admin#
```

43-2 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-3000-26TC:admin#disable mac_notification
Command: disable mac_notification

Success.

DGS-3000-26TC:admin#
```

43-3 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 config the Switch's Mac address table notification global settings:

```
DGS-3000-26TC:admin#config mac_notification interval 1 historysize 500
Command: config mac_notification interval 1 historysize 500

Success.

DGS-3000-26TC:admin#
```

43-4 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 - Enables the port's MAC address table notification.

disable - Disables the port's MAC address table notification.

Restrictions

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

Example

To enable 7th port's mac address table notification:

```
DGS-3000-26TC:admin#config mac_notification ports 7 enable
Command: config mac_notification ports 7 enable

Success.

DGS-3000-26TC:admin#
```

43-5 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-3000-26TC:admin#show mac_notification
Command: show mac_notification

Global MAC Notification Settings

State          : Disabled
Interval       : 1
History Size   : 1

DGS-3000-26TC:admin#
```

43-6 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-3000-26TC: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 44 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]

```

44-1 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-3000-26TC:admin#enable mac_based_access_control
Command: enable mac_based_access_control

Success.

DGS-3000-26TC:admin#
```

44-2 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-3000-26TC:admin#disable mac_based_access_control
Command: disable mac_based_access_control

Success.

DGS-3000-26TC:admin#
```

44-3 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 - In RADIUS mode, the Switch will communicate with the RADIUS server using this password. The maximum length of the key is 16.
<password> - Enter the password used here. 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-3000-26TC:admin#config mac_based_access_control password switch
Command: config mac_based_access_control password switch

Success.

DGS-3000-26TC:admin#
```

44-4 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-3000-26TC:admin#config mac_based_access_control method local
Command: config mac_based_access_control method local

Success.

DGS-3000-26TC:admin#
```

44-5 config mac_based_access_control guest_vlan

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, please see the description for the “config mac_based_access_control ports” command.

Format

config mac_based_access_control guest_vlan ports <portlist>

Parameters

ports - Specifies MAC-based Access Control guest VLAN membership.

<portlist> - Enter the list of port used for this configuration here.

Restrictions

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

Example

To set the MAC-based Access Control guest VLAN membership:

```
DGS-3000-26TC:admin#config mac_based_access_control guest_vlan ports 1-8
Command: config mac_based_access_control guest_vlan ports 1-8

Success.

DGS-3000-26TC:admin#
```

44-6 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

ports - Specifies a range of ports for configuring the MAC-based Access Control function parameters.

<portlist> - Enter the list of port used for this configuration here.

all - Specifies all existed ports of switch for configuring the MAC-based Access Control function parameters.

state - (Optional) 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 - (Optional) 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 - (Optional) 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 - (Optional) If a host fails to pass the authentication, the next authentication will not start within the block time unless the user clears the entry state manually. If the block time is set to 0, it means do not block the client that failed authentication.

<sec 0-300> - Enter the block time value here. This value must be between 0 and 300 seconds.

max_users - (Optional) Specifies maximum number of users per port.

<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. The default value is 128.

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-3000-26TC: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-3000-26TC: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-3000-26TC: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-3000-26TC:admin#
```

44-7 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-3000-26TC:admin#create mac_based_access_control guest_vlan VLAN8
Command: create mac_based_access_control guest_vlan VLAN8

Success.

DGS-3000-26TC:admin#
```

44-8 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-3000-26TC:admin#delete mac_based_access_control guest_vlan default
Command: delete mac_based_access_control guest_vlan default

Success.

DGS-3000-26TC:admin#
```

44-9 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 to delete the MAC addresses of all MAC-based Access Control enabled ports.
<portlist> - Enter the list of port 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-3000-26TC:admin#clear mac_based_access_control auth_state ports all
Command: clear mac_based_access_control auth_state ports all

Success.

DGS-3000-26TC: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-3000-26TC: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-3000-26TC:admin#
```

44-10 create mac_based_access_control_local**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

mac - Specifies the MAC address that can pass local authentication.

<macaddr> - Enter the MAC address used here.

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, not specify the target VLAN 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-3000-26TC: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-3000-26TC:admin#
```

44-11 config mac_based_access_control_local

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

mac - Specifies the authenticated host's MAC address.

<macaddr> - Enter the MAC address used 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 - Not specify the target VLAN. When this host is authorized, will not assign 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 00-00-00-00-01:

```
DGS-3000-26TC: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-3000-26TC:admin#
```

44-12 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 - Deletes local database entry by specific MAC address.
<macaddr> - Enter the MAC address used here.

vlan - Deletes 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 - Deletes 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-3000-26TC: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-3000-26TC:admin#
```

To delete the MAC-based Access Control local database entry for the VLAN name VLAN3:

```
DGS-3000-26TC:admin#delete mac_based_access_control_local vlan VLAN3
Command: delete mac_based_access_control_local vlan VLAN3

Success.

DGS-3000-26TC:admin#
```

44-13 config mac_based_access_control authorization attributes

Description

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

When authorization is enabled for MAC-based Access Controls with RADIUS authentication, the authorized attributes (for example VLAN, 802.1p default priority, and ACL) assigned by the RADIUS server will be accepted if the global authorization status is enabled.

When authorization is enabled for MAC-based Access Controls with local authentication, the authorized attributes assigned by the local database will be accepted.

Format

config mac_based_access_control authorization attributes {radius [enable | disable] | local [enable | disable]}(1)

Parameters

radius - (Optional) If specified to enable, the authorized attributes (for example VLAN, 802.1p default priority, and ACL) assigned by the RADIUS server will be accepted if the global authorization status is enabled. The default state is enabled.

enable - Specifies that the radius attributes will be enabled.

disable - Specifies that the radius attributes will be disabled.

local - (Optional) If specified to enable, the authorized attributes assigned by the local database will be accepted if the global authorization status is enabled. The default state is enabled.

enable - Specifies that the local attributes will be enabled.

disable - Specifies that the local attributes will be disabled.

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-3000-26TC:admin#config mac_based_access_control authorization attributes
local disable
Command: config mac_based_access_control authorization attributes local disable

Success.

DGS-3000-26TC:admin#
```

44-14 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) Displays the MAC-based Access Control settings for a specific port or range of ports.
<portlist> - (Optional) Enter the list of port 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-3000-26TC:admin#show mac_based_access_control ports 1-4
Command: show mac_based_access_control ports 1-4
```

| Port | State | Aging Time (min) | Block Time (sec) | Auth Mode | Max User |
|------|----------|---------------------|---------------------|------------|----------|
| 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-3000-26TC:admin#
```

44-15 show mac_based_access_control_local

Description

This command is used to display the MAC-based Access Control local database entry(s).

Format

show mac_based_access_control_local {[mac <macaddr> | vlan <vlan_name 32> | vlanid <vlanid 1-4094>]}

Parameters

mac - (Optional) Displays MAC-based Access Control local database entries for a specific MAC

address.

<macaddr> - Enter the MAC address used here.

vlan - (Optional) Displays 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) Displays 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 the parameter is no specified, displays all MAC-based Access Control local database entries.

Restrictions

None.

Example

To show MAC-based Access Control local database for the VLAN called 'default':

```
DGS-3000-26TC:admin#show mac_based_access_control_local vlan default
Command: show mac_based_access_control_local vlan default

MAC Address          VID
-----
00-00-00-00-00-01   1
00-00-00-00-00-04   1

Total Entries:2

DGS-3000-26TC:admin#
```

44-16 show mac_based_access_control auth_state

Description

This command is used to display the MAC-based Access Control authentication status.

Format

show mac_based_access_control auth_state ports {<portlist>}

Parameters

ports - Displays authentication status by specific port.

<portlist> - (Optional) Enter the list of port used for this configuration here.

If not specified port(s), it will display all of MAC-based Access Control ports authentication status.

Restrictions

None.

Example

To display the MAC-based Access Control authentication status on port 1-4

```

DGS-3000-26TC: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-3000-26TC:admin#

```

44-17 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

max_users - Specifies to set the maximum number of authorized clients on the whole device.
<value 1-1000> - Enter the maximum users here. This value must be between 1 and 1000.
no_limit - Specifies to not limit the maximum number of users on the system. By default, there is no limit on the number of users.

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-3000-26TC:admin#config mac_based_access_control max_users 128
Command: config mac_based_access_control max_users 128

Success.

DGS-3000-26TC:admin#

```

44-18 config mac_based_access_control trap state

Description

This command is used to enable or disable sending of MAC-based Access Control traps.

Format

config mac_based_access_control trap state [enable | disable]

Parameters

enable - Enables trap for MAC-based Access Control. The trap of MAC-based Access Control will be sent out.
disable - Disables trap for MAC-based Access Control.

Restrictions

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

Example

To enable trap state of MAC-based Access Control:

```
DGS-3000-26TC:admin#config mac_based_access_control trap state enable
Command: config mac_based_access_control trap state enable

Success.

DGS-3000-26TC:admin#
```

44-19 config mac_based_access_control log state

Description

This command is used to enable or disable generating of MAC-based Access Control logs.

Format

config mac_based_access_control log state [enable | disable]

Parameters

enable - Enables log for MAC-based Access Control. The log of MAC-based Access Control will be generated.
disable - Disables 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-3000-26TC:admin#config mac_based_access_control log state disable
Command: config mac_based_access_control log state disable

Success.

DGS-3000-26TC:admin#
```

Chapter 45 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>]}

```

45-1 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

mac_address - Specifies the MAC address used.

<macaddr> - Enter the MAC address here.

vlan - 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-3000-26TC:admin#create mac_based_vlan mac_address 00-11-22-33-44-55 vlanid 100
100
Command: create mac_based_vlan mac_address 00-11-22-33-44-55 vlanid 100

Success.

DGS-3000-26TC:admin#

```


45-2 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) 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 static configured 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-3000-26TC: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-3000-26TC:admin#
```

45-3 show mac_based_vlan

Description

This command is used to display the static or dynamic MAC-Based VLAN entry. If the MAC address and VLAN is not specified, all static and dynamic entries will be displayed.

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.

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-3000-26TC: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-3000-26TC:admin#
```

Chapter 46 Mirror Command List

```
config mirror port <port> {[add | delete] source ports <portlist> [rx | tx | both]}
```

```
enable mirror
```

```
disable mirror
```

```
show mirror
```

46-1 config mirror

Description

This command is used to configure a mirror port – source port pair on the Switch. Traffic from any source port to a target port can be mirrored for real-time analysis. A logic analyzer or an RMON probe then can be attached to study the traffic crossing the source port in a completely unobtrusive manner. 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.

Format

```
config mirror port <port> {[add | delete] source ports <portlist> [rx | tx | both]}
```

Parameters

```
port - The port that will receive the packets duplicated at the mirror port.
```

```
  <port> - Enter the port number to be configured here.
```

```
add - (Optional) The mirror entry to be added.
```

```
delete - (Optional) The mirror entry to be deleted.
```

```
source ports - (Optional) The port that will be mirrored. All packets entering and leaving the source port can be duplicated in the mirror port.
```

```
  <portlist> - Enter the list of port to be configured here.
```

```
rx - (Optional) Allows the mirroring packets received (flowing into) the port or ports in the port list.
```

```
tx - (Optional) Allows the mirroring packets sent (flowing out of) the port or ports in the port list.
```

```
both - (Optional) Mirrors 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-3000-26TC:admin#config mirror port 3 add source ports 7-12 both
```

```
Command: config mirror port 3 add source ports 7-12 both
```

```
Success.
```

```
DGS-3000-26TC:admin#
```

46-2 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-3000-26TC:admin#enable mirror
Command: enable mirror

Success.

DGS-3000-26TC:admin#
```

46-3 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-3000-26TC:admin#disable mirror
Command: disable mirror

Success.

DGS-3000-26TC:admin#
```

46-4 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-3000-26TC:admin#show mirror
Command: show mirror

Current Settings
Mirror Status: Enabled
Target Port   : 3
Mirrored Port
              RX: 7-12
              TX: 7-12

DGS-3000-26TC:admin#
```

Chapter 47 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.

| |
|--|
| 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>]} |

47-1 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_leave function. enable - Specifies to enable MLD snooping fast_leave function. If enable, the membership is immediately removed when the system receive the MLD leave message. disable - Specifies to disable MLD snooping fast_leave function. |
| report_suppression - Specifies wheather to send the first MLD report from all hosts for a group to all the multicast routers. enable - When MLD report suppression is enabled, the Switch sends the first MLD report from all hosts for a group to all the multicast routers. The Switch does not send the remaining MLD reports for the group to the multicast routers. If the multicast router query includes requests only for MLDv1 reports, the Switch forwards only the first MLDv1 report from all hosts for a group to all the multicast routers. If the multicast router query also includes requests for MLDv2 reports, the Switch forwards all MLDv2 reports for a group to the multicast devices. This is the default. disable - Specifies not to send any MLD report from all hosts for a group to all the multicast routers. |
| proxy reporting - Specifies MLD proxy reporting. state - Specifies to enable or disable the proxy reporting. enable - Enables the proxy reporting. disable - Disables 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-3000-26TC:admin#config mld_snooping vlan_name default state enable
Command: config mld_snooping vlan_name default state enable

Success.

DGS-3000-26TC:admin#
```

47-2 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>}
```

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 | - Provides fine-tuning to allow for expected packet loss on a subnet. The value of the robustness variable is used in calculating the following MLD message intervals: |
| <value 1-7> | - Enter the robustness variable value here. This value must be between 1 and 7. |
| | <ul style="list-style-type: none"> • Group listener interval—Amount of time that must pass before a multicast router decides there are no more listeners of a group on a network. This interval is calculated as follows: (robustness variable * query interval) + (1 * query response interval). • Other querier present interval—Amount of time that must pass before a multicast router decides that there is no longer another multicast router that is the querier. This interval is calculated as follows: (robustness variable * query interval) + (0.5 * query response interval). • Last listener query count—Number of group-specific queries sent before the router assumes there are no local listeners of a group. The default number is the value of the robustness variable. • By default, the robustness variable is set to 2. You might want to increase this value if you expect a subnet to be loosely. |
| last_listener_query_interval | - (Optional) 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 | - (Optional) This allows the Switch to be specified as an MLD Querier (sends MLD query packets) or a Non-Querier (does not send MLD query packets). Set to enable or disable. |
| enable | - Enables the MLD querier state. |
| disable | - Disables the MLD querier state. |

version - (Optional) 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-3000-26TC: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-3000-26TC:admin#
```

47-3 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> - 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-3000-26TC:admin#config mld_snooping mrouter_ports vlan default add 1-10
Command: config mld_snooping mrouter_ports vlan default add 1-10

Success.

DGS-3000-26TC:admin#
```

47-4 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> - Specifies 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-3000-26TC:admin#config mld_snooping mrouter_ports_forbidden vlan default
add 11
Command: config mld_snooping mrouter_ports_forbidden vlan default add 11

Success.

DGS-3000-26TC:admin#
```

47-5 enable mld_snooping

Description

This command is used to enable MLD snooping on the Switch. MLD snooping is disabled by default. 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-3000-26TC:admin#enable mld_snooping
Command: enable mld_snooping

Success.

DGS-3000-26TC:admin#
```

47-6 disable mld_snooping

Description

This command is used to disable MLD snooping on the Switch. Disabling MLD snooping allows all MLD and IP multicast traffic to flood within a given IP interface. Note that disabling MLD snooping will also disable the forward multicast router only function.

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-3000-26TC:admin#disable mld_snooping
Command: disable mld_snooping

Success.

DGS-3000-26TC:admin#
```

47-7 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 VLAN is not specified, the system will display all current MLD snooping configurations.

Restrictions

None.

Example

To show MLD snooping:

```
DGS-3000-26TC:admin#show mld_snooping
Command: show mld_snooping

MLD Snooping Global State           : Disabled
Multicast router Only                : Disabled
Data Driven Learning Max Entries    : 256

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                           :
Querier Expiry Time                  : 100 secs
State                                : Disabled
```

```

Fast Leave                : Enabled
Rate Limit                : 100
Report Suppression       : Disabled
Porxy Reporting          : Disabled
Porxy Reporting Source IP : ::
Version                  : 3
Data Driven Learning State : Disabled
Data Driven Learning Aged Out : Disabled

VLAN Name                : vlan2
Query Interval           : 125
Max Response Time        : 10
Robustness Value         : 2
Last Member Query Interval : 1
Querier State            : Disabled
Querier Role              : Non-Querier
Querier IP                : ::
Querier Expiry Time      : 100 secs
State                    : Disabled
Fast Leave                : Enabled
Rate Limit                : No Limit
Report Suppression       : Enabled
Porxy Reporting          : Disabled
Porxy Reporting Source IP : ::
Version                  : 3
Data Driven Learning State : Disabled
Data Driven Learning Aged Out : Disabled

DGS-3000-26TC:admin#

```

47-8 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 port here.

<ipv6addr> - (Optional) Specifies the group IPv6 address for which you want to view MLD snooping group information.

data_driven - (Optional) Displays 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-3000-26TC:admin#show mld_snooping group
Command: show mld_snooping group
```

```
Source/Group      : 2001::1/FE1E::1
VLAN Name/VID     : default/1
Member Ports     : 1-2
UP Time          : 26
Expiry Time      : 258
Filter Mode      : INCLUDE
```

```
Source/Group      : 2002::2/FE1E::1
VLAN Name/VID     : default/1
Member Ports     : 3
UP Time          : 29
Expiry Time      : 247
Filter Mode      : EXCLUDE
```

```
Source/Group      : NULL/FE1E::2
VLAN Name/VID     : default/1
Member Ports     : 4-5
UP Time          : 40
Expiry Time      : 205
Filter Mode      : EXCLUDE
```

```
Source/Group      : NULL/FF1E::5
VLAN Name/VID     : default/1
Member Ports     :
Router Ports     : 24
UP Time          : 100
Expiry Time      : 200
Filter Mode      : EXCLUDE
```

```
Total Entries : 4
```

```
DGS-3000-26TC:admin#
```

```
DGS-3000-26TC:admin#show mld_snooping group data_driven
Command: show mld_snooping group data_driven
```

```
Source/Group      : NULL/FF1E::5
VLAN Name/VID     : default/1
Member Ports     :
Router Ports     : 24
UP Time          : 100
Expiry Time      : 200
Filter Mode      : EXCLUDE
```

```
Total Entries : 1
```

```
DGS-3000-26TC:admin#
```

47-9 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-3000-26TC: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-3000-26TC:admin#
```


47-10 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) 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 the mld_snooping mrouter ports:

```
DGS-3000-26TC: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-3000-26TC:admin#
```

47-11 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-3000-26TC:admin#create mld_snooping static_group vlan default FF1E::1
Command: create mld_snooping static_group vlan default FF1E::1

Success.

DGS-3000-26TC:admin#
```

47-12 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> - Specifies 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-3000-26TC:admin#delete mld_snooping static_group vlan default FF1E::1
Command: delete mld_snooping static_group vlan default FF1E::1

Success.

DGS-3000-26TC:admin#
```

47-13 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> - Specifies 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-3000-26TC: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-3000-26TC:admin#
```

47-14 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) Specifies the multicast group IPv6 address.

Restrictions

None.

Example

To display all the MLD snooping static groups:

```
DGS-3000-26TC:admin#show mld_snooping static_group
VLAN ID/Name          IP Address           Static Member Ports
-----
1 / Default           FF1E ::1            9-10

Total Entries : 1

DGS-3000-26TC:admin#
```

47-15 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 that if a data-driven group is created and MLD member ports are learned later, the entry will become an ordinary MLD snooping entry. That is, the aging out mechanism will follow the ordinary MLD snooping entry.

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. By default, the state is enabled. enable - Enter enable to enable the data driven learning state. disable - Enter disable to disable the data driven learning state. |
| aged_out - (Optional) Specifies to enable or disable the aging out of entries. By default, the state is disabled. enable - Specifies to enable the aged out option. disable - Specifies to disable the aged out 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-3000-26TC:admin#config mld_snooping data_driven_learning vlan default state
enable
Command: config mld_snooping data_driven_learning vlan default state enable

Success.

DGS-3000-26TC:admin#
```

47-16 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

max_learned_entry - Specifies the maximum number of groups that can be learned by data driven. The default setting is 128.

<value 1-1024> - Enter the maximum learned entry value here. This value must be between 1 and 1024.

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-3000-26TC:admin#config mld_snooping data_driven_learning max_learned_entry
50
Command: config mld_snooping data_driven_learning max_learned_entry 50

Success.

DGS-3000-26TC:admin#
```

47-17 clear mld_snooping data_driven_group

Description

This command is used to delete the MLD snooping groups learned by data driven.

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> - Specifies the group's IP address learned by data driven.

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-3000-26TC:admin#clear mld_snooping data_driven_group all
Command: clear mld_snooping data_driven_group all

Success.

DGS-3000-26TC:admin#
```

47-18 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 port here.

Restrictions

None.

Example

To show MLD snooping statistics counters:

```
DGS-3000-26TC:admin#show mld_snooping statistic counter vlanid 1
Command: show mld_snooping statistic counter vlanid 1

VLAN name          : default
-----
Group Number       : 0

Receive Statistics
  Query
    MLD v1 Query           : 0
    MLD v2 Query           : 0
    Total                   : 0
    Dropped By Rate Limitation : 0
    Dropped By Multicast VLAN : 0

  Report & Done
    MLD v1 Report          : 0
    MLD v2 Report          : 0
    MLD v1 Done            : 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
    MLD v1 Query           : 0
    MLD v2 Query           : 0
    Total                   : 0

  Report & Done
    MLD v1 Report          : 0
    MLD v2 Report          : 0
    MLD v1 Done            : 0
    Total                  : 0

Total Entries : 1

DGS-3000-26TC:admin#
```

47-19 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-3000-26TC:admin#clear mld_snooping statistics counter
Command: clear mld_snooping statistics counter

Success.

DGS-3000-26TC:admin#
```

47-20 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> - Configures 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 - Configures 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-3000-26TC:admin#config mld_snooping rate_limit ports 1 100
Command: config mld_snooping rate_limit ports 1 100

Success.

DGS-3000-26TC:admin#
```

47-21 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-3000-26TC: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-3000-26TC:admin#
```

47-22 show mld_snooping host

Description

This command is used to display the MLD hosts that have joined groups on specific ports or specific VLANs.

Format

show mld_snooping host {[vlan <vlan_name 32> | vlanid <vlanid_list> | ports <portlist> | group <ipv6addr>]}

Parameters

| |
|---|
| vlan - (Optional) Specifies the VLAN name. |
| <vlan_name 32> - Enter the VLAN name here. This name can be up to 32 characters long. |
| vlanid - (Optional) Specifies the VLAN ID. |
| <vlanid_list> - Enter the VLAN ID here. |
| ports - (Optional) Specifies that list of port that will be displayed. |
| <portlist> - Enter the list of ports here. |
| group - (Optional) Specifies the group. |
| <ipaddr> - Enter the group IPv6 address here. |

If no parameter is specified, all joining hosts will be displayed.

Restrictions

None.

Example

To display the host IP information:

```
DGS-3000-26TC:admin#show mld_snooping host vlan default
Command: show mld_snooping host vlan default

VLAN ID:    1
Group:      FF1E::1
Port:       2
Host: 2001::1

VLAN ID:    1
Group:      FF1E::2
Port:       3
Host: 2001::1

VLAN ID:    1
Group:      FF1E::3
Port:       4
Host: 2001::1

VLAN ID:    1
Group:      FF1E::1
Port:       5
```

```
Host: 2001::2

Total Entries : 4

DGS-3000-26TC:admin#
```

To display the host's IP information for the group "FF1E::1":

```
DGS-3000-26TC:admin# show mld_snooping host group FF1E::1
Command: show mld_snooping host group FF1E::1

VLAN ID:    1
Group:      FF1E::1
Port:       2
Host:       2001::1

VLAN ID:    1
Group:      FF1E::1
Port:       5
Host:       2001::2

Total Entries : 2

DGS-3000-26TC:admin#
```

Chapter 48 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]
```

48-1 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> - Specifies 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 - Disables the debug mechanism.
```

```
    brief - Sets the debug level to brief.
```

```
    detail - Sets 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-3000-26TC:admin#debug stp config ports all all state brief
Command: debug stp config ports all all state brief

Success.

DGS-3000-26TC:admin#
```

48-2 debug stp show information

Description

This command is used to display STP detailed information, such as the hardware tables, the STP state machine, etc.

Format

debug stp show information

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To show STP debug information:

```
DGS-3000-26TC: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
-----
Root Priority And Times:
Instance 0:
Designated Root Bridge : 36795/FD-7F-C3-FF-EF-12
External Root Cost     : -139756361
Regional Root Bridge   : 65447/3D-D5-7D-35-D8-FF
Internal Root Cost     : 1466613107
Designated Bridge      : 61882/9F-F3-FF-C7-EB-B5
CTRL+C  ESC  q  Quit  SPACE  n  Next Page  ENTER  Next Entry  a  All
```

48-3 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> - (Optional) Enter the list of port 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-3000-26TC: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
6                   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

DGS-3000-26TC:admin#
```

48-4 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 for display.
 - <portlist>** - Enter the list of port used for this configuration here.
 - all** - Display all port's counters.
-

If no parameter is specified, display the global counters.

Restrictions

Only Administrators can issue this command.

Example

To show the STP counters for port 9:

```
DGS-3000-26TC:admin#debug stp show counter ports 9
Command: debug stp show counter ports 9

STP Counters
-----
Port 9      :
Receive:
Total STP Packets      : 0
Configuration BPDU    : 0
TCN BPDU               : 0
RSTP TC-Flag          : 0
RST BPDU               : 0
Transmit:
Total STP Packets      : 0
Configuration BPDU    : 0
TCN BPDU               : 0
RSTP TC-Flag          : 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
```

48-5 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 port used for this configuration here.
 - all** - Clears all port counters.
-

Restrictions

Only Administrators can issue this command.

Example

To clear all STP counters on the Switch:

```
DGS-3000-26TC:admin#debug stp clear counter ports all
Command: debug stp clear counter ports all

Success.

DGS-3000-26TC:admin#
```

48-6 debug stp state

Description

This command is used to enable or disable the STP debug state.

Format

debug stp state [enable | disable]

Parameters

state - Specifies the STP debug state.
enable - Enables the STP debug state.
disable - Disables 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-3000-26TC:admin#debug stp state enable
Command: debug stp state enable

Success.

DGS-3000-26TC:admin#debug stp state disable
Command: debug stp state disable

Success.

DGS-3000-26TC:admin#
```

Chapter 49 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 I3_control_pkt <portlist> [{dvmrp pim igmp_query ospf rip vrrp} all] state [enable disable] |
| show cpu_filter I3_control_pkt ports <portlist> |
| config control_pkt [ipv4 [{igmp vrrp rip pim dvmrp ospf}(1) all] ipv6 [{mld pim ospf ripng nd}(1) all]] replace {priority [<value 0-7> none] dscp [<value 0-63> none]}(1) |
| show control_pkt {[ipv4 ipv6]} |

49-1 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) Adds an IPv4 multicast profile. |
| ipv6 - (Optional) Adds an IPv6 multicast profile. |
| profile_id - The ID of the profile. <value 1-24> - Enter the profile ID value here. This value must be between 1 and 24. |
| profile_name - Provides a meaningful 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-3000-26TC:admin#create mcast_filter_profile profile_id 2 profile_name MOD
Command: create mcast_filter_profile profile_id 2 profile_name MOD

Success.

DGS-3000-26TC:admin#
```

49-2 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 - ID of the profile.
<value 1-24> - Enter the profile ID value here. This value must be between 1 and 24.

profile_name - Provides 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 - (Optional) Provides 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 - (Optional) Specifies to add a multicast address.

delete - (Optional) Specifies to delete a multicast address.

<mcast_address_list> - (Optional) 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-3000-26TC: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-3000-26TC:admin#
```

49-3 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 - ID of the profile.

<value 1-24> - Enter the profile ID value here. This value must be between 1 and 24.

profile_name - Provides 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 - (Optional) Provides 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 - (Optional) Specifies to add an IPv6 multicast address.

delete - (Optional) Specifies to delete an IPv6 multicast address.

<mcastv6_address_list> - (Optional) Lists the IPv6 multicast addresses to put in 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-3000-26TC:admin#config mcast_filter_profile ipv6 profile_id 3 add
FFF0E::100:0:0:20- FFF0E::100:0:0:22
Command: config mcast_filter_profile ipv6 profile_id 3 add FFF0E::100:0:0:20-
FFF0E::100:0:0:22
```

```
Success.
```

```
DGS-3000-26TC:admin#
```

49-4 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 - 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-3000-26TC:admin#delete mcast_filter_profile profile_id 3
Command: delete mcast_filter_profile profile_id 3
Success.

DGS-3000-26TC:admin#
```

To delete the multicast address profile called MOD:

```
DGS-3000-26TC:admin#delete mcast_filter_profile profile_name MOD
Command: delete mcast_filter_profile profile_name MOD

Total entries: 2

DGS-3000-26TC:admin#
```

49-5 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 display an IPv4 multicast profile. |
| ipv6 - (Optional) Specifies to display 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-3000-26TC: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-3000-26TC:admin#
```

49-6 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 port 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) Adds a multicast address profile to a port.
-
- delete** - (Optional) Deletes a multicast address profile to a port.
-
- profile_id** - (Optional) 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 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-3000-26TC: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-3000-26TC:admin#
```

49-7 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 - (Optional) 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 group value will be set to infinite. Infinite means that the maximum number of multicast groups per port or VLAN is not limited by the Switch.

action - (Optional) Specifies the action for handling newly learned groups when the register is full.

drop - The new group will be dropped.

replace - 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-3000-26TC:admin#config max_mcast_group ports 1, 3 max_group 100
Command: config max_mcast_group ports 1, 3 max_group 100

Success.

DGS-3000-26TC:admin#
```

49-8 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-3000-26TC: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-3000-26TC:admin#
```

To display the maximum number of multicast groups that VLANs 1 and 2 can join:

```
DGS-3000-26TC: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-3000-26TC:admin#
```

49-9 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 port 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-3000-26TC: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-3000-26TC:admin#
```

To show the limited multicast settings configured on VLAN 1:

```
DGS-3000-26TC: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-3000-26TC:admin#
```

49-10 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. The default is disabled.
enable - Enables the filtering function.
disable - Disables the filtering function.

Restrictions

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

Example

To filter the DVMRP control packets on ports 1 to 2:

```
DGS-3000-26TC: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-3000-26TC:admin#
```

49-11 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-3000-26TC: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 | Disabl ed |
| 2 | Disabled | Enabled | Disabled | Disabled | Disabled | Disabl ed |

```
DGS-3000-26TC:admin#
```

49-12 config control_pkt

Description

This command is used to change the priority and/or Differentiated Services Code Point (DSCP) fields for specific control packets which are forwarded by software.

Format

config control_pkt [ipv4 [{igmp | vrrp | rip | pim | dvmrp | ospf}(1) | all] | ipv6 [{mld | pim | ospf | ripng | nd}(1) | all]] replace {priority [<value 0-7> | none] | dscp [<value 0-63> | none]}(1)

Parameters

ipv4 - Specifies IPv4 protocols.

igmp - Specifies that the Switch will examine the Internet Group Management Protocol (IGMP) field within each packet.

vrrp - Specifies that the Switch will examine the Virtual Router Redundancy Protocol (VRRP) field within each packet.

rip - Specifies that the Switch will examine the Routing Information Protocol (RIP) field within each packet.

pim - Specifies that the Switch will examine the Protocol-Independent Multicast (PIM) field within each packet.

dvmrp - Specifies that the Switch will examine the Distance Vector Multicast Routing Protocol (DVMRP) field within each packet.

ospf - Specifies that the Switch will examine the Open Shortest Path First (OSPF) field within each packet.

all - Specifies that the Switch will examine all above field within each packet.

ipv6 - Specifies the IPv6 protocols.

mld - Specifies that the Switch will examine the Multicast Listener Discovery (MLD) field within each packet.

pim - Specifies that the Switch will examine the Protocol-Independent Multicast (PIM) field within each packet.

ospf - Specifies that the Switch will examine the Open Shortest Path First (OSPF) field within each packet.

ripng - Specifies that the Switch will examine the IP Version 6 (IPv6) Routing Information Protocol - next generation (RIPng) field within each packet.

nd - Specifies that the Switch will examine the IP Version 6 (IPv6) Neighbor Discovery (ND) field within each packet.

all - Specifies that the Switch will examine all above field within each packet.

replace - Specifies to change the priority or DSCP.

priority - Specifies the priority value

<value 0-7> - Enter the value between 0 and 7.

none - Specifies not to change the priority.

dscp - Specifies the DSCP.

<value 0-63> - Enter the value between 0 and 63

none - Specifies not to change the DSCP.

Restrictions

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

Example

To change the priority of DVMRP packets to 3:

```
DGS-3000-26TC:admin#config control_pkt ipv4 dvmrp replace priority 3
Command: config control_pkt ipv4 dvmrp replace priority 3

Success.

DGS-3000-26TC:admin#
```

49-13 show control_pkt

Description

This command is used to display the priority and DSCP values configured for specific control packets.

Format

show control_pkt {[ipv4| ipv6]}

Parameters

ipv4 - Displays the IPv4 protocols.

ipv6 - Displays the IPv6 protocols.

If no parameter is specified the system will display all protocols.

Restrictions

None.

Example

To display the priority and DSCP values configured for all protocols:

```
DGS-3000-26TC:admin#show control_pkt
```

```
Command: show control_pkt
```

| Protocol | Priority | DSCP |
|-----------|----------|-------|
| ----- | ----- | ----- |
| igmp | None | None |
| vrrp | None | None |
| rip | None | None |
| pim | None | None |
| dvmrp | 3 | None |
| ospf | None | None |
| mld | None | None |
| ipv6 pim | None | None |
| ipv6 ospf | None | None |
| ripng | None | None |
| nd | None | None |

```
DGS-3000-26TC:admin#
```

Chapter 50 Multicast VLAN Command List

```

create igmp_snooping multicast_vlan <vlan_name 32> <vlanid 2-4094> {remap_priority [<value
0-7> | none] {replace_priority}}
config igmp_snooping multicast_vlan <vlan_name 32> {[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)
create igmp_snooping multicast_vlan_group_profile <profile_name 1-32>
config igmp_snooping multicast_vlan_group_profile <profile_name 1-32> [add | delete]
<mcast_address_list>
delete igmp_snooping multicast_vlan_group_profile [profile_name <profile_name 1-32> | all]
show igmp_snooping multicast_vlan_group_profile {< profile_name 1-32>}
config igmp_snooping multicast_vlan_group <vlan_name 32> [add | delete] profile_name
<profile_name 1-32>
show igmp_snooping multicast_vlan_group {<vlan_name 32>}
delete igmp_snooping multicast_vlan <vlan_name 32>
enable igmp_snooping multicast_vlan
disable igmp_snooping multicast_vlan
config igmp_snooping multicast_vlan forward_unmatched [enable | disable]
show igmp_snooping multicast_vlan {<vlan_name 32>}

```

50-1 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> - The VLAN ID of the multicast VLAN to be created. This value must be between 2 and 4094.

remap_priority - (Optional) 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-3000-26TC:admin#create igmp_snoop multicast_vlan mv1 2
Command: create igmp_snoop multicast_vlan mv1 2

Success.

DGS-3000-26TC:admin#
```

50-2 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 - 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 port to be configured here.

source_port - A port or range of ports to be added to the multicast VLAN.

<portlist> - Enter the list of port 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 port 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 port to be configured here.

state - Specifies that the multicast VLAN for a chosen VLAN should be enabled or disabled.

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 - Before forwarding the report packet sent by the host, the source IP address in the join packet must be replaced by this IP address. 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 - 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 "v1", make ports 1 and 3 members of the VLAN, and set the state to enable:

```
DGS-3000-26TC: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-3000-26TC:admin#
```

50-3 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-3000-26TC:admin#create igmp_snooping multicast_vlan_group_profile test
Command: create igmp_snooping multicast_vlan_group_profile test

Success.

DGS-3000-26TC:admin#
```

50-4 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

multicast_vlan_group_profile - Specifies the multicast VLAN profile name. The maximum length is 32 characters.

<profile_name 1-32> - Enter the multicast VLAN group name here. This name can be up to 32 characters long.

add - Adds a multicast address list to or from this multicast VLAN profile.

delete - Deletes a multicast address list to or from this multicast VLAN profile.

<mcast_address_list> - Enter the multicast VLAN IP address here. It can be a continuous single multicast address, such as 225.1.1.1, 225.1.1.3, 225.1.1.8, a multicast address range, such as 225.1.1.1-225.2.2.2, or both of types, such as 225.1.1.1, 225.1.1.18-225.1.1.20.

Restrictions

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

Example

To add the single multicast address 225.1.1.1 to the IGMP snooping multicast VLAN profile named "test":

```
DGS-3000-26TC:admin#config igmp_snooping multicast_vlan_group_profile test add
225.1.1.1
Command: config igmp_snooping multicast_vlan_group_profile test add 225.1.1.1

Success.

DGS-3000-26TC:admin#
```

50-5 delete igmp_snooping multicast_vlan_group_profile

Description

This command is used to delete an IGMP snooping multicast group profile on the Switch. Specifies a profile name to delete it. Specifies all to remove all profiles along with the groups that belong to that profile.

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-3000-26TC:admin#delete igmp_snooping multicast_vlan_group_profile
profile_name MOD
Command: delete igmp_snooping multicast_vlan_group_profile profile_name MOD

Success.

DGS-3000-26TC:admin#
```

50-6 show igmp_snooping multicast_vlan_group_profile

Description

This command is used to show the 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-3000-26TC: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-3000-26TC:admin#
```

50-7 config igmp_snooping multicast_vlan_group**Description**

This command is used to configure the multicast group learned with the specific multicast VLAN. The following cases can be considered for examples:

Case 0- If the IGMP Snooping is enabled on the VLAN of the join packet, the multicast VLAN won't process the packet.

Case 1- The multicast group is not configured, multicast VLANs do not have any member ports overlapping and the join packet received by the member port is learned on only the multicast VLAN that this port is a member of.

Case 2- The join packet is learned with the multicast VLAN that contains the destination multicast group. If the destination multicast group of the join packet cannot be classified into any multicast VLAN to which this port belongs, it will be forwarded or dropped according to forward unmatched mode.

Note that 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-3000-26TC: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-3000-26TC:admin#
```

50-8 show igmp_snooping multicast_vlan_group

Description

This command is used to show an IGMP snooping multicast VLAN group.

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-3000-26TC: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-3000-26TC:admin#
```

50-9 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

multicast_vlan - The name of the multicast VLAN to be deleted.
<vlan_name 32> -Enter the 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-3000-26TC:admin#delete igmp_snooping multicast_vlan v1
Command: delete igmp_snooping multicat_vlan v1

Success.

DGS-3000-26TC:admin#
```

50-10 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-3000-26TC:admin#enable igmp_snooping multicast_vlan
Command: enable igmp_snooping multicast_vlan

Success.

DGS-3000-26TC:admin#
```

50-11 disable igmp_snooping multicast_vlan

Description

This command is used to disable the IGMP multicast VLAN function. The command disable igmp_snooping is used to disable the ordinary IGMP snooping 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-3000-26TC:admin#disable igmp_snooping multicast_vlan
Command: disable igmp_snooping multicast_vlan

Success.

DGS-3000-26TC:admin#
```


50-12 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 all profiles, 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 - The packet will be flooded on the VLAN.

disable - 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-3000-26TC:admin#config igmp_snooping multicast_vlan forward_unmatched
enable
Command: config igmp_snooping multicast_vlan forward_unmatched enable

Success.

DGS-3000-26TC:admin#
```

50-13 show igmp_snooping multicast_vlan

Description

This command is used to display information for IGMP snooping multicast VLANs.

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-3000-26TC: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-3000-26TC:admin#
```

Chapter 51 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> fbpdudisable [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] fbpdudisable [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>} |

51-1 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-3000-26TC:admin#enable stp
Command: enable stp

Success.

DGS-3000-26TC:admin#
```

51-2 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-3000-26TC:admin#disable stp
Command: disable stp

Success.

DGS-3000-26TC:admin#
```

51-3 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) The time interval for sending configuration BPDUs by the Root Bridge. The default value is 2 seconds. This parameter is for STP and RSTP version. MSTP version uses per-port hellotime parameter. |
| <value 1-2> - Enter the hello time value here. This value must be between 1 and 2. |
| forwarddelay - (Optional) 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 in service provide site. It can use 802.1d GVRP address, 802.1ad service provider GVRP address or an 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 configure STP:

```
DGS-3000-26TC:admin#config stp maxage 25
Command: config stp maxage 25

Success.

DGS-3000-26TC:admin#
```

51-4 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-3000-26TC: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-3000-26TC:admin#
```

51-5 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

instance_id - Specifies the MSTP instance ID. Instance 0 represents for default instance, CIST.
<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-3000-26TC:admin#create stp instance_id 2
Command: create stp instance_id 2

Success.

DGS-3000-26TC:admin#
```

51-6 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

instance_id - Specifies the MSTP instance ID. Instance 0 represents for default instance, CIST.
<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-3000-26TC:admin#config stp instance_id 2 add_vlan 1-3
Command: config stp instance_id 2 add_vlan 1-3

Success.

DGS-3000-26TC:admin#
```

To remove a VLAN ID from an MSTP instance:

```
DGS-3000-26TC:admin#config stp instance_id 2 remove_vlan 2
Command: config stp instance_id 2 remove_vlan 2

Success.

DGS-3000-26TC:admin#
```

51-7 delete stp instance_id

Description

This command is used to delete an MST Instance.

Format

delete stp instance_id <value 1-7>

Parameters

instance_id - Specifies the MSTP instance ID. Instance 0 represents for default instance, CIST.

<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-3000-26TC:admin#delete stp instance_id 2
Command: delete stp instance_id 2

Success.

DGS-3000-26TC:admin#
```

51-8 config stp mst_config_id

Description

This command is used to change the name or the revision level of the MST configuration identification.

Format

config stp mst_config_id {revision_level <int 0-65535> | name <string>}

Parameters

name - (Optional) Specifies the name given for a specific MST region.

<string> - Enter the MST region name here.

revision_level - (Optional) 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.

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-3000-26TC: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-3000-26TC:admin#
```

51-9 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-3000-26TC: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-3000-26TC:admin#
```

51-10 config stp mst_ports

Description

This command is used to configure the ports management parameters.

Format

```
config stp mst_ports <portlist> instance_id <value 0-7> {internalCost [auto | <value 1-200000000>] | priority <value 0-240>}
```

Parameters

mst_ports - Specifies to be distinguished from the parameters of ports only at CIST level.

<portlist> - Enter a list of ports used for the configuration here.

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-3000-26TC:admin#config stp mst_ports 1 instance_id 0 internalCost auto
Command: config stp mst_ports 1 instance_id 0 internalCost auto

Success.

DGS-3000-26TC:admin#
```

51-11 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 a list of ports used for the configuration here.

external_cost - (Optional) 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.

| |
|---|
| <p>hellotime - (Optional) The default value is 2 . This parameter is for MSTP version. For STP and RSTP version, uses the per system hellotime parameter. <value 1-2> - Enter the hello time value here. This value must be between 1 and 2.</p> |
| <p>migrate - (Optional) Operation of management in order to specify the port to send MSTP BPDU 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.</p> |
| <p>edge - (Optional) To decide if this port is connected to a LAN or a Bridged LAN. true - Specifies that the specified port(s) is edge. false - Specifies that the specified port(s) is not edge. auto - In auto mode, the bridge will delay for a period to become edge port if no bridge BPDU is received. The default is auto mode.</p> |
| <p>p2p - (Optional) To decide if 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.</p> |
| <p>state - (Optional) To decide if 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.</p> |
| <p>restricted_role - (Optional) To decide if this port not to be selected as Root Port. The default value is false. true - Specifies that the port can be specified as the root port. false - Specifies that the port can not be specified as the root port.</p> |
| <p>restricted_tcn - (Optional) To decide if this port not to propagate topology change. The default value is false. true - Specifies that the port can be set to propagate a topology change. false - Specifies that the port can not be set to propagate a topology change.</p> |
| <p>fbpdu - (Optional) To decide if this port will flood STP BPDU when STP functionality is disabled. When the state is set to enable, the received BPDU will be forwarded. When the state is set to disable, the received BPDU 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 can not be set to flood the STP BPDU when the STP functionality is disabled.</p> |

Restrictions

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

Example

To configure STP ports:

```
DGS-3000-26TC:admin#config stp ports 1 externalCost auto
Command: config stp ports 1 externalCost auto

Success.

DGS-3000-26TC:admin#
```

51-12 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**

ports - Displays parameters of the designated port numbers, to be distinguished from showing parameters of the bridge.

<portlist> - (Optional) Enter a list of ports used for the configuration here.

Restrictions

None.

Example

To show STP ports:

```
DGS-3000-26TC: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

51-13 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

-
- priority** - Specifies the bridge priority value. This value must be divisible by 4096.
<value 0-61440> - Enter the bridge priority value here. 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-3000-26TC:admin#config stp priority 61440 instance_id 0
Command: config stp priority 61440 instance_id 0

Success.

DGS-3000-26TC:admin#
```

51-14 config stp version

Description

This command is used to configure the STP version.

Format

config stp version [mstp | rstp | stp]

Parameters

-
- version** - Specifies to decide to run under which version of STP.
mstp - Multiple Spanning Tree Protocol.
rstp - Rapid Spanning Tree Protocol. This is the default option.
stp - Spanning Tree Protocol.
-

Restrictions

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

Example

To configure STP version:

```
DGS-3000-26TC:admin#config stp version mstp
Command: config stp version mstp

Success.

DGS-3000-26TC:admin#
```

To config STP version with the same value of old configuration:

```
DGS-3000-26TC:admin#config stp version mstp
Command: config stp version mstp

Configure value is the same with current value.
Success.

DGS-3000-26TC:admin#
```

51-15 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

instance - Specifies the MSTP instance ID.

<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-3000-26TC: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-3000-26TC:admin#
```

Chapter 52 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

```

52-1 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-3000-26TC:admin#create nlb unicast_fdb 02-bf-01-01-01-01
Command: create nlb unicast_fdb 02-BF-01-01-01-01

Success.

DGS-3000-26TC:admin#

```


52-2 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> - Specifies 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> - Specifies 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-3000-26TC: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-3000-26TC:admin#
```

52-3 delete nlb unicast_fdb

Description

This command is used to delete the NLB unicast FDB entry.

Format

delete nlb unicast_fdb <macaddr>

Parameters

<macaddr> - Specifies 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-3000-26TC:admin#delete nlb unicast_fdb 02-bf-01-01-01-01
Command: delete nlb unicast_fdb 02-BF-01-01-01-01

Success.

DGS-3000-26TC:admin#
```

52-4 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> - Specifies 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-3000-26TC: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-3000-26TC:admin#
```

52-5 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> - Specifies 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> - Specifies 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-3000-26TC: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-3000-26TC:admin#
```

52-6 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> - Specifies 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> - Specifies 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-3000-26TC: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-3000-26TC:admin#
```

52-7 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-3000-26TC: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-3000-26TC:admin#
```

Chapter 53 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>}
```

53-1 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> - Specifies a range of ports to be displayed.

Restrictions

None.

Example

To display the packets analysis for port 7:

```

DGS-3000-26TC: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

```

53-2 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> - Specifies a range of ports to be displayed.

Restrictions

None.

Example

To display the errors of the port:

```

DGS-3000-26TC: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

53-3 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-3000-26TC: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 | | | | |
| 8 | 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 | | | | |

```
DGS-3000-26TC:admin#
```

To display the CPU utilization:


```
DGS-3000-26TC: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
```

53-4 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-3000-26TC:admin#show utilization dram
Command: show utilization dram

DRAM Utilization :
    Total DRAM      : 131072    KB
    Used DRAM       : 118556    KB
    Utilization     : 90 %

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

53-5 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-3000-26TC:admin#show utilization flash
Command: show utilization flash

Flash Memory Utilization :
    Total Flash      : 29618    KB
    Used Flash       : 5784     KB
    Utilization      : 19 %

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

53-6 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 be configured.

<portlist> - Enter a list of ports used for the configuration here.

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

Restrictions

Only Administrators and Operators can issue this command.

Example

To clear the Switch's statistics counters:

```
DGS-3000-26TC:admin#clear counters ports 7-9
```

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

```
Success.
```

```
DGS-3000-26TC:admin#
```

Chapter 54 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
148810-1000000000> | 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]
```

54-1 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. Note that 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. The 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> | - Specifies a range of ports to be configured. |
| all | - Specifies all ports 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> | - Specifies the range from 0 to 4294967295. |
| window | - The range is 1000 to 60000 ms. The default value is 1000ms. |
| <millisecond 1000-60000> | -The range is 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> | - Specifies a threshold range between 0 and 4294967295. |
| window | - The range is 1000 to 60000 ms. The default value is 1000ms. |
| <millisecond 1000-60000> | - The range is 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_seconds | - Specifies error frame time. |
| threshold | - Specifies a threshold range between 1 and 900. |
| <range 1-900> | -Specifies a threshold range between 1 and 900. |
| window | - The range is 1000 to 900000 ms. |
| <millisecond 10000-900000> | - The range is 1000 to 900000 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_period | - Specifies error frame period. |
| threshold | - Specifies a threshold range between 0 and 4294967295. |
| <range 0-4294967295> | -Specifies a threshold range between 0 and 4294967295. |
| window | - The range is 148810 to 100000000 ms. |
| <number 148810-100000000> | - The range is 148810 to 100000000 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. |

critical_link_event –Specifies critical link event.

dying_gasp - An unrecoverable local failure condition has occurred.

critical_event - 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 - If start is specified, it will request the peer to change to the remote loopback mode.

stop - If stop is specified, it will 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 default method is "ignore".

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure Ethernet OAM on ports 1 to 2 in active mode:

```
DGS-3000-26TC:admin#config ethernet_oam ports 1-2 mode active
Command: config ethernet_oam ports 1-2 mode active

Success.

DGS-3000-26TC:admin#
```

To enable Ethernet OAM on port 1:

```
DGS-3000-26TC:admin#config ethernet_oam ports 1 state enable
Command: config ethernet_oam ports 1 state enable

Success.

DGS-3000-26TC:admin#
```

To configure the error symbol threshold to 2 and period to 1000ms for port 1:

```
DGS-3000-26TC: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-3000-26TC:admin#
```

To configure the error frame threshold to 2 and period to 1000 ms for port 1:

```
DGS-3000-26TC: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-3000-26TC:admin#
```

To configure the error frame seconds threshold to 2 and period to 10000 ms for port 1:

```
DGS-3000-26TC: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-3000-26TC:admin#
```

To configure the error frame threshold to 10 and period to 1000000 ms for port 1:

```
DGS-3000-26TC: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-3000-26TC:admin#
```

To configure a dying gasp event for port 1:

```
DGS-3000-26TC: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-3000-26TC:admin#
```

To start remote loopback on port 1:

```
DGS-3000-26TC:admin#config ethernet_oam ports 1 remote_loopback start
Command: config ethernet_oam ports 1 remote_loopback start

Success.

DGS-3000-26TC:admin#
```

To configure the method of processing the received remote loopback command as “process” on port 1:

```
DGS-3000-26TC:admin#config ethernet_oam ports 1 received_remote_loopback
process
Command: config ethernet_oam ports 1 received_remote_loopback process

Success.

DGS-3000-26TC:admin#
```

54-2 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:
 1. 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).
 2. Loopback: It indicates that the OAM entity can initiate and respond to loopback commands.
 3. Link Monitoring: It indicates that the OAM entity can send and receive Event Notification OAMPDUs.

4. 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) Specifies the range of ports to display.

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) Specifies 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-3000-26TC: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 OAMPDU TX : 0
Organization Specific OAMPDU RX : 0
Unsupported OAMPDU TX          : 0
Unsupported OAMPDU RX          : 0
Frames Lost Due To OAM         : 0

DGS-3000-26TC:admin#

```

54-3 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> - Specifies 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-3000-26TC:admin#clear ethernet_oam ports 1 statistics
Command: clear ethernet_oam ports 1 statistics

Success.

DGS-3000-26TC:admin#
```

To clear port 1 OAM events:

```
DGS-3000-26TC:admin#clear ethernet_oam ports 1 event_log
Command: clear ethernet_oam ports 1 event_log

Success.

DGS-3000-26TC:admin#
```

Chapter 55 Peripherals Command List

show device_status
show environment
config temperature threshold {high <temperature -500-500> | low <temperature -500-500>}

config temperature [trap | log] state [enable | disable]

55-1 show device_status

Description

This command is used to display current status of power(s) and fan(s) on the system.

Within fan(s) status display, for example, there are three fans on the left of the Switch, if three fans is working normally, there will display "OK" in the Left Fan field. If some fans work failed, such as fan 1,3 , there will only display the failed fans in the Left Fan field, such as "1,3 Fail".

In the same way, the Right Fan, Back Fan is same to Left Fan. Because there is only one CPU Fan, if it is working failed, display "Fail", otherwise display "OK".

Format

show device_status

Parameters

None.

Restrictions

None.

Example

To show device status:

```
DGS-3000-26TC:admin#show device_status
Command: show device_status

    Internal Power: OK
    External Power: None
    Right Fan      : OK

DGS-3000-26TC:admin#
```

55-2 show environment

Description

This command is used to display the power and temperature status of the system.

Format

show environment

Parameters

None.

Restrictions

None.

Example

To display the device environment:

```
DGS-3000-26TC:admin#show environment
Command: show environment

Temperature Trap State      : Enabled
Temperature Log State      : Enabled
Internal Power             : Active
External Power             : None
Current Temperature(Celsius) : 32
High Warning Temperature Threshold(Celsius) : 79
Low Warning Temperature Threshold(Celsius) : 11

DGS-3000-26TC:admin#
```

55-3 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>}

Parameters

-
- high** - (Optional) Specifies to configure high threshold value. The high threshold must bigger than the low threshold.
<temperature -500-500> - Enter the high threshold temperature.
-
- low** - (Optional) Specifies to configure 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-3000-26TC:admin#config temperature threshold high 80
Command: config temperature threshold high 80

Success.

DGS-3000-26TC:admin#
```

55-4 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 state - Specifies the trap state for the warning temperature event.
enable - Enable trap state for warning temperature event. The default state is enabled.
disable - Disable trap state for warning temperature event.

log state - Specifies the log state for the warning temperature event.
enable - Enable log state for warning temperature event. The default state is enabled.
disable - Disable log state for warning temperature event.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the warning temperature trap state:

```
DGS-3000-26TC:admin#config temperature trap state enable
Command: config temperature trap state enable

Success.

DGS-3000-26TC:admin#
```

Chapter 56 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>}
```

56-1 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> - Specifies the IP address of the host.

<domain_name 255> - Specifies the domain name of the host.

times - (Optional) 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 the "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) Defines 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 ICMP echo message to “10.51.17.1” for 4 times:

```
DGS-3000-26TC: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-3000-26TC:admin#
```

56-2 ping6

Description

This command is used to send IPv6 Internet Control Message Protocol (ICMPv6) 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.

<domain_name 255> - Specifies the domain name of the host.

times - (Optional) The number of individual ICMPv6 echo messages to be sent. A value of 0 will send an infinite ICMPv6 echo messages. The maximum value is 255. The default is 0, indicating infinity. Press the "CTRL+C" to break the ping test.

<value 1-255> - Enter the number of individual ICMPv6 echo messages to be sent here. This value must be between 1 and 255.

size - (Optional) 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) Defines 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 ICMPv6 echo message to “3000::1” for 4 times:


```
DGS-3000-26TC: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-3000-26TC:admin#
```

Chapter 57 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> 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 |

57-1 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 - No limitation on the number of port security entries that can be learned by the system. By default, the number is set to no_limit.

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-3000-26TC:admin#config port_security system max_learning_addr 256
Command: config port_security system max_learning_addr 256

Success.

DGS-3000-26TC:admin#
```

57-2 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> | 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 port used for this configuration here.

all - Specifies that all ports will be configured.

admin_state - (Optional) 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 - (Optional) 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.

lock_address_mode - (Optional) Indicates the lock address mode. The default mode is deleteonreset.

permanent - 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 - This entry will be removed if the entry is idle for the specified aging time.

deleteonreset - 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.

vlan - (Optional) 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 - (Optional) Specifies the VLAN ID used here.

<vidlist> - Enter the VLAN ID used here.

max_learning_addr - (Optional) 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-3000-26TC: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-3000-26TC:admin#
```

57-3 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. The default value is "no_limit"

<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 - No limitation on the number of port security entries that can be learned by a specific VLAN.

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-3000-26TC:admin#config port_security vlan vlanid 1 max_learning_addr 64
Command: config port_security vlan vlanid 1 max_learning_addr 64

Success.

DGS-3000-26TC:admin#
```

57-4 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-3000-26TC: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-3000-26TC:admin#
```

57-5 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 the range of ports to be configured.
<portlist> - The port security entries learned on the specified port will be cleared.
all - All the port security entries learned by the system will be cleared.
-
- vlan** - (Optional) 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-3000-26TC:admin#clear port_security_entry ports 6
Command: clear port_security_entry ports 6

Success.

DGS-3000-26TC:admin#
```

57-6 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. While this parameter is null, to show the entries on all of the ports.
<portlist> - Enter the list of port 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.
-

Restrictions

None.

Example

To show all the port security entries:

```
DGS-3000-26TC: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-3000-26TC:admin#
```

57-7 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. While this parameter is null, to show the entries on all of the ports.

<portlist> - Enter the list of port 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.

Restrictions

None.

Example

To display the global configuration of port security:

```
DGS-3000-26TC: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-3000-26TC:admin#
```

57-8 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-3000-26TC:admin#enable port_security trap_log
Command: enable port_security trap_log

Success.

DGS-3000-26TC:admin#
```

57-9 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-3000-26TC:admin#disable port_security trap_log
Command: disable port_security trap_log

Success.

DGS-3000-26TC:admin#
```

Chapter 58 Power Saving Command List

| |
|---|
| config power_saving mode {length_detection 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] |
| show power_saving {length_detection link_detection led port hibernation} |
| show led state [enable disable] |
| show led |

58-1 config power_saving mode

Description

This command is used to set the power saving state.

For link detection and length detection function, they apply to the ports with copper media. If the power saving link detection state is enabled, the power is saved by following mechanisms:

- 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.
- When a link is detected on the port, for a shorter cable, the power consumption will be reduced by lowering the signal amplitude, since the signal attenuation is proportional to the cable length. The port will adjust the power based on the cable length and still maintain error free applications from both sides of the link. This mechanism is only available using the hardware support cable diagnostics function.

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 {length_detection | link_detection | led | port | hibernation} [enable | disable]

Parameters

length_detection - (Optional) Specifies the power saving link detection state.

link_detection - (Optional) Specifies the length detection used.

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-3000-26TC:admin#config power_saving mode port hibernation enable
Command: config power_saving mode port hibernation enable

Success.

DGS-3000-26TC:admin#
```

58-2 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-3000-26TC:admin#config power_saving hibernation add time_range range_1
Command: config power_saving hibernation add time_range range_1

Success.

DGS-3000-26TC:admin#
```

58-3 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-3000-26TC:admin#config power_saving led add time_range range_1
Command: config power_saving led add time_range range_1

Success.

DGS-3000-26TC:admin#
```

58-4 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> - Specifies 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-3000-26TC:admin#config power_saving port 1 add time_range range_1
Command: config power_saving port 1 add time_range range_1

Success.

DGS-3000-26TC:admin#
```

To delete a time range named "range_2" on port 1:

```
DGS-3000-26TC:admin#config power_saving port 1 delete time_range range_2
Command: config power_saving port 1 delete time_range range_2

Success.

DGS-3000-26TC:admin#
```

58-5 show power_saving

Description

This command is used to display the current state of power saving.

Format

show power_saving {length_detection | link_detection | led | port | hibernation}

Parameters

length_detection - (Optional) Displays the length detection configuration of power saving.

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-3000-26TC:admin#show power_saving
Command: show power_saving

Function Version: 3.00

Link Detection State: Enabled
Length Detection State: Disabled

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
-----
1         range_1

DGS-3000-26TC:admin#
```

58-6 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-3000-26TC:admin#config led state disable
Command: config led state disable

Success.

DGS-3000-26TC:admin#
```

58-7 show led

Description

This command is used to display the setting of all port's LED admin state.

Format

show led

Parameters

None.

Restrictions

None.

Example

To display the setting of all port's LED admin state:

```
DGS-3000-26TC:admin#show led
Command: show led

Port LED State: Disabled

DGS-3000-26TC:admin#
```


Chapter 59 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>}

```

59-1 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-3000-26TC:admin#config pppoe circuit_id_insertion state enable
Command: config pppoe circuit_id_insertion state enable

Success.

DGS-3000-26TC:admin#

```

59-2 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 - Enables port's PPPoE circuit ID insertion function.

disable - Disables port's PPPoE circuit ID insertion function.

circuit_id - Specifies to configure the device ID part for encoding of the circuit ID option.

mac - The MAC address of the Switch will be used to encode the circuit ID option.

ip - The Switch's IP address will be used to encode the circuit ID option. This is the default.

udf - A user specified 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-3000-26TC:admin#config pppoe circuit_id_insertion ports 5 state enable
Command: config pppoe circuit_id_insertion ports 5 state enable
```

```
Success.
```

```
DGS-3000-26TC:admin#
```

59-3 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-3000-26TC:admin#show pppoe circuit_id_insertion
Command: show pppoe circuit_id_insertion

Global PPPoE State: Enabled

DGS-3000-26TC:admin#
```

59-4 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-3000-26TC: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-3000-26TC:admin#
```

Chapter 60 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>]} |
| show 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>} |

60-1 create dot1v_protocol_group

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

| |
|---|
| group_id - The ID of protocol group which is used to identify a set of protocols <id> - Enter the group ID used here. |
| group_name - (Optional) 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-3000-26TC: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-3000-26TC:admin#
```

60-2 config dot1v_protocol_group add protocol

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 - The ID of the protocol group which is used to identify a set of protocols. <id> - Enter the group ID used here. |
| group_name - 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 - 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-3000-26TC: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-3000-26TC:admin#
```

60-3 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-3000-26TC:admin#delete dot1v_protocol_group group_id 100
Command: delete dot1v_protocol_group group_id 100

Success.

DGS-3000-26TC:admin#
```

60-4 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 group ID is specified, all the configured protocol groups will be displayed.
-

Restrictions

None.

Example

To display the protocol group ID 10:

```
DGS-3000-26TC: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-3000-26TC:admin#
```

60-5 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 option.

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

The example is to assign VLAN marketing-1 for untagged ipv6 packet ingress from port 3.

To configure the group ID 10 on port 3 to be associated with VLAN marketing-1:

```
DGS-3000-26TC: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-3000-26TC:admin#
```

60-6 show port dot1v

Description

This command is used to display the VLAN to be associated with untagged packet ingressed from 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 port is specified, information for all ports will be displayed.

Restrictions

None.

Example

The example display the protocol VLAN information for ports 1:

```
DGS-3000-26TC: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 | - |

```
Total Entries: 4
```

```
DGS-3000-26TC:admin#
```

Chapter 61 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]} |
| 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] {cvd <vidlist>} |
| show vlan_translation {[ports <portlist> cvd <vidlist>]} |

61-1 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-3000-26TC:admin#enable qinq
Command: enable qinq

Success.

DGS-3000-26TC:admin#
```

61-2 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-3000-26TC:admin#disable qinq
Command: disable qinq

Success.

DGS-3000-26TC:admin#
```

61-3 config qinq inner_tpid

Description

The 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

inner_tpid - Specifies the inner-TPID of the system.
<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-3000-26TC:admin#config qinq inner_tpid 0x9100
Command: config qinq inner_tpid 0x9100

Success.

DGS-3000-26TC:admin#
```

61-4 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**]}

Parameters

| | |
|-------------------------------|---|
| <portlist> | - Enter the list of ports to be configured here. |
| all | - Specifies that all the ports will be used for the configuration. |
| role | - (Optional) 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 | - (Optional) 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 | - (Optional) Specifies the outer-TPID of a port. |
| <hex 0x1-0xffff> | - Enter the outer-TPID value used here. |
| add_inner_tag | - (Optional) 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-3000-26TC:admin#config qinq ports 1-4 role nni outer_tpid 0x88A8
Command: config qinq ports 1-4 role nni outer_tpid 0x88A8

Success.

DGS-3000-26TC:admin#
```

61-5 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-3000-26TC:admin#show qinq
Command: show qinq

Qinq Status : Enabled

DGS-3000-26TC:admin#
```

61-6 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-3000-26TC:admin#show qinq inner_tpid
Command: show qinq inner_tpid

Inner TPID: 0x9100

DGS-3000-26TC:admin#
```

61-7 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-3000-26TC: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-3000-26TC:admin#
```

61-8 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-3000-26TC:admin#create vlan_translation ports 1 replace cvid 20 svid 200
Command: create vlan_translation ports 1 replace cvid 20 svid 200

Success.

DGS-3000-26TC: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-3000-26TC:admin#create vlan_translation ports 1 add cvid 30 svid 300
Command: create vlan_translation ports 1 add cvid 30 svid 300

Success.

DGS-3000-26TC:admin#
```

61-9 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-3000-26TC:admin#delete vlan_translation ports 1-4
Command: delete vlan_translation ports 1-4

Success.

DGS-3000-26TC:admin#
```

61-10 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-3000-26TC: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-3000-26TC:admin#
```

Chapter 62 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>]} |
| 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 wdr] |
| 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>} |
| 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>} |

62-1 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> - Specifies 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 - Indicates there is no limit on receiving bandwidth of the configured ports. An integer value from m to n sets a maximum limit in Kbits/sec. The actual bandwidth will be an adjusted value based on the user specified bandwidth. The actual limit may be equal to the user specified limit, but will not exceed it. The actual limit recognized by the device, will be displayed when the command is executed. |
| <value 64-10240000> - Enter the receiving data rate here. This value must be between 64 and 10240000. |
| tx_rate - (Optional) Specifies the limitation applied to transmit data rate. |
| no_limit - Indicates there is no limit on port tx bandwidth. An integer value from m to n sets a maximum limit in Kbits/sec. The actual bandwidth will be an adjusted value based on the user specified bandwidth. The actual limit may be equal to the user specified limit, but will not exceed it. The actual limit recognized by the device, will be displayed when the |

command is executed.
<value 64-10240000> - Enter the transmitting data rate here. This value must be between 64 and 10240000.

Restrictions

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

Example

To configure the port bandwidth:

```
DGS-3000-26TC:admin#config bandwidth_control 1-10 tx_rate 100
Command: config bandwidth_control 1-10 tx_rate 100

Success

DGS-3000-26TC:admin#
```

62-2 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 that 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 specified, system will display all ports bandwidth configurations.

Restrictions

None.

Example

To display port bandwidth control table:

```
DGS-3000-26TC:admin#show bandwidth_control 1-10
Command: show bandwidth_control 1-10
```

Bandwidth Control Table

| Port | RX Rate (Kbit/sec) | TX Rate (Kbit/sec) | Effective RX (Kbit/sec) | Effective TX (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-3000-26TC:admin#
```

62-3 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>]}
```

Parameters

ports - (Optional) Specifies a range of ports to be configured.

<portlist> - Enter the list of port used for this configuration here.

all - For set all ports in the system, you may use "all" parameter. If no parameter is specified, system will set all ports.

<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 that one of the parameters below (no_limit or <value m-n>) will be applied to the mini-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 multiple of minimum granularity, the rate will be adjusted.

max_rate - (Optional) Specifies that one of the parameters below (no_limit or <value m-n >) will be applied to 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 multiple of 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-3000-26TC: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

Success.

DGS-3000-26TC:admin#
```

62-4 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-3000-26TC: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-3000-26TC:admin#
```

62-5 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 - Specifies a range of ports to be configured.

<portlist> - Enter the list of port used for this configuration here.

<class_id 0-7> - Specifies the 8 hardware priority queues which the config scheduling command will apply to. The four hardware priority queues are identified by number from 0 to 7 with the 0 queue being the lowest priority.

strict - The queue will operate in strict mode.

weight - Specifies the weights for weighted round robin. A value between 0 and n can be specified.

<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-3000-26TC:admin#config scheduling ports 10 1 weight 25
Command: config scheduling ports 10 1 weight 25

Success.

DGS-3000-26TC:admin#
```

62-6 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 | wdr]

Parameters

ports - (Optional) Specifies a range of ports to be configured.
 <portlist> - Enter the list of port used for this configuration here.
 all - Specifies to set all ports in the system. If no port is specified, system will set all ports.

strict - 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 - Use the weighted round-robin algorithm to handle packets in an even distribution in priority classes of service.

wdr - 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-3000-26TC:admin#config scheduling_mechanism strict
Command: config scheduling_mechanism strict

Success.

DGS-3000-26TC:admin#
```

To configure the traffic scheduling mechanism for CoS queue on port 1:

```
DGS-3000-26TC:admin#config scheduling_mechanism ports 1 strict
Command: config scheduling_mechanism ports 1 strict

Success.

DGS-3000-26TC:admin#
```


62-7 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 specified, system will display all ports scheduling configurations.

Restrictions

None.

Example

To display the traffic scheduling parameters for each CoS queue on port 1 (take eight hardware priority queues for example):

```
DGS-3000-26TC: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-3000-26TC:admin#
```

62-8 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 specified, system will display all ports scheduling mechanism configurations.

Restrictions

None.

Example

To show scheduling mechanism:

```
DGS-3000-26TC: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 |

```
DGS-3000-26TC:admin#
```

62-9 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> - The 802.1p user priority you want to associate with the <class_id> (the number of the hardware queue) with.

<class_id 0-7> - 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-3000-26TC:admin#config 802.1p user_priority 1 3
Command: config 802.1p user_priority 1 3

Success.

DGS-3000-26TC:admin#
```

62-10 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-3000-26TC: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-3000-26TC:admin#

```

62-11 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> - This specifies 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> - 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-3000-26TC:admin#config 802.1p default_priority all 5
Command: config 802.1p default_priority all 5

Success.

DGS-3000-26TC:admin#
```

62-12 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 that 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-3000-26TC: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-3000-26TC:admin#
```

62-13 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.

Format

```
config dscp trust [<portlist> | all] state [enable | disable]
```

Parameters

<portlist> - Enter the list of port used for this configuration.

all - Specifies that the command apply to all ports on the Switch.

state - Specifies to enable or disable to trust DSCP. By default, DSCP trust is disabled.

enable - Specifies to enable the DSCP trust state.

disable - Specifies to disable the DSCP trust state.

Restrictions

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

Example

Enable DSCP trust on ports 1-8.

```
DGS-3000-26TC:admin#config dscp trust 1-8 state enable
Command: config dscp trust 1-8 state enable
```

```
Success.
```

```
DGS-3000-26TC:admin#
```

62-14 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 port used for this configuration. |
| all | - (Optional) Specifies that the command apply to all ports on the Switch. |
| 1p_color | - The list of source priority for incoming packets. |
| <priority_list> | - Specifies the list of source priority for incoming packets. |
| to | - 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-3000-26TC: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-3000-26TC:admin#
```

62-15 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

None.

Example

To show the 802.1p color mapping on port 1:

```
DGS-3000-26TC:admin#show 802.1p map lp_color 1
Command: show 802.1p map lp_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-3000-26TC:admin#
```

62-16 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) A range of ports to display.
 If not specify the port, all ports for DSCP trust status on the Switch will be displayed.

Restrictions

None.

Example

Display DSCP trust status on ports 1-8.


```

DGS-3000-26TC: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-3000-26TC:admin#

```

62-17 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 port used for this configuration here.

all - Specifies that all the ports will be included in this configuration.

dscp_priority - Specifies a list of DSCP value 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> - Specifies the result priority of mapping.

dscp_dscp - Specifies a list of DSCP value 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> - Specifies the result DSCP of mapping.

dscp_color - Specifies a list of DSCP value 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-3000-26TC:admin#config dscp map 1-8 dscp_priority 1 to 1
Command: config dscp map 1-8 dscp_priority 1 to 1

Success.

DGS-3000-26TC:admin#
```

To configure the global mapping of the DSCP priority to priority 1:

```
DGS-3000-26TC:admin#config dscp map dscp_priority 1 to 1
Command: config dscp map dscp_priority 1 to 1

Success.

DGS-3000-26TC:admin#
```

62-18 show dscp map

Description

This command is used to show DSCP trusted port list and mapped color, priority and DSCP.

Format

show dscp map {<portlist>} [**dscp_priority** | **dscp_dscp** | **dscp_color**] {**dscp** <dscp_list>}

Parameters

<portlist> - (Optional) A range of ports to show. If no port is specified, all ports' DSCP mapping will be displayed.

dscp_priority - Specifies a list of DSCP value to be mapped to a specific priority.

dscp_dscp - Specifies a list of DSCP value to be mapped to a specific DSCP.

dscp_color - Specifies a list of DSCP value to be mapped to a specific color.

dscp - (Optional) This specifies DSCP value that will be mapped.

<dscp_list> - Enter the DSCP list here.

Restrictions

None.

Example

In case of project support per port configure, show DSCP map configuration on port 1.

```
DGS-3000-26TC: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-3000-26TC:admin#
```

Chapter 63 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_client
```

```
show acct_client
```

63-1 config radius add

Description

This command is used to add a new RADIUS server. The server with lower index has higher authenticative 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 - The key pre-negotiated between switch and the RADIUS server. It is used to encrypt user's
authentication data before being transmitted over internet. The maximum length of the key is
32.
```

```
<password 32> - Enter the password here. The password can be up to 32 characters long.
```

```
default - Sets 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. The range is 1 to 65535.
```

```
<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. The range is 1 to 65535.
```

```
<udp_port_number 1-65535> - Enter the accounting port number here. This value must be
between 1 and 65535.
```

```
timeout - The waiting time in second for the server to 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 - 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-3000-26TC: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-3000-26TC:admin#
```

63-2 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> - Specifies to delete a RADIUS server. Enter the RADIUS server index.

Restrictions

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

Example

To delete a radius server:

```
DGS-3000-26TC:admin#config radius delete 1
Command: config radius delete 1

Success.

DGS-3000-26TC:admin#
```

63-3 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_number1-65535> |
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 - The IP address of the RADIUS server. |
| <server_ip> - Enter the RADIUS server IP address here. |
| <ipv6addr> - Enter the RADIUS server IPv6 address used here. |
| key - The key pre-negotiated between switch and RADIUS server. It is used to encrypt user's authentication data before being transmitted over internet. The maximum length of the key is 32. |
| <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 range is 1 to 65535. 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 range is 1 to 65535. 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 - 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 - 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-3000-26TC:admin#config radius 1 auth_port 60
Command: config radius 1 auth_port 60

Success.

DGS-3000-26TC:admin#
```

63-4 show radius

Description

This command is used to display RADIUS server configurations.

Format**show radius****Parameters**

None.

Restrictions

None.

Example

To display RADIUS server configurations:

```
DGS-3000-26TC:admin#show radius
Command: show radius

Index  IP Address          Auth-Port  Acct-Port  Timeout  Retransmit  Key
-----  -----
1      10.48.74.121       60         1813      5        2          dlink

Total Entries : 1

DGS-3000-26TC:admin#
```

63-5 show auth_client**Description**

This command is used to display information of RADIUS authentication client.

Format**show auth_client****Parameters**

None.

Restrictions

None.

Example

To display authentication client information:

```
DGS-3000-26TC: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-3000-26TC:admin#
```

63-6 show acct_client

Description

This command is used to display information of RADIUS accounting client.

Format

show acct_client

Parameters

None.

Restrictions

None.

Example

To display information of RADIUS accounting client:


```
DGS-3000-26TC: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-3000-26TC:admin#
```

Chapter 64 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
```

64-1 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 disabled.

 - utilization** - (Optional) Specifies to configure 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 to enable or disable the trap and log mechanism.
 - enable** - Specifies that the trap and log mechanism will be enabled.
 - disable** - Specifies that the trap and log mechanism will be disabled.

 - mode** - (Optional) Determines the control method of broadcasting traffic.
 - strict** - In 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 the ARP packet is the Switch itself) to the Switch. That means that no matter what the reasons for high CPU utilization are (may not be caused by an ARP storm), the Switch reluctantly processes the specified traffic, mentioned previously in the Exhausted mode.
 - fuzzy** - In fuzzy mode, the Switch will adjust the bandwidth dynamically.
-

Restrictions

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

Example

To configure CPU protection:

```
DGS-3000-26TC: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-3000-26TC:admin#
```

64-2 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-3000-26TC: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-3000-26TC:admin#
```

Note: Safeguard engine current status has two modes: exhausted and normal mode.

Chapter 65 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 |

65-1 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 - The 3DES cipher is 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) - Advanced Encryption Standard. |
| arcfour - RC4 (also known as ARC4 or ARCFOUR meaning Alleged RC4) is the most widely-used software stream cipher. |
| blowfish - Blowfish is a keyed, symmetric block cipher. |
| cast128 - 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) - Twofish has a 128-bit block size, a key size ranging from 128 to 256 bits. |
| MD5 - Message-Digest Algorithm 5. |
| SHA1 - Secure Hash Algorithm. |
| RSA - RSA encryption algorithm is a non-symmetric encryption algorithm. |
| DSA - Digital Signature Algorithm. |
| enable - Enables the algorithm. |
| disable - Disables the algorithm. |

Restrictions

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

Example

To enable SSH server public key algorithm:

```
DGS-3000-26TC:admin#config ssh algorithm DSA enable
Command: config ssh algorithm DSA enable

Success.

DGS-3000-26TC:admin#
```

65-2 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-3000-26TC: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-3000-26TC:admin#
```

65-3 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 using password.

publickey - Specifies the user authentication method using public key.

hostbased - Specifies the user authentication method using host-based.

enable - Enables the user authentication method.

disable - Disables the user authentication method.

Restrictions

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

Example

To configure user authentication method:

```
DGS-3000-26TC:admin#config ssh authmode publickey enable
Command: config ssh authmode publickey enable

Success.

DGS-3000-26TC:admin#
```

65-4 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-3000-26TC:admin#show ssh authmode
Command: show ssh authmode

The SSH Authentication Method:
Password      : Enabled
Public Key    : Enabled
Host-based    : Enabled

DGS-3000-26TC:admin#
```

65-5 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> | <ipv6addr>]] | password | publickey]

Parameters

<username 15> - Enter the user name. This name can be up to 15 characters long.

authmode - Specifies the authentication method.

hostbased - Specifies user authentication method.

hostname - Specifies host domain name.

<domain_name 32> - Enter the domain name here. This name can be up to 32 characters long.

hostname_IP - Specifies host domain name and IP address.

<domain_name 32> - Specifies host name if configuring Host-based method.

<ipaddr> - Specifies host IP address if configuring Host-based method.

<ipv6addr> - Specifies host IPv6 address if configuring Host-based method.

password - Specifies user authentication method.

publickey - Specifies user authentication method.

Restrictions

Only Administrators can issue this command.

Example

To update user "test" authentication method:

```
DGS-3000-26TC:admin#config ssh user test authmode publickey
Command: config ssh user test authmode publickey

Success.

DGS-3000-26TC:admin#
```

65-6 show ssh user authmode

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-3000-26TC:admin#show ssh user authmode
Command: show ssh user authmode

Current Accounts:
User Name          Authentication Host Name          Host IP
-----
User1              Password
User2              Public Key
User3              Host-based      domain.com          10.70.89.111
User4              Password

Total Entries : 4

DGS-3000-26TC:admin#

```

65-7 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 session at the same time, maximum 8 sessions.
<int 1-8> - Enter the maximum session 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 user maximum fail attempts.
<int 2-20> - Enter the user 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, which the never means do NOT re-generate session key
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-3000-26TC:admin#config ssh server maxsession 3
Command: config ssh server maxsession 3

Success.

DGS-3000-26TC:admin#
```

65-8 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-3000-26TC:admin#enable ssh
Command: enable ssh

Success.

DGS-3000-26TC:admin#
```

65-9 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-3000-26TC:admin#disable ssh
Command: disable ssh

Success.

DGS-3000-26TC:admin#
```

65-10 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-3000-26TC: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-3000-26TC:admin#
```

Chapter 66 Secure Sockets Layer (SSL) Command List

```

download ssl certificate {<ipaddr> certfilename <path_filename 64> keyfilename <path_filename 64>}
enable ssl {ciphersuite {RSA_with_RC4_128_MD5 | RSA_with_3DES_EDE_CBC_SHA | DHE_DSS_with_3DES_EDE_CBC_SHA | RSA_EXPORT_with_RC4_40_MD5}}
disable ssl {ciphersuite {RSA_with_RC4_128_MD5 | RSA_with_3DES_EDE_CBC_SHA | DHE_DSS_with_3DES_EDE_CBC_SHA | RSA_EXPORT_with_RC4_40_MD5}}
show ssl {certificate}
show ssl cachetimeout
config ssl cachetimeout <value 60-86400>

```

66-1 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> - Enter the certificate file path with respect to the TFTP server root path.
    This can be up to 64 characters long.
keyfilename - (Optional) Specifies the private key file name which accompany with the certificate.
  <path_filename 64> - Enter the private key file path with respect to the TFTP server root path.
    This can be up to 64 characters long.

```

Restrictions

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

Example

To download certificate from TFTP server:

```
DGS-3000-26TC: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

Certificate Loaded Successfully!

DGS-3000-26TC:admin#
```

66-2 enable ssl

Description

This command is used to enable SSL status and its ciphersuites. Using “enable ssl” command will enable SSL feature which means enable SSLv3 and TLSv1. For each ciphersuites, user must specify it by this command.

Format

```
enable ssl {ciphersuite {RSA_with_RC4_128_MD5 | RSA_with_3DES_EDE_CBC_SHA |
DHE_DSS_with_3DES_EDE_CBC_SHA | RSA_EXPORT_with_RC4_40_MD5}}
```

Parameters

ciphersuite - (Optional) Specifies the cipher suite combination used for this configuration.

- RSA_with_RC4_128_MD5** - Indicates RSA key exchange with RC4 128 bits encryption and MD5 hash.
- RSA_with_3DES_EDE_CBC_SHA** - Indicates RSA key exchange with 3DES_EDE_CBC encryption and SHA hash.
- DHE_DSS_with_3DES_EDE_CBC_SHA** - Indicates DH key exchange with 3DES_EDE_CBC encryption and SHA hash.
- RSA_EXPORT_with_RC4_40_MD5** - Indicates RSA_EXPORT key exchange with RC4 40 bits encryption and MD5 hash.

Restrictions

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

Example

To enable the SSL ciphersuite for RSA_with_RC4_128_MD5:

```
DGS-3000-26TC:admin#enable ssl ciphersuite RSA_with_RC4_128_MD5
Command: enable ssl ciphersuite RSA_with_RC4_128_MD5

Success.

DGS-3000-26TC:admin#
```

To enable SSL:

```
DGS-3000-26TC:admin#enable ssl
Command: enable ssl

Success.

DGS-3000-26TC:admin#
```

Note: Web will be disabled when SSL is enabled.

66-3 disable ssl

Description

This command is used to disable SSL feature and supported ciphersuites. Using “disable ssl” command will disable SSL feature and for each ciphersuites status user must specified it by this command.

Format

disable ssl {ciphersuite {RSA_with_RC4_128_MD5 | RSA_with_3DES_EDE_CBC_SHA | DHE_DSS_with_3DES_EDE_CBC_SHA | RSA_EXPORT_with_RC4_40_MD5}}

Parameters

ciphersuite - (Optional) Specifies the cipher suite combination used for this configuration.

- RSA_with_RC4_128_MD5** - Indicates RSA key exchange with RC4 128 bits encryption and MD5 hash.
- RSA_with_3DES_EDE_CBC_SHA** - Indicates RSA key exchange with 3DES_EDE_CBC encryption and SHA hash.
- DHE_DSS_with_3DES_EDE_CBC_SHA** - Indicates DH key exchange with 3DES_EDE_CBC encryption and SHA hash.
- RSA_EXPORT_with_RC4_40_MD5** - Indicates RSA_EXPORT key exchange with RC4 40 bits encryption and MD5 hash.

Restrictions

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

Example

To disable SSL ciphersuite for RSA_with_RC4_128_MD5:

```
DGS-3000-26TC:admin#disable ssl ciphersuite RSA_with_RC4_128_MD5
Command: disable ssl ciphersuite RSA_with_RC4_128_MD5

Success.

DGS-3000-26TC:admin#
```

To disable SSL:

```
DGS-3000-26TC:admin#disable ssl
Command: disable ssl

Success.

DGS-3000-26TC:admin#
```

66-4 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-3000-26TC:admin#show ssl
Commands: show ssl

SSL Status                               Enabled

RSA_WITH_RC4_128_MD5                     0x0004 Enabled
RSA_WITH_3DES_EDE_CBC_SHA                 0x000A Enabled
DHE_DSS_WITH_3DES_EDE_CBC_SHA             0x0013 Enabled
RSA_EXPORT_WITH_RC4_40_MD5                0x0003 Enabled

DGS-3000-26TC:admin#
```

To show certificate:

```
DGS-3000-26TC:admin#show ssl certificate
Command: show ssl certificate

Loaded with RSA Certificate!

DGS-3000-26TC:admin#
```


66-5 show ssl cachetimeout

Description

This command is used to show cahce 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-3000-26TC:admin#show ssl cachetimeout
Commands: show ssl cachetimeout

Cache timeout is 600 second(s)

DGS-3000-26TC:admin#
```

66-6 config ssl cachetimeout

Description

This command is used to configure cahce 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

timeout - Specifies the SSL cache timeout value attributes.

<value 60-86400> - Enter the 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-3000-26TC:admin#config ssl cachetimeout 60
Commands: config ssl cachetimeout 60

Success.

DGS-3000-26TC:admin#
```

Chapter 67 Show Technical Support Command List

show tech_support**upload tech_support_toTFTP** {<ipaddr> <path_filename 64>}

67-1 show tech_support

Description

This command is especially used by the technical support personnel to dump the device overall operation information.

- Basic System Information
- System Log
- Running Configuration
- Layer 1 Information
- Layer 2 Information
- Storm Control
- Layer 2 Multicast
- Layer 3 Information
- Security
- Application
- OS Status
- Management

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 technique's support:

```

DGS-3000-26TC:admin#show tech_support
Command: show tech_support

#-----
#
#           DGS-3000-26TC Gigabit Ethernet Switch
#           Technical Support Information
#
#           Firmware: Build 1.00.015
#           Copyright(C) 2013 D-Link Corporation. All rights reserved.
#-----

*****      Basic System Information      *****

[SYS 2000-2-20 03:09:28]

Boot Time           : 20 Feb 2000  00:53:18
RTC Time            : 2000/02/20 03:09:28
Boot PROM Version   : Build 1.00.001
Firmware Version    : Build 1.00.015
Hardware Version    : A1
MAC Address         : 00-01-02-03-04-00
[ERROR_LOG 2000-2-20 03:09:28]

*****
# debug log: 1
# firmware version: 0.00.000
# level: CPU exception
# clock: 9710 ms
# time : 2000-01-01 00:00:10

```

67-2 upload tech_support_toTFTP

Description

This command is used to upload the information of technique's support to TFTP server.

- Basic System Information
- System Log
- Running Configuration
- Layer 1 Information
- Layer 2 Information
- Storm Control
- Layer 2 Multicast
- Layer 3 Information
- Security
- Application
- OS Status
- Management

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) Specifies the IP address of TFTP server.

<path_filename 64> - Specifies the file name to store the information of technique's support in TFTP server. The max size of the file name is 64.

Restrictions

Only Administrators and Operators can issue this command.

Example

To upload the information of technique's support:

```
DGS-3000-26TC: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-3000-26TC:admin#
```

Chapter 68 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

68-1 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-3000-26TC:admin#enable smtp
Command: enable smtp

Success.

DGS-3000-26TC:admin#
```

68-2 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-3000-26TC:admin#disable smtp
Command: disable smtp

Success.

DGS-3000-26TC:admin#
```

68-3 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 a SMTP server IP address:

```
DGS-3000-26TC:admin#config smtp server 172.18.208.9
Command: config smtp server 172.18.208.9

Success.

DGS-3000-26TC:admin#
```

To configure an SMTP server port:

```
DGS-3000-26TC:admin#config smtp server_port 25
Command: config smtp server_port 25

Success.

DGS-3000-26TC:admin#
```

To configure a mail source address:

```
DGS-3000-26TC:admin#config smtp self_mail_addr mail@dlink.com
Command: config smtp self_mail_addr mail@dlink.com

Success.

DGS-3000-26TC:admin#
```

To add a mail destination address:

```
DGS-3000-26TC:admin#config smtp add mail_receiver receiver@dlink.com
Command: config smtp add mail_receiver receiver@dlink.com

Success.

DGS-3000-26TC:admin#
```

To delete a mail destination address:

```
DGS-3000-26TC:admin#config smtp delete mail_receiver 1
Command: config smtp delete mail_receiver 1

Success.

DGS-3000-26TC:admin#
```

68-4 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-3000-26TC: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-3000-26TC:admin#
```

68-5 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-3000-26TC:admin#smtp send_testmsg
Command: smtp send_testmsg

Subject:e-mail heading
Content:e-mail content

Sending mail, please wait...

Success.

DGS-3000-26TC:admin#
```

Chapter 69 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 |

69-1 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 - Specifies the community string value used in the authentication of users wanting to access the Switch's SNMP agent.

<community_string 32> - Enter the community string value here. This string can be up to 32 characters long.

view_name - Specifies the view name of the MIB.

<view_name 32> - Enter the MIB view name here. This name can be up to 32 characters long.

readonly - Allows the user to use the above mentioned community string to have read-only access to the Switch's SNMP agent. The default read-only community string is public.

readwrite - Allows the user to use the above mentioned community string to have read and write access to the Switch's SNMP agent. 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-3000-26TC:admin#create snmp community System view CommunityView read_only
Command: create snmp community System view CommunityView read_only

Success.

DGS-3000-26TC:admin#
```

69-2 delete snmp community

Description

This command is used to delete an SNMP community string.

Format

delete snmp community <community_string 32>

Parameters

community - Specifies that the community string will be deleted.

<community_string 32> - Enter the community string value here. This value can be up to 32 characters long.

Restrictions

Only Administrators can issue this command.

Example

To delete a SNMP community "System":

```
DGS-3000-26TC:admin#delete snmp community System
Command: delete snmp community System

Success.

DGS-3000-26TC:admin#
```

69-3 show snmp community

Description

This command is used to display the community string configurations.

Format

show snmp community <community_string 32>

Parameters

<community_string 32> - (Optional) Specifies the Community string.

If no parameter is specified, all community string information will be displayed.

Restrictions

None.

Example

To display SNMP community:

```

DGS-3000-26TC: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-3000-26TC:admin#

```

69-4 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>** - The name of the user on the host that connects to the agent. The name can be up to 32 characters long.
-
- <groupname 32>** - The name of the group to which the user is associated. The name can be up to 32 characters long.
-
- encrypted** - (Optional) Specifies whether the password appears in encrypted format.
- by_password** - (Optional) Indicates input password for authentication and privacy.
- auth** - Initiates an authentication level setting session. The options are md5 and sha.
 - md5** - 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** - 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** - (Optional) 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** - (Optional) Indicates input key for authentication and privacy.
- auth** - An authentication string used by MD5 or SHA1.
 - md5** - 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** - 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** - (Optional) 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-3000-26TC: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-3000-26TC:admin#
```

69-5 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> - The name of the user on the host that connects to the agent. The name can be up to 32 characters long.

Restrictions

Only Administrators can issue this command.

Example

To delete a SNMP user “user123”:

```
DGS-3000-26TC:admin#delete snmp user user123
Command: delete snmp user user123

Success.

DGS-3000-26TC:admin#
```

69-6 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

None.

Example

To show SNMP user:

```
DGS-3000-26TC: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-3000-26TC:admin#
```

69-7 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

group - Specifies the name of the group.

<groupname 32> - Enter the group name here. This name can be up to 32 characters long.

v1 - The least secure of the possible security models.

v2c - The second least secure of the possible security models.

v3 - The most secure of the possible.

noauth_nopriv - Neither support packet authentication nor encrypting.

auth_nopriv - Support packet authentication.

auth_priv - Support packet authentication and encrypting.

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-3000-26TC: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-3000-26TC:admin#
```

69-8 delete snmp group

Description

This command is used to remove a SNMP group.

Format

delete snmp group <groupname 32>

Parameters

<groupname 32> - The name of the group will be deleted.

Restrictions

Only Administrators can issue this command.

Example

To delete SNMP group "group123":

```
DGS-3000-26TC:admin#delete snmp group group123
Command: delete snmp group group123

Success.

DGS-3000-26TC:admin#
```

69-9 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

None.

Example

To show SNMP groups:

```

DGS-3000-26TC:admin#show snmp groups
Command: show snmp groups

Vacm Access Table Settings

Group Name      : public
ReadView Name   : CommunityView
WriteView Name  :
Notify View Name : CommunityView
Security Model  : SNMPv1
Security Level   : NoAuthNoPriv

Group Name      : public
ReadView Name   : CommunityView
WriteView Name  :
Notify View Name : CommunityView
Security Model  : SNMPv2
Security Level   : NoAuthNoPriv

Group Name      : initial
ReadView Name   : restricted
WriteView Name  :
Notify View Name : restricted
Security Model  : SNMPv3
Security Level   : NoAuthNoPriv

Group Name      : WriteGroup
ReadView Name   : CommunityView
WriteView Name  : CommunityView
Notify View Name : CommunityView
Security Model  : SNMPv2
Security Level   : NoAuthNoPriv

Total Entries: 10

DGS-3000-26TC:admin#

```

69-10 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 - Specifies the view name to be created.

<view_name 32> - Enter the view name here. The name can be up to 32 characters long.

<oid> - Object-Identified tree, MIB tree.

view_type - Specifies the access type of the MIB tree in this view.

included - Includes for this view.

excluded - Excludes for this view.

Restrictions

Only Administrators can issue this command.

Example

To create SNMP view "view123":

```
DGS-3000-26TC:admin#create snmp view view123 1.3.6 view_type included
Command: create snmp view view123 1.3.6 view_type included

Success.

DGS-3000-26TC:admin#
```

69-11 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 to be deleted. The name can be up to 32 characters long.

all - Specifies that all view records will be removed.

<oid> - Object-Identified tree, MIB tree.

Restrictions

Only Administrators can issue this command.

Example

To delete SNMP view "view123":

```
DGS-3000-26TC:admin#delete snmp view view123 all
Command: delete snmp view view123 all

Success.

DGS-3000-26TC:admin#
```

69-12 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> - Enter the view name to be displayed. The name can be up to 32 characters long.

Restrictions

None.

Example

To show SNMP view:

```
DGS-3000-26TC: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-3000-26TC:admin#
```

69-13 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> - 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> - The IPv6 address of the recipient for which the traps are targeted. |
| v1 - Specifies that SNMPv1 will be used. This 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> - Specifies 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-3000-26TC:admin#create snmp host 10.0.0.1 v1 public
Command: create snmp host 10.0.0.1 v1 public

Success.

DGS-3000-26TC:admin#
```

69-14 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-3000-26TC:admin#delete snmp host 10.0.0.1
Command: delete snmp host 10.0.0.1

Success.

DGS-3000-26TC:admin#
```

69-15 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 of the recipient for which the traps are targeted.
If no parameter specified, all SNMP hosts will be displayed.

Restrictions

None.

Example

To show SNMP host:

```
DGS-3000-26TC: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-3000-26TC:
```

69-16 show snmp v6host

Description

This command is used to display the recipient for which the traps are targeted.

Format

show snmp v6host {<ipv6addr>}

Parameters

<ipv6addr> - (Optional) Enter the IPv6 host address used for the configuration here.

If no parameter specified, all SNMP hosts will be displayed.

Restrictions

None.

Example

To show SNMP host:

```
DGS-3000-26TC: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-3000-26TC:admin#
```


69-17 config snmp engineID

Description

This command is used to configure a 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-3000-26TC:admin#config snmp engineID 1023457890
Command: config snmp engineID 1023457890

Success.

DGS-3000-26TC:admin#
```

69-18 show snmp engineID

Description

The show snmp engineID command displays 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-3000-26TC:admin#show snmp engineID
Command: show snmp engineID

SNMP Engine ID : 1023457890

DGS-3000-26TC:admin#
```

69-19 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-3000-26TC:admin#enable snmp
Command: enable snmp

Success.

DGS-3000-26TC:admin#
```

69-20 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-3000-26TC:admin#disable snmp
Command: disable snmp

Success.

DGS-3000-26TC:admin#
```

69-21 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 SNMP system name used here. This name can be up to 255 characters long.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the Switch name for "DGS-30xx":

```
DGS-3000-26TC:admin#config snmp system_name DGS-30xx
Command: config snmp system_name DGS-30xx

Success.

DGS-3000-26TC:admin#
```

69-22 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 SNMP system location string here. This string can be up to 255 characters long.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the Switch location for "HQ 5F":

```
DGS-3000-26TC:admin#config snmp system_location HQ 5F
Command: config snmp system_location HQ 5F

Success.

DGS-3000-26TC:admin#
```

69-23 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 SNMP system contact string here. This name can be up to 255 characters long.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the Switch contact to "MIS Department II":

```
DGS-3000-26TC:admin#config snmp system_contact "MIS Department II"
Command: config snmp system_contact "MIS Department II"

Success.

DGS-3000-26TC:admin#
```

69-24 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-3000-26TC:admin#enable snmp traps
Command: enable snmp traps

Success.

DGS-3000-26TC:admin#
```

69-25 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-3000-26TC:admin#disable snmp traps
Command: disable snmp traps

Success.

DGS-3000-26TC:admin#
```

69-26 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-3000-26TC:admin#enable snmp authenticate_traps
Command: enable snmp authenticate_traps

Success.

DGS-3000-26TC:admin#
```

69-27 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-3000-26TC:admin#disable snmp authenticate_traps
Command: disable snmp authenticate_traps

Success.

DGS-3000-26TC:admin#
```

69-28 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-3000-26TC:admin#enable snmp linkchange_traps
Command: enable snmp linkchange_traps

Success.

DGS-3000-26TC:admin#
```

69-29 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-3000-26TC:admin#disable snmp linkchange_traps
Command: disable snmp linkchange_traps

Success.

DGS-3000-26TC:admin#
```

69-30 config snmp linkchange_traps ports

Description

This command is used to configure the sending of linkchange traps and per port control for sending of change trap.

Format

config snmp linkchange_traps ports [all | <portlist>] [enable | disable]

Parameters

all - Specifies that all ports will be used.

<portlist> - Enter the range of ports used.

enable - Enables the sending of the link change trap for this port.

disable - Disables the 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-3000-26TC:admin#config snmp linkchange_traps ports 1-4 enable
Command: config snmp linkchange_traps ports 1-4 enable

Success.

DGS-3000-26TC:admin#
```


69-31 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 - Enables the trap of the coldstart event. The default state is enabled.

disable - Disables the trap of the coldstart event.

Restrictions

Only Administrators can issue this command.

Example

To configure the trap for coldstart event:

```
DGS-3000-26TC:admin#config snmp coldstart_traps enable
Command: config snmp coldstart_traps enable

Success.

DGS-3000-26TC:admin#
```

69-32 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 - Enables the trap of the warmstart event. The default state is enabled.

disable - Disables the trap of the warmstart event.

Restrictions

Only Administrators can issue this command.

Example

To configure the trap state for warmstart event:

```
DGS-3000-26TC:admin#config snmp warmstart_traps enable
Command: config snmp warmstart_traps enable

Success.

DGS-3000-26TC:admin#
```

69-33 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 that the SNMP trap sending status will be displayed.
ports - (Optional) Specifies the ports for the display.
<portlist> - Enter the list of ports used for the display here.

Restrictions

None.

Example

```
DGS-3000-26TC:admin#show snmp traps
Command: show snmp traps

SNMP Traps           : Enabled
Authenticate Trap    : Enabled
Linkchange Traps     : Enabled
Coldstart Traps     : Enabled
Warmstart Traps      : Enabled

DGS-3000-26TC:admin#
```

69-34 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 - (Optional) 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 - (Optional) 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-3000-26TC:admin#config rmon trap rising_alarm disable
Command: config rmon trap rising_alarm disable

Success.

DGS-3000-26TC:admin#
```

69-35 show rmon

Description

This command is used to display the RMON related setting.

Format

show rmon

Parameters

None.

Restrictions

None.

Example

To display the RMON related setting:

```
DGS-3000-26TC:admin#show rmon
Command: show rmon

RMON Rising Alarm Trap      : Enabled
RMON Falling Alarm Trap    : Enabled

DGS-3000-26TC:admin#
```

Chapter 70 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> <path_filename> {[members <mslist 1-32> all]}} |
| upload sim_ms [configuration_to_tftp log_to_tftp] {<ipaddr> <path_filename> {[members <mslist> all]}} |
| config sim trap [enable disable] |

70-1 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-3000-26TC:admin#enable sim
Command: enable sim

Success.

DGS-3000-26TC:admin#
```

70-2 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-3000-26TC:admin#disable sim
Command: disable sim

Success.

DGS-3000-26TC:admin#
```

70-3 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 show the self information in detail:

```
DGS-3000-26TC:admin#show sim
Command: show sim

SIM Version      : VER-1.61
Firmware Version : 1.00.015
Device Name     :
MAC Address      : 00-01-02-03-04-00
Capabilities     : L2
Platform        : DGS-3000-26TC L2 Switch
SIM State       : Disabled
Role State      : Candidate
Discovery Interval : 30 sec
Hold Time       : 100 sec

DGS-3000-26TC:admin#
```

To show the candidate information in summary, if user specify candidate id, it would show information in detail:

```
DGS-3000-26TC:admin#show sim candidates
Command: show sim candidates

ID  MAC Address          Platform /          Hold  Firmware  Device Name
   MAC Address          Capability          Time  Version
---  -
  1  00-01-02-03-04-00  DGS-3000-26TC L2 Switch  40   1.00.015  Device
  2  00-55-55-00-55-00  DGS-3000-26TC L2 Switch  140  1.00.015  Device2

Total Entries: 2

DGS-3000-26TC:admin#
```

To show the member information in summary, if user specify member id, it will show information in detail:

```
DGS-3000-26TC:admin#show sim members
Command: show sim members

ID  MAC Address          Platform /           Hold  Firmware  Device Name
   MAC Address          Capability           Time  Version
-----
  1  00-01-02-03-04-00 DGS-3000-26TC L2 Switch  40    1.00.015  Device
  2  00-55-55-00-55-00 DGS-3000-26TC L2 Switch  140   1.00.015  Device2

Total Entries: 2

DGS-3000-26TC:admin#
```

To show other groups information in summary, if user specify group name, it will show information in detail:

```
DGS-3000-26TC:admin#show sim group
Command: show sim group

SIM Group Name : default

ID  MAC Address          Platform /           Hold  Firmware  Device Name
   MAC Address          Capability           Time  Version
-----
*1  00-01-02-03-04-00 DGS-3000-26TC L2 Switch  40    1.00.015  Device
   2  00-55-55-00-55-00

SIM Group Name : SIM2

ID  MAC Address          Platform /           Hold  Firmware  Device Name
   MAC Address          Capability           Time  Version
-----
*1  00-01-02-03-04-00 DGS-3000-26TC L2 Switch  40    1.00.015  Device
   2  00-55-55-00-55-00
   3  00-55-55-00-55-11

Total Entries: 2

DGS-3000-26TC:admin#
```

To show neighbor table of SIM:


```
DGS-3000-26TC:admin#show sim neighbor
Command: show sim neighbor

Neighbor Table

Port      MAC Address          Role
-----  -
23        00-35-26-00-11-99   Commander
23        00-35-26-00-11-91   Member
24        00-35-26-00-11-90   Candidate

Total Entries: 3

DGS-3000-26TC:admin#
```

70-4 reconfig

Description

This command is used to re-telnet to member.

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 re-telnet to member:

```
DGS-3000-26TC:admin#reconfig member_id 1
Command: reconfig member_id 1

DGS-3000-26TC:admin#
Login:
```

70-5 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-3000-26TC:admin#config sim_group add 2
Command: config sim_group add 2

Please wait for ACK !!!
SIM Configure Success !!!

Success.

DGS-3000-26TC:admin#
```

To delete a member:

```
DGS-3000-26TC:admin#config sim_group delete 1
Command: config sim_group delete 1

Please wait for ACK !!!
SIM Configure Success !!!

Success.

DGS-3000-26TC:admin#
```

70-6 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) 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) 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-3000-26TC:admin#config sim commander
Command: config sim commander

Success.

DGS-3000-26TC:admin#
```

To transfer to candidate:

```
DGS-3000-26TC:admin#config sim candidate
Command: config sim candidate

Success.

DGS-3000-26TC:admin#
```

To update name of group:

```
DGS-3000-26TC:admin#config sim commander group_name mygroup
Command: config sim commander group_name mygroup

Success.

DGS-3000-26TC:admin#
```

To change the time interval of discovery protocol:

```
DGS-3000-26TC:admin#config sim dp_interval 30
Command: config sim dp_interval 30

Success.

DGS-3000-26TC:admin#
```

To change the hold time of discovery protocol:

```
DGS-3000-26TC:admin#config sim hold_time 200
Command: config sim hold_time 200

Success.

DGS-3000-26TC:admin#
```

70-7 download sim_ms

Description

This command is used to download firmware or configuration to indicated device.

Format

**download sim_ms [firmware_from_tftp | configuration_from_tftp] {<ipaddr>
<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) Specifies the IP address of the TFTP server.

<path_filename> - (Optional) Specifies 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-3000-26TC: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-3000-26TC:admin#
```

To download firmware:

```
DGS-3000-26TC: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-3000-26TC:admin#
```

70-8 upload sim_ms

Description

This command is used to upload configuration to TFTP server.

Format

upload sim_ms [configuration_to_tftp | log_to_tftp] [<ipaddr> <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) Specifies the IP address of the TFTP server.

<path_filename> - Specifies the file path to store the configuration in the TFTP server.

members - (Optional) Specifies a range of members who can up this configuration.

<mslist> - (Optional) 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-3000-26TC: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-3000-26TC:admin#
```

70-9 config sim trap**Description**

This command is used to control sending of traps issued from the member switch.

Format

config sim trap [enable | disable]

Parameters

enable - Enable the trap state.

disable - Disable the trap state.

Restrictions

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

Example

To enable sim trap:

```
DGS-3000-26TC:admin#config sim trap enable
Command: config sim trap enable

Success.

DGS-3000-26TC:admin#
```

Chapter 71 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
```

71-1 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. If only specify this parameter, the least IPv4 address and the smallest IPv6 address of ipif_name will be used as source IP addresses. This name can be up to 12 characters long.

<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-3000-26TC:admin#config syslog source_ipif ipif3 14.0.0.5
Command: config syslog source_ipif ipif3 14.0.0.5

Success

DGS-3000-26TC:admin#
```

To clear the configured source IP interface for syslog:

```
DGS-3000-26TC:admin#config syslog source_ipif none
Command: config syslog source_ipif none

Success

DGS-3000-26TC:admin#
```

71-2 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-3000-26TC:admin#show syslog source_ipif
Command: show syslog source_ipif

Syslog Source IP Interface Configuration:

IP Interface           : ipif3
IPv4 Address           : 14.0.0.5
IPv6 Address           : None

DGS-3000-26TC:admin#
```

71-3 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 - Specifies the IP interface name. If only specify this parameter, the least IPv4 address and the smallest IPv6 address of ipif_name will be used as source IP addresses.
<ipif_name 12> - Enter the IP interface name here. This name can be up to 12 characters long.
<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-3000-26TC:admin#config trap source_ipif System
Command: config trap source_ipif System

Success

DGS-3000-26TC:admin#
```

To clear the configured trap source IP interface:

```
DGS-3000-26TC:admin#config trap source_ipif none
Command: config trap source_ipif none

Success

DGS-3000-26TC:admin#
```

71-4 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-3000-26TC: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-3000-26TC:admin#
```

Chapter 72 System Log Command List

| |
|--|
| clear 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 |
| enable syslog |
| disable syslog |
| show 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]}(1) |
| delete syslog host [<index 1-4> all] |
| show syslog host {<index 1-4>} |
| config log_save_timing [time_interval <min 1-65535> on_demand log_trigger] |
| show log_save_timing |
| show attack_log {index <value_list>} |
| clear attack_log |

72-1 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-3000-26TC:admin#clear log
Command: clear log

Success.

DGS-3000-26TC:admin#
```

72-2 show log

Description

This command is used to display the Switch's history log.

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 the index value of log entries that will be displayed. For example, specifying 1-5 will display the history log from 1 to 5.

<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-3000-26TC: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-3000-26TC:admin#

```

72-3 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-3000-26TC:admin#show log_software_module
Command: show log_software_module

ERPS                ERROR_LOG           MSTP

DGS-3000-26TC:admin#

```

72-4 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-3000-26TC:admin#enable syslog
Command: enable syslog

Success.

DGS-3000-26TC:admin#
```

72-5 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-3000-26TC:admin#disable syslog
Command: disable syslog

Success.

DGS-3000-26TC:admin#
```

72-6 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-3000-26TC:admin#show syslog
Command: show syslog

Syslog Global State: Enabled

DGS-3000-26TC:admin#
```

72-7 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) 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-3000-26TC: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-3000-26TC:admin#
```

72-8 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]}(1)
```

Parameters

| |
|---|
| <index> - Enter the host index value here. |
| all - Specifies that all the host indexes will be used. |
| severity - 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 - 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 - Specifies the UDP port number. <udp_port_number> - Enter the UDP port number used here. |
| ipaddress - 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 - 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-3000-26TC:admin#config syslog host all severity debug facility local0
Command: config syslog host all severity debug facility local0

Success.

DGS-3000-26TC:admin#
```

72-9 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-3000-26TC:admin#delete syslog host 4
Command: delete syslog host 4

Success.

DGS-3000-26TC:admin#
```

72-10 show syslog host

Description

This command is used to display the syslog host configurations.

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-3000-26TC:admin#show syslog host
Command: show syslog host

Syslog Global State: Disabled

Host 1
  IP Address      : 10.90.90.1
  Severity       : Debug(7)
  Facility       : Local0
  UDP Port       : 514
  Status        : Disabled

Total Entries : 1

DGS-3000-26TC:admin#

```

72-11 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 time interval used for saving the log. If there is no new log event during this time interval, the Switch will not save any log entries.

<min 1-65535> - Enter the time interval value here. This value must be between 1 and 65535 minutes.

on_demand - Specifies that the log will only be saved when an on-demand event occurs. For example, issuing the command **save all** or **save log**. This is the default option.

log_trigger - Specifies that the log will be saved when a new log event is triggered.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the method for saving a log as on demand:

```
DGS-3000-26TC:admin#config log_save_timing on_demand
Command: config log_save_timing on_demand

Success.

DGS-3000-26TC:admin#
```

72-12 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-3000-26TC:admin#show log_save_timing
Command: show log_save_timing

Saving Log Method: On_demand

DGS-3000-26TC:admin#
```

72-13 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. 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, the 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-3000-26TC: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-3000-26TC:admin#
```

72-14 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-3000-26TC:admin#clear attack_log
Command: clear attack_log

Success.

DGS-3000-26TC:admin#
```

Chapter 73 System Severity Command List

```
config system_severity [trap | log | all] [emergency | alert| critical | error | warning | notice |  
information | debug | <level 0-7>]  
show system_severity
```

73-1 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 - Severity level 0.

alert - Severity level 1.

critical - Severity level 2.

error - Severity level 3.

warning - Severity level 4.

notice - Severity level 5.

information - Severity level 6.

debug - Severity level 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-3000-26TC:admin#config system_severity trap warning
Command: config system_severity trap warning

Success.

DGS-3000-26TC:admin#
```

73-2 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-3000-26TC:admin#show system_severity
Command: show system_severity

System Severity Trap : warning(4)
System Severity Log : information(6)

DGS-3000-26TC:admin#
```

Chapter 74 Telnet Client Command List

```
telnet [<ipaddr> | <domain_name 255> [<ipv6addr>] {tcp_port <value 1-65535>}
```

74-1 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> - The IP address of the TLENET server.

<domain_name 255> - The domain name of the TLENET server.

<ipv6addr> - 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.

<ipaddr> - The IP 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-3000-26TC:admin#telnet 10.90.90.90
Command: telnet 10.90.90.90

DGS-3000-26TC Gigabit Ethernet Switch
Command Line Interface

Firmware: Build 1.00.015
Copyright(C) 2013 D-Link Corporation. All rights reserved.

UserName:
```


Chapter 75 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_filename 64>
  {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

```

75-1 download

Description

This command is used to download the firmware image and configuration from 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 firmware from a TFTP server.

<ipaddr> - (Optional) The IP address of the TFTP server.

<ipv6addr> - (Optional) The IPv6 address of the TFTP server.

<domain_name 255> - (Optional) The domain name of the TFTP server.

src_file - (Optional) Specifies the source file path name.

<path_filename 64> - Enter the source file path name here. This name can be up to 64 characters long.

dest_file - (Optional) Specifies the destination file path name.

<pathname 64> - Enter the destination file path name 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) The IP address of the TFTP server.

<ipv6addr> - (Optional) The IPv6 address of the TFTP server.

<domain_name 255> - (Optional) The domain name of the TFTP server.

src_file - (Optional) Specifies the source file path name.

<path_filename 64> - 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 the destination file path name.

<pathname 64> - 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) The IP address of the FTP server.

tcp_port - Specifies the TCP port.

<tcp_port number 1-65535> - Enter a value between 1 and 65535.

src_file - Specifies the source file location.

<path_filename 64> - 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 the destination file path name.

<path_filename 64> - The pathname specifies an absolute pathname on the device file system. If pathname is not specified, it refers to the boot_up configuration 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> - 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 the source file path name.

<path_filename 64> - 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 the destination file path name.

<path_filename 64> - 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-3000-26TC: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-3000-26TC:admin#
```

To download configuration from TFTP:

```
DGS-3000-26TC: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-3000-26TC:admin#
```

75-2 upload

Description

This command is used to upload firmware and configuration from device to TFTP/FTP server.

Format

```
upload [cfg_toTFTP {[<ipaddr> | <ipv6addr> | <domain_name 255>] dest_file <path_filename
64> {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>** - The IP address of the TFTP server.
 - <ipv6addr>** - (Optional) The IPv6 address of the TFTP server.
 - <domain_name 255>** - (Optional) The domain name of the TFTP server.
 - dest_file** - Specifies the destination file path name.
 - <path_filename 64>** - 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 the source file path name.
 - <pathname 64>** - 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) The first line that contains the specified filter string will be the first line of the output.
 - <filter_string 80>** - A filter string is enclosed by symbol. Thus, the filter string itself cannot contain the character. The filter string is case sensitive. This string can be up to 80 characters long.
 - <filter_string 80>** - (Optional) A filter string is enclosed by symbol. Thus, the filter string itself cannot contain the character. The filter string is case sensitive. This string can be up to 80 characters long.
 - <filter_string 80>** - (Optional) A filter string is enclosed by symbol. Thus, the filter string itself cannot contain the character. The filter string is case sensitive. This string 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) The first line that contains the specified filter string will be the first line of the output.
 - <filter_string 80>** - A filter string is enclosed by symbol. Thus, the filter string itself cannot contain the character. The filter string is case sensitive. This string can be up to 80 characters long.
 - <filter_string 80>** - (Optional) A filter string is enclosed by symbol. Thus, the filter string itself cannot contain the character. The filter string is case sensitive. This string can be up to 80 characters long.
 - <filter_string 80>** - (Optional) A filter string is enclosed by symbol. Thus, the filter string itself cannot contain the character. The filter string is case sensitive. This string 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) The first line that contains the specified filter string will be the first line of the output.
 - <filter_string 80>** - A filter string is enclosed by symbol. Thus, the filter string itself cannot contain the character. The filter string is case sensitive. This string can be up to 80 characters long.
 - <filter_string 80>** - (Optional) A filter string is enclosed by symbol. Thus, the filter string itself cannot contain the character. The filter string is case sensitive. This string can be up to 80 characters long.
 - <filter_string 80>** - (Optional) A filter string is enclosed by symbol. Thus, the filter string itself cannot contain the character. The filter string is case sensitive. This string can be up to 80 characters long.
-
- log_toTFTP** - Specifies to upload a log file from device to TFTP server.
- <ipaddr>** - The IP address of the TFTP server.
 - <ipv6addr>** - (Optional) The IPv6 address of the TFTP server.
 - <domain_name 255>** - (Optional) The domain name of the TFTP server.
 - dest_file** - Specifies the destination file path name.
 - <path_filename 64>** - 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> - The IP address of the TFTP server.

<ipv6addr> - (Optional) The IPv6 address of the TFTP server.

<domain_name 255> - (Optional) The domain name of the TFTP server.

dest_file - Specifies the destination file path name.

<path_filename 64> - Specifies the path name 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> - The IP address of the TFTP server.

<ipv6addr> - (Optional) The IPv6 address of the TFTP server.

<domain_name 255> - (Optional) The domain name of the TFTP server.

dest_file - Specifies the destination file path name.

<path_filename 64> - 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 the source file path name.

<pathname 64> - 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> - 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 the destination file path name.

<path_filename 64> - 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 the source file path name.

<pathname 64> - 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) The first line that contains the specified filter string will be the first line of the output.

<filter_string 80> - A filter string is enclosed by symbol. Thus, the filter string itself cannot contain the character. The filter string is case sensitive. This string can be up to 80 characters long.

<filter_string 80> - (Optional) A filter string is enclosed by symbol. Thus, the filter string itself cannot contain the character. The filter string is case sensitive. This string can be up to 80 characters long.

<filter_string 80> - (Optional) A filter string is enclosed by symbol. Thus, the filter string itself cannot contain the character. The filter string is case sensitive. This string 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) The first line that contains the specified filter string will be the first line of the output.

<filter_string 80> - A filter string is enclosed by symbol. Thus, the filter string itself cannot contain the character. The filter string is case sensitive. This string can be up to 80 characters long.

<filter_string 80> - (Optional) A filter string is enclosed by symbol. Thus, the filter string itself cannot contain the character. The filter string is case sensitive. This string can be up to 80 characters long.

<filter_string 80> - (Optional) A filter string is enclosed by symbol. Thus, the filter string itself cannot contain the character. The filter string is case sensitive. This string 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) The first line that contains the specified filter string will be the first line of the output.

<filter_string 80> - A filter string is enclosed by symbol. Thus, the filter string itself cannot contain the character. The filter string is case sensitive. This string can be up to 80 characters long.

<filter_string 80> - (Optional) A filter string is enclosed by symbol. Thus, the filter string itself cannot contain the character. The filter string is case sensitive. This string can be up to 80 characters long.

<filter_string 80> - (Optional) A filter string is enclosed by symbol. Thus, the filter string itself cannot contain the character. The filter string is case sensitive. This string can be up to 80 characters long.

log_toFTP - Specifies to upload a log file from device to FTP server.

<ipaddr> - 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 the destination file path name.

<path_filename 64> - 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> - 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 the destination file path name.

<path_filename 64> - Specifies the path name 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> - 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 the destination file path name.

<path_filename 64> - 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 the source file path name.

<pathname 64> - 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-3000-26TC: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-3000-26TC: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 exist.

```
DGS-3000-26TC: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-3000-26TC:admin#
```

To upload configuration from TFTP:

```
DGS-3000-26TC: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-3000-26TC: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 exist.

```
DGS-3000-26TC: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-3000-26TC:admin#
```

To upload the attack log:

```
DGS-3000-26TC: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-3000-26TC:admin#
```

75-3 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> - The IP address of the TFTP server. |
| firmware_file - (Optional) Specifies the pathname supports "download/upload firmware_fromTFTP" function. <path_filename 64> - Specifies the pathname supports "download/upload firmware_fromTFTP" function. |
| cfg_file - (Optional) Specifies the pathname supports "download/upload cfg_fromTFTP" function. <path_filename 64> - Specifies the pathname supports "download/upload cfg_fromTFTP" function. |
| log_file - (Optional) Specifies the pathname supports "upload log_toTFTP" function. <path_filename 64> - Specifies the pathname supports "upload log_toTFTP" function. |
| attack_log_file - (Optional) Specifies the pathname supports "upload attack_log_toTFTP" function. <path_filename 64> - Specifies the pathname supports "upload attack_log_toTFTP" function. |
| certificate_file - (Optional) Specifies the pathname supports "download ssl certificate" function. <path_filename 64> - Specifies the pathname supports "download ssl certificate" function. |
| key_file - (Optional) Specifies the pathname supports "download ssl certificate" function. <path_filename 64> - Specifies the pathname supports "download ssl certificate" function. |
| tech_support_file - (Optional) Specifies specifying the pathname supports "upload tech_support_toTFTP" function. <path_filename 64> - Specifies 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> - Specifies 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> - Specifies 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> - Specifies 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> - Specifies 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-3000-26TC:admin#config tftp server 10.90.90.10
Command: config tftp server 10.90.90.10

Success.

DGS-3000-26TC:admin#
```

To configure TFTP server and specify the pre defined firmware file, log file:

```
DGS-3000-26TC:admin#config tftp server 10.90.90.1 firmware_file DGS3000.had
cfg_file log_tmp
Command: config tftp server 10.90.90.1 firmware_file DGS3000.had cfg_file
log_tmp

Success.

DGS-3000-26TC:admin#
```

75-4 show tftp

Description

This command is used to show the TFTP server and the file path pre-configured by administrator.

Format

show tftp

Parameters

None.

Restrictions

None.

Example

To show TFTP settings, if pre-configure server IPv4 address, firmware_file and cfg_file only:

```
DGS-3000-26TC:admin#show tftp
```

```
Command: show tftp
```

```
TFTP Server Settings
```

```
IPv4 Address : 10.90.90.1
```

| File Type | Path_filename |
|----------------------|---------------|
| ----- | ----- |
| firmware_file | DGS3000.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-3000-26TC:admin#
```

Chapter 76 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 |

76-1 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) SNTP primary server IP address. <ipaddr> - Enter the IP address used for this configuration here. |
| secondary - (Optional) 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, Operators and Power-Users can issue this command.

Example

To configure SNTP:

```
DGS-3000-26TC: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-3000-26TC:admin#
```

76-2 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-3000-26TC:admin#show sntp  
Command: show sntp  
  
Current Time Source : System Clock  
SNTP : Disabled  
SNTP Primary Server : 10.1.1.1  
SNTP Secondary Server : 10.1.1.2  
SNTP Poll Interval : 30 sec  
  
DGS-3000-26TC:admin#
```

76-3 enable sntp

Description

This command is used to turn on SNTP support.

Format

enable sntp

Parameters

None.

Restrictions

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

Example

To enable SNTP:

```
DGS-3000-26TC:admin#enable sntp
Command: enable sntp

Success.

DGS-3000-26TC:admin#
```

76-4 disable sntp

Description

This command is used to turn off SNTP support.

Format

disable sntp

Parameters

None.

Restrictions

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

Example

To disable SNTP:

```
DGS-3000-26TC:admin#disable sntp
Command: disable sntp

Success.

DGS-3000-26TC:admin#
```

76-5 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, Operators and Power-Users can issue this command.

Example

To configure time:

```
DGS-3000-26TC:admin#config time 30jun2003 16:30:30
Command: config time 30jun2003 16:30:30

Success.

DGS-3000-26TC:admin#
```

76-6 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, Operators and Power-Users can issue this command.

Example

To configure time_zone:

```
DGS-3000-26TC:admin#config time_zone operator + hour 2 min 30
Command: config time_zone operator + hour 2 min 30

Success.

DGS-3000-26TC:admin#
```

76-7 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 - Sets the Daylight Saving Time to repeating mode.

s_week - (Optional) Specifies the start week 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 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 - (Optional) Specifies 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 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 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 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 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 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) Indicates 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 - Set the Daylight Saving Time to annual mode.

s_date - (Optional) Specifies 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 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 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 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 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 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) Indicates 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, Operators and Power-Users can issue this command.

Example

To configure time:

```
DGS-3000-26TC: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-3000-26TC:admin#
```

76-8 show time

Description

This command is used to display time states.

Format

show time

Parameters

None.

Restrictions

None.

Example

To show time:

```
DGS-3000-26TC: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-3000-26TC:admin#
```

Chapter 77 Trace Route Command List

```

tracert [<ipaddr> | <domain_name 255>] {ttl <value 1-60> | port <value 30000-64900> |
  timeout <sec 1-65535> | probe <value 1-9>}
tracert6 [<ipv6addr> | <domain_name 255>] {ttl <value 1-60> | port <value 30000-64900> |
  timeout <sec 1-65535> | probe <value 1-9>}

```

77-1 tracert

Description

This command is used to trace the routed path between the Switch and a destination end station.

Format

```

tracert [<ipaddr> | <domain_name 255>] {ttl <value 1-60> | port <value 30000-64900> |
  timeout <sec 1-65535> | probe <value 1-9>}

```

Parameters

<ipaddr> - Specifies the IP address of the destination end station.

<domain_name 255> - The domain name of the destination end station.

ttl - (Optional) 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 tracert 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) 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) 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-3000-26TC: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-3000-26TC:admin#
```

77-2 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> - Specifies the IPv6 address of the destination end station.

<domain_name 255> - The domain name of the destination end station.

ttl - (Optional) 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) 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) 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-3000-26TC: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-3000-26TC:admin#
```

Trace the IPv6 routed path between the Switch and 1210:100::11 with port 40000:

```
DGS-3000-26TC: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-3000-26TC:admin#
```

Chapter 78 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>] |

78-1 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> - Specifies 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) One of the two options for action is specified for storm control, 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) The upper threshold, at which point the specified storm control is triggered. The <value> is the number of broadcast/multicast/unknown unicast packets per second received by the Switch that will trigger the storm traffic control measure. The threshold is expressed as PPS (packets per second) and must be an unsigned integer. |
| <value 0-255000> - Enter the upper threshold value here. This value must be between 0 and 255000. |

countdown - (Optional) Timer for shutdown mode. If a port enters the shutdown Rx state and this timer runs out, port will be shutdown forever. The parameter is not applicable if “drop” (mode) is specified for the “action” parameter.

<min 0> - 0 disables the forever state, meaning 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) The sampling interval of received packet counts. The possible value will be m-n seconds. The parameter is not applicable if “drop” (mode) is specified for the “action” parameter.

<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-3000-26TC: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-3000-26TC:admin#
```

78-2 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 - No trap state is specified for storm control.

storm_occurred - Occurred mode is enabled and cleared mode is disabled.

storm_cleared - Occurred mode is disabled and cleared mode is enabled.

both - Both occurred and cleared modes are enabled.

Restrictions

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

Example

To enable both the occurred mode and cleared mode traffic control traps:

```
DGS-3000-26TC:admin#config traffic trap both
Command: config traffic trap both

Success.

DGS-3000-26TC:admin#
```

78-3 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-3000-26TC: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-3000-26TC:admin#

```

78-4 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 - Both occurred and cleared are logged.

disable - Neither occurred nor cleared is logged.

Restrictions

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

Example

To configure the traffic log state on the Switch:


```
DGS-3000-26TC:admin#config traffic control log state enable
Command: config traffic control log state enable

Success.

DGS-3000-26TC:admin#
```

78-5 config traffic control auto_recover_time

Description

This command is used to configure the traffic auto-recovery time that is allowed for a port to recover from the shutdown forever status. When the auto-recovery option is disabled on a port, the port will remain in the shutdown mode. The only way to restore the port to the forwarding state is by entering the **config ports [<portlist> | all] state enable** command manually.

Format

config traffic control auto_recover_time [<min 0> | <min 1-65535>]

Parameters

<min 0> - Specifies that the auto-recovery option will be disabled. This is the default value.

<min 1-65535> - Enter the auto-recovery from shutdown 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-recovery time to 5 minutes:

```
DGS-3000-26TC:admin#config traffic control auto_recover_time 5
Command: config traffic control auto_recover_time 5

Success.

DGS-3000-26TC:admin#
```

Chapter 79 Traffic Segmentation Command List

```
config traffic_segmentation [<portlist> | all] forward_list [null | all | <portlist>]
show traffic_segmentation {<portlist>}
```

79-1 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> - Specifies 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> - Specifies a range of ports to be configured.

Restrictions

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

Example

To configure traffic segmentation:

```
DGS-3000-26TC:admin#config traffic_segmentation 1-10 forward_list 11-15
Command: config traffic_segmentation 1-10 forward_list 11-15

Success.

DGS-3000-26TC:admin#
```

79-2 show traffic_segmentation

Description

This command is used to display current traffic segmentation table.

Format

```
show traffic_segmentation {<portlist>}
```

Parameters

<portlist> - (Optional) Specifies 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-3000-26TC:admin#show traffic_segmentation 1-10
```

```
Command: show traffic_segmentation 1-10
```

```
Traffic Segmentation Table
```

```
Port   Forward Portlist
```

| 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-3000-26TC:admin#
```

Chapter 80 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
```

80-1 create trusted_host

Description

This command is used to create the trusted host. The switch allows you to specify up to ten IPv4 and IPv6 addresses that are allowed to manage the Switch via in-band SNMP, TELNET or WEB based management software. These IPv4 or IPv6 addresses must be members of the Management VLAN. If no IPv4 or IPv6 addresses are specified, then there is nothing to prevent any IPv4 or IPv6 addresses 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> - The IP address of the trusted host.
<ipv6addr> - The IPv6 address of the trusted host.
network - 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 that IPv6 prefix here.
  <ipv6networkaddr> - Enter the IPv6 network address here.
snmp - (Optional) Specifies trusted host for SNMP.
telnet - (Optional) Specifies trusted host for TELENT.
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-3000-26TC:admin#create trusted_host 10.48.74.121
Command: create trusted_host 10.48.74.121

Success.

DGS-3000-26TC:admin#
```

80-2 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 - The IP address of the trusted host.

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

ipv6addr - The IPv6 address of the trusted host.

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

network - The network address of the trusted network.

<network_address> - Enter the network address used for this configuration here.

ipv6_prefix - The IPv6 subnet prefix of the trusted network.

<ipv6networkaddr> - Enter the IPv6 subnet prefix here.

all - All trusted hosts will be deleted.

Restrictions

Only Administrators and Operators can issue this command.

Example

To delete the trusted host:

```
DGS-3000-26TC:admin#delete trusted_host ipaddr 10.48.74.121
Command: delete trusted_host ipaddr 10.48.74.121

Success.

DGS-3000-26TC:admin#
```

80-3 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> - The IP address of the trusted host. |
| <ipv6addr> - The IPv6 address of the trusted host. |
| network - 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 - The IPv6 subnet prefix of the trusted network. |
| <ipv6networkaddr> - Enter the IPv6 subnet prefix here. |
| add - Adds interfaces for that trusted host. |
| delete - Deletes interfaces for that trusted host. |
| snmp - (Optional) Specifies trusted host for SNMP. |
| telnet - (Optional) Specifies trusted host for TELENT. |
| 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-3000-26TC:admin#config trusted_host 10.48.74.121 add ssh telnet
Command: config trusted_host 10.48.74.121 add ssh telnet

Success.

DGS-3000-26TC:admin#
```

80-4 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-3000-26TC:admin#show trusted_host
Command: show trusted_host

Management Stations

IP Address                               Access Interface
-----
10.48.74.121                             SNMP Telnet SSH HTTP HTTPs Ping

Total Entries: 1

DGS-3000-26TC:admin#
```

Chapter 81 Unicast Routing Command List

create iproute [default] <ipaddr> {<metric 1-65535>}**delete iproute** [default]**show iproute** {<network_address>} {static}

81-1 create iproute

Description

This command is used to create an IP static route.

Format

create iproute [default] <ipaddr> {<metric 1-65535>}

Parameters

default - Specifies to create an IP default route (0.0.0.0/0).**<ipaddr>** - The IP address for the next hop router.**<metric 1-65535>** - (Optional) Enter the metric value here. This value must be between 1 and 65535. The default setting is 1.

Restrictions

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

Example

To add an IP default route:

```
DGS-3000-26TC:admin#create iproute default 10.1.1.254
```

```
Command: create iproute default 10.1.1.254
```

```
Success.
```

```
DGS-3000-26TC:admin#
```

81-2 delete iproute

Description

This command is used to delete an IP route entry from the Switch's IP routing table.

Format

delete iproute [default]

Parameters

default - Deletes an IP default route (0.0.0.0/0).

Restrictions

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

Example

To delete an IP default route:

```
DGS-3000-26TC:admin#delete iproute default 10.1.1.254
Command: delete iproute default 10.1.1.254

Success.

DGS-3000-26TC:admin#
```

81-3 show iproute

Description

This command is used to display the Switch's current IP routing table.

Format

show iproute {<network_address>} {static}

Parameters

<network_address> - (Optional) Specifies the destination network address of the route to 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-3000-26TC:admin#show iproute  
Command: show iproute
```

Routing Table

| IP Address/Netmask | Gateway | Interface | Cost | Protocol |
|--------------------|---------|-----------|------|----------|
| 10.1.1.0/24 | 0.0.0.0 | System | 1 | Local |
| 192.168.1.0/24 | 0.0.0.0 | ip1 | 1 | Local |

Total Entries : 2

```
DGS-3000-26TC:admin#
```

Chapter 82 VLAN Trunking Command List

| |
|--|
| enable vlan_trunk |
| disable vlan_trunk |
| config vlan_trunk ports [<portlist> all] state [enable disable] |
| show vlan_trunk |

82-1 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-3000-26TC:admin#enable vlan_trunk
Command: enable vlan_trunk

Success.

DGS-3000-26TC:admin#
```

82-2 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-3000-26TC:admin#disable vlan_trunk
Command: disable vlan_trunk

Success.

DGS-3000-26TC:admin#
```

82-3 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 member port of all VLANs. That is, if a VLAN is already configured by the user, but the trunk port is not member port of that VLAN, this trunk port will automatically become tagged member port of that VLAN. If a VLAN is not created yet, 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 passed will not be advertised by GVRP on this port. However, since the traffic on these VLANs are forwarded, this VLAN trunk port should participate the MSTP instances corresponding to these VLAN.

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-3000-26TC:admin#config vlan_trunk ports 1-5 state enable
Command: config vlan_trunk ports 1-5 state enable

Success.

DGS-3000-26TC:admin#
```

Port 6 is LA-1 member port; port 7 is LA-2 master port:

```
DGS-3000-26TC:admin#config vlan_trunk ports 6-7 state enable
Command: config vlan_trunk ports 6-7 state enable

Warning: Port 6 is a Link Aggregation member port, VLAN trunk is not enabled on
port 6.
Success.

DGS-3000-26TC:admin#config vlan_trunk ports 7 state disable
Command: config vlan_trunk ports 7 state disable

Success.

DGS-3000-26TC:admin#config vlan_trunk ports 6-7 state disable
Command: config vlan_trunk ports 6-7 state disable

Warning: Port 6 is a Link Aggregation member port, VLAN trunk is not enabled on
port 6.
Success.

DGS-3000-26TC:admin#
```

Port 6 is LA-1 member port; port 7 is LA-1 master port:

```
DGS-3000-26TC:admin#config vlan_trunk ports 6-7 state enable
Command: config vlan_trunk ports 6-7 state enable

Success.

DGS-3000-26TC: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-3000-26TC:admin#config vlan_trunk ports 7 state disable
Command: config vlan_trunk ports 7 state disable

Success.

DGS-3000-26TC:admin#config vlan_trunk ports 6-7 state disable
Command: config vlan_trunk ports 6-7 state disable

Success.

DGS-3000-26TC:admin#
```

82-4 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-3000-26TC:admin#show vlan_trunk
Command: show vlan_trunk

VLAN Trunk Global Setting
-----
VLAN Trunk Status   : Disabled
VLAN Trunk Member Ports : 1-5

DGS-3000-26TC:admin#
```

The following example displays the VLAN information which will also display VLAN trunk setting:

```
DGS-3000-26TC: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 : 1-26
Static Ports : 1-26
Current Tagged Ports :
Current Untagged Ports: 1-26
Static Tagged Ports  :
Static Untagged Ports : 1-26
Forbidden Ports      :

Total Static VLAN Entries: 1
Total GVRP VLAN Entries: 0

DGS-3000-26TC:admin#
```

Chapter 83 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 |

83-1 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-3000-26TC:admin#enable voice_vlan v2
Command: enable voice_vlan v2

Success.

DGS-3000-26TC:admin#
```

83-2 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-3000-26TC:admin#disable voice_vlan
Command: disable voice_vlan

Success.

DGS-3000-26TC:admin#
```

83-3 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 priority 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-3000-26TC:admin#config voice_vlan priority 6
Command: config voice_vlan priority 6

Success.

DGS-3000-26TC:admin#
```

83-4 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 - Deletes a user-defined OUI of a voice device vendor.

<macaddr> - The user-defined OUI MAC address.

<macmask> - 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-3000-26TC:admin#config voice_vlan oui add 00-0A-0B-00-00-00 FF-FF-FF-00-00-00
0
Command: config voice_vlan oui add 00-0A-0B-00-00-00 FF-FF-FF-00-00-00

Success.

DGS-3000-26TC:admin#
```

83-5 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 - 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 - 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-3000-26TC:admin#config voice_vlan ports 4-6 state enable
Command: config voice_vlan ports 4-6 state enable

Success.

DGS-3000-26TC:admin#
```

To set the mode auto to voice VLAN ports 3-5:

```
DGS-3000-26TC:admin#config voice_vlan ports 3-5 mode auto
Command: config voice_vlan ports 3-5 mode auto

Success.

DGS-3000-26TC:admin#
```

83-6 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-3000-26TC:admin#config voice_vlan aging_time 60
Command: config voice_vlan aging_time 60

Success.

DGS-3000-26TC:admin#
```

83-7 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-3000-26TC:admin#config voice_vlan log state enable
Command: config voice_vlan log state enable

Success.

DGS-3000-26TC:admin#
```

83-8 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-3000-26TC: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-3000-26TC:admin#
```

To display the voice VLAN global information when voice VLAN is disabled:

```
DGS-3000-26TC: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-3000-26TC:admin#
```

83-9 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-3000-26TC: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-3000-26TC:admin#
```

83-10 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-3000-26TC: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-3000-26TC:admin#
```

83-11 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-3000-26TC: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  2008-10-6 09:00    2008-10-6 10:30
1      00-E0-BB-00-00-02  2008-10-6 14:10    2008-10-6 15:00
1      00-E0-BB-00-00-03  2008-10-6 14:20    2008-10-6 15:30
2      00-03-6B-00-00-01  2008-10-6 17:15    2008-10-6 18:00
4      00-E0-75-00-00-02  2008-10-6 18:15    2008-10-6 20:00
5      00-01-E3-01-02-03  2008-10-6 18:30    2008-10-6 20:30

Total Entries : 6

DGS-3000-26TC:admin#
```

83-12 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-3000-26TC: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-3000-26TC:admin#
```

Chapter 84 Password Recovery Command List

enable password_recovery
disable password_recovery
show password_recovery

84-1 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-3000-26TC:admin#enable password_recovery
Command: enable password_recovery

Success.

DGS-3000-26TC:admin#
```

84-2 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-3000-26TC:admin#disable password_recovery
Command: disable password_recovery

Success.

DGS-3000-26TC:admin#
```

84-3 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-3000-26TC:admin#show password_recovery
Command: show password_recovery

Running Configuration   : Enabled
NV-RAM Configuration   : Enabled

DGS-3000-26TC: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.

```

Boot Procedure                                     V1.00.001
-----
Power On Self Test ..... 100 %

MAC Address   : 00-01-02-03-04-00
H/W Version   : A1

Please Wait, Loading V1.00.015 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 | Configuration saved to flash by console(Username: <username>, IP: <ipaddr>) | Informational |
| | System log saved to flash | System log saved to flash by console(Username: <username>, IP: <ipaddr>) | Informational |
| | Configuration and log saved to flash | Configuration and log saved to flash by console(Username: <username>, IP: <ipaddr>) | Informational |
| | Internal Power failed | Internal Power failed | Critical |
| | Internal Power is recovered | Internal Power is recovered | Critical |
| | Redundant Power failed | Redundant Power failed | Critical |
| | Redundant Power is working | Redundant Power is working | Critical |
| | Side Fan failed | Side Fan failed | Critical |
| | Side Fan recovered | Side Fan recovered | Critical |
| | Back Fan failed | Back Fan failed | Critical |
| | Back Fan recovered | Back Fan 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 |
| up/down-load | Firmware upgraded successfully | Firmware upgraded by console successfully (Username: <username>, IP: <ipaddr>) | Informational |
| | Firmware upgrade was unsuccessful | Firmware upgrade by console was unsuccessful! (Username: <username>, IP: <ipaddr>) | Warning |
| | Configuration successfully downloaded | Configuration successfully downloaded by console(Username: <username>, IP: <ipaddr>) | Informational |
| | Configuration download was unsuccessful | Configuration download by console was unsuccessful! (Username: <username>, IP: <ipaddr>) | Warning |
| | Configuration successfully uploaded | Configuration successfully uploaded | Informational |

| | | | |
|------------------|---------------------------------------|---|---------------|
| | | by console (Username: <username>, IP: <ipaddr>) | |
| | Configuration upload was unsuccessful | Configuration upload by console was unsuccessful! (Username: <username>, IP: <ipaddr>) | Warning |
| | Log message successfully uploaded | Log message successfully uploaded by console (Username: <username>, IP: <ipaddr>) | Informational |
| | Log message upload was unsuccessful | Log message upload by console was unsuccessful! (Username: <username>, IP: <ipaddr>) | Warning |
| | Firmware successfully uploaded | Firmware successfully uploaded by console (Username: <username>, IP: <ipaddr>) | Informational |
| | Firmware upload was unsuccessful | Firmware upload by console was unsuccessful! (Username: <username>, IP: <ipaddr>) | Warning |
| Interface | Port link up | Port <portNum> link up, <link state> | Informational |
| | Port link down | Port <portNum> link down | Informational |
| Console | 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 |
| Web | Successful login through Web | Successful login through Web (Username: <username>, IP: <ipaddr>) | Informational |
| | Login failed through Web | Login failed through Web (Username: <username>, IP: <ipaddr>) | Warning |
| | Logout through Web | Logout through Web (Username: <username>, IP: <ipaddr>,) | Informational |
| | Web session timed out | Web session timed out (Username: <username>, IP: <ipaddr>,) | Informational |
| | Successful login through Web(SSL) | Successful login through Web(SSL) (Username: <username>, IP: <ipaddr>,) | Informational |
| | Login failed through Web(SSL) | Login failed through Web(SSL) (Username: <username>, IP: <ipaddr>,) | Warning |
| | Logout through Web(SSL) | Logout through Web(SSL) (Username: <username>, IP: <ipaddr>,) | Informational |
| | Web(SSL) session timed out | Web(SSL) session timed out (Username: <username>, IP: <ipaddr>,) | Informational |
| Telnet | Successful login through Telnet | Successful login through Telnet (Username: <username>, IP: <ipaddr>,) | Informational |
| | Login failed through Telnet | Login failed through Telnet | Warning |

| | | | |
|-------------|--|--|---------------|
| | | (Username: <username>, IP: <ipaddr>,) | |
| | Logout through Telnet | Logout through Telnet (Username: <username>, IP: <ipaddr>,) | Informational |
| | Telnet session timed out | Telnet session timed out (Username: <username>, IP: <ipaddr>,) | Informational |
| SNMP | SNMP request received with invalid community string | SNMP request received from <ipAddress> 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 |
| | 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 | <p>Spoofting attack</p> <ol style="list-style-type: none"> 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> MAC: <macaddr> Port: <portNum>) | Critical |
| | The DoS attack is blocked | <dos_name> is blocked from (IP: <ipaddr> Port: <portNum>) | Critical |
| SSH | Successful login through SSH | Successful login through SSH (Username: <username>, IP: <ipaddr>) | Informational |
| | Login failed through SSH | Login failed through SSH (Username: <username>, IP: <ipaddr>,) | Warning |
| | Logout through SSH | Logout through SSH (Username: <username>, IP: <ipaddr>) | Informational |
| | SSH session timed out | SSH session timed out (Username: <username>, IP: <ipaddr>) | Informational |
| | 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 authenticated by AAA local method | Successful login through Web from <userIP> authenticated by AAA local method (Username: <username>) | Informational |
| | Login failed through Web authenticated by AAA local method | Login failed failed through Web from <userIP> authenticated by AAA local method (Username: <username>) | Warning |
| | Successful login through Web(SSL) authenticated by AAA local method | Successful login through Web(SSL) from <userIP> authenticated by AAA local method (Username: <username>) | Informational |
| | Login failed through Web(SSL) authenticated by AAA local method | Login failed through Web(SSL) from <userIP> authenticated by AAA local method (Username: <username>) | Warning |
| | Successful login through Telnet authenticated by AAA local method | Successful login through Telnet from <userIP> authenticated by AAA local method (Username: <username>,) | Informational |
| | Login failed through Telnet authenticated by AAA local method | Login failed through Telnet from <userIP> authenticated by AAA local method (Username: <username>) | Warning |
| | Successful login through SSH authenticated by AAA local method | Successful login through SSH from <userIP> authenticated by AAA local method (Username: <username>) | Informational |
| | Login failed through SSH | Login failed through SSH from | Warning |

| | | | |
|--|---|---|---------------|
| | authenticated by AAA local method | <userIP> authenticated by AAA local method (Username: <username>) | |
| | Successful login through Console authenticated by AAA none method | Successful login through Console authenticated by AAA none method (Username: <username>) | Informational |
| | Successful login through Web authenticated by AAA none method | Successful login through Web from <userIP> authenticated by AAA none method (Username: <username>) | Informational |
| | Successful login through Web(SSL) authenticated by AAA none method | Successful login through Web(SSL) from <userIP> authenticated by AAA none method (Username: <username>) | Informational |
| | Successful login through Telnet authenticated by AAA none method | Successful login through Telnet from <userIP> authenticated by AAA none method (Username: <username>) | Informational |
| | Successful login through SSH authenticated by AAA none method | Successful login through SSH from <userIP> authenticated by AAA none (Username: <username>) | Informational |
| | Successful login through Console authenticated by AAA server | Successful login through Console authenticated by AAA server <serverIP> (Username: <username>) | Informational |
| | Login failed through Console authenticated by AAA server | Login failed through Console authenticated by AAA server <serverIP> (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 authenticated by AAA server | Successful login through Web from <userIP> authenticated by AAA server <serverIP> (Username: <username>) | Informational |
| | Login failed through Web authenticated by AAA server | Login failed through Web from <userIP> authenticated by AAA server <serverIP> (Username: <username>) | Warning |
| | Login failed through Web due to AAA server timeout or improper configuration | Login failed through Web from <userIP> due to AAA server timeout or improper configuration (Username: <username>) | Warning |
| | Successful login through Web(SSL) authenticated by AAA server | Successful login through Web(SSL) from <userIP> authenticated by AAA server <serverIP> (Username: <username>) | Informational |
| | Login failed through Web(SSL) authenticated by AAA server | Login failed through Web(SSL) from <userIP> authenticated by AAA server <serverIP> (Username: <username>) | Warning |
| | Login failed through Web(SSL) due to AAA server timeout or improper configuration | Login failed through Web(SSL) from <userIP> due to AAA server timeout or improper configuration (Username: <username>) | Warning |
| | Successful login through Telnet authenticated by AAA server | Successful login through Telnet from <userIP> authenticated by AAA server <serverIP> (Username: <username>) | Informational |
| | Login failed through Telnet authenticated by AAA server | Login failed through Telnet from <userIP> authenticated by AAA server <serverIP> (Username: <username>) | Warning |

| | | | |
|--|---|---|---------------|
| | Login failed through Telnet due to AAA server timeout or improper configuration | Login failed through Telnet from <userIP> due to AAA server timeout or improper configuration (Username: <username>) | Warning |
| | Successful login through SSH authenticated by AAA server | Successful login through SSH from <userIP> authenticated by AAA server <serverIP> (Username: <username>) | Informational |
| | Login failed through SSH authenticated by AAA server | Login failed through SSH from <userIP> authenticated by AAA server <serverIP> (Username: <username>) | Warning |
| | Login failed through SSH due to AAA server timeout or improper configuration | Login failed through SSH from <userIP> 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 authenticated by AAA local_enable method | Successful Enable Admin through Web from <userIP> authenticated by AAA local_enable method (Username: <username>) | Informational |
| | Enable Admin failed through Web authenticated by AAA local_enable method | Enable Admin failed through Web from <userIP> authenticated by AAA local_enable method (Username: <username>) | Warning |
| | Successful Enable Admin through Web(SSL) authenticated by AAA local_enable method | Successful Enable Admin through Web(SSL) from <userIP> authenticated by AAA local_enable method (Username: <username>,) | Informational |
| | Enable Admin failed through Web(SSL) authenticated by AAA local_enable method | Enable Admin failed through Web(SSL) from <userIP> authenticated by AAA local_enable method (Username: <username>) | Warning |
| | Successful Enable Admin through Telnet authenticated by AAA local_enable method | Successful Enable Admin through Telnet from <userIP> authenticated by AAA local_enable method (Username: <username>) | Informational |
| | Enable Admin failed through Telnet authenticated by AAA local_enable method | Enable Admin failed through Telnet from <userIP> authenticated by AAA local_enable method (Username: <username>) | Warning |
| | Successful Enable Admin through SSH authenticated by AAA local_enable method | Successful Enable Admin through SSH from <userIP> authenticated by AAA local (Username: <username>) | Informational |
| | Enable Admin failed through SSH authenticated by AAA local_enable method | Enable Admin failed through <Telnet or Web or SSH> from <userIP> 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 authenticated by AAA none method | Successful Enable Admin through Web from <userIP> authenticated by AAA none method (Username: <username>) | Informational |
| | Successful Enable Admin through Web(SSL) authenticated by AAA none method | Successful Enable Admin through Web(SSL) from <userIP> authenticated by AAA none method (Username: <username>) | Informational |
| | Successful Enable Admin through Telnet authenticated by AAA none method | Successful Enable Admin through Telnet from <userIP> authenticated by AAA none method (Username: <username>) | Informational |
| | Successful Enable Admin through SSH authenticated by AAA none method | Successful Enable Admin through SSH from <userIP> authenticated by AAA none (Username: <username>) | Informational |
| | Successful Enable Admin through Console authenticated by AAA server | Successful Enable Admin through Console authenticated by AAA server <serverIP> (Username: <username>) | Informational |
| | Enable Admin failed through Console authenticated by AAA server | Enable Admin failed through Console authenticated by AAA server <serverIP> (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 Web authenticated by AAA server | Successful Enable Admin through Web from <userIP> authenticated by AAA server <serverIP> (Username: <username>) | Informational |
| | Enable Admin failed through Web authenticated by AAA server | Enable Admin failed through Web from <userIP> authenticated by AAA server <serverIP> (Username: <username>) | Warning |
| | Enable Admin failed through Web due to AAA server timeout or improper configuration | Enable Admin failed through Web from <userIP> due to AAA server timeout or improper configuration (Username: <username>) | Warning |
| | Successful Enable Admin through Web(SSL) authenticated by AAA server | Successful Enable Admin through Web(SSL) from <userIP> authenticated by AAA server <serverIP> (Username: <username>) | Informational |
| | Enable Admin failed through Web(SSL) authenticated by AAA server | Enable Admin failed through Web(SSL) from <userIP> authenticated by AAA server <serverIP> (Username: <username>) | Warning |
| | Enable Admin failed through Web(SSL) due to AAA server timeout or improper configuration | Enable Admin failed through Web(SSL) from <userIP> due to AAA server timeout or improper configuration (Username: <username>) | Warning |
| | Successful Enable Admin through Telnet authenticated by AAA server | Successful Enable Admin through Telnet from <userIP> authenticated by AAA server <serverIP> (Username: <username>) | Informational |
| | Enable Admin failed through Telnet authenticated by AAA server | Enable Admin failed through Telnet from <userIP> authenticated by AAA server <serverIP> (Username: <username>) | Warning |

| | | | |
|--------------------------------|---|---|---------------|
| | | <username>) | |
| | Enable Admin failed through Telnet due to AAA server timeout or improper configuration | Enable Admin failed through Telnet from <userIP> due to AAA server timeout or improper configuration (Username: <username>) | Warning |
| | Successful Enable Admin through SSH authenticated by AAA server | Successful Enable Admin through SSH from <userIP> authenticated by AAA server <serverIP> (Username: <username>) | Informational |
| | Enable Admin failed through SSH authenticated by AAA server | Enable Admin failed through SSH from <userIP> authenticated by AAA server <serverIP> (Username: <username>) | Warning |
| | Enable Admin failed through SSH due to AAA server timeout or improper configuration | Enable Admin failed through SSH from <userIP> due to AAA server timeout or improper configuration (Username: <username>) | Warning |
| | AAA server timed out | AAA server <serverIP> (Protocol: <protocol>) connection failed | Warning |
| | AAA server ACK error | AAA server <serverIP> (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 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 | Management IP address was changed by (Username: <username>,IP:<ipaddr>) | Informational |
| | Password change activity | Password was changed by (Username: <username>,IP:<ipaddr>) | 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 |
| | 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 untag port member. | Radius server <ipaddr> 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> 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> 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> assigned 802.1p default priority:<priority> to port <portNum> (account : <username>) | Informational |
| | 802.1x Authentication failure | 802.1x Authentication failure from (Username: <username>, Port: <portNum>, MAC: <macaddr>) | Warning |
| | 802.1x Authentication success | 802.1x Authentication success [for <reason>] 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 |
| | Can not 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 |
| ARP | Gratuitious ARP detected duplicate IP. | Conflict IP was detected with this device ! (IP: <ipaddr>, MAC: <macaddr>, Port <portNum>, Interface: <ipif_name>). | Warning |
| DHCP | Detect untrusted DHCP server IP address | Detected untrusted DHCP server(IP: <ipaddr>, Port: <portNum>) | Informational |
| COMMAND LOGGING | Command Logging | <username>: execute command "<string>" | Informational |
| MBAC | A host passes the authentication | MAC-based Access Control host login successful (MAC: <macaddr>, port: <[unitID]portNum>, VID: <vid>) | Informational |
| | A host fails to pass the authentication | MAC-based Access Control unauthenticated host(MAC: <macaddr>, Port <[unitID:]portNum>, VID: <vid>) | Critical |
| | A host is aged out | MAC-based Access Control host aged out (MAC: <macaddr>, port: <[unitID]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 |
| | System re-start reason: system fatal error | System re-start reason: system fatal error | Emergent |
| | System re-start reason: CPU exception | System re-start reason: CPU exception | Emergent |

| | | | |
|-------------------|----------------------------|----------------------------------|---------------|
| Diagnostic | Diagnostic: Burn in start | Diagnostic: Burn in start at %S | Informational |
| | Diagnostic: Burn in end | Diagnostic: Burn in end at %S | Informational |
| | Diagnostic: Burn in result | Diagnostic: Burn in result is %S | Informational |

Appendix C Trap Log Entries

This table lists the trap logs found on the Switch.

| Trap Name | Trap Description | OID |
|-----------------------|--|----------------------|
| risingAlarm | The SNMP trap that is generated when an alarm entry crosses its rising threshold and generates an event that is configured for sending SNMP traps. Binding: 1.alarmIndex 2.alarmVariable 3.alarmSampleType 4.alarmValue 5.alarmRisingThreshold | 1.3.6.1.2.1.16.0.1 |
| fallingAlarm | The SNMP trap that is generated when an alarm entry crosses its falling threshold and generates an event that is configured for sending SNMP traps. Binding: 1.alarmIndex 2.alarmVariable 3.alarmSampleType 4.alarmValue 5.alarmFallingThreshold | 1.3.6.1.2.1.16.0.2 |
| LldpRemTablesChange | A lldpRemTablesChange notification is sent when the value of lldpStatsRemTableLastChangeTime changes. It can be utilized by an NMS to trigger LLDP remote systems table maintenance polls. Note that transmission of lldpRemTablesChange notifications are throttled by the agent, as specified by the 'lldpNotificationInterval' object. Binding: 1.lldpStatsRemTablesInserts 2.lldpStatsRemTablesDeletes 3.lldpStatsRemTablesDrops 4.lldpStatsRemTablesAgeouts | 1.0.8802.1.1.2.0.0.1 |
| coldStart | A coldStart trap signifies that the SNMPv2 entity, acting in an agent role, is reinitializing itself and that its configuration may have been altered. | 1.3.6.1.6.3.1.1.5.1 |
| warmStart | A warmStart trap signifies that the SNMPv2 entity, acting in an agent role, is reinitializing itself such that its configuration is unaltered. | 1.3.6.1.6.3.1.1.5.2 |
| authenticationFailure | An authenticationFailure trap signifies that the SNMPv2 entity, acting in an agent role, has received a protocol message that is not properly authenticated. | 1.3.6.1.6.3.1.1.5.5 |
| linkDown | A linkDown trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links is about to enter the down state from some other state (but not from the notPresent | 1.3.6.1.6.3.1.1.5.3 |

| | | |
|---------------------|--|-------------------------|
| | <p>state). This other state is indicated by the included value of ifOperStatus.</p> <p>1.ifIndex 2.ifAdminStatus 3.ifOperStatus</p> | |
| linkUp | <p>A linkUp trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links left the down state and transitioned into some other state (but not into the notPresent state). This other state is indicated by the included value of ifOperStatus.</p> <p>Binding: 1.ifIndex 2.ifAdminStatus 3.ifOperStatus</p> | 1.3.6.1.6.3.1.1.5.4 |
| newRoot | <p>The newRoot trap indicates that the sending agent has become the new root of the Spanning Tree; the trap is sent by a bridge soon after its election as the new root, e.g., upon expiration of the Topology Change Timer, immediately subsequent to its election. Implementation of this trap is optional.</p> | 1.3.6.1.2.1.17.0.1 |
| topologyChange | <p>A topologyChange trap is sent by a bridge when any of its configured ports transitions from the Learning state to the Forwarding state, or from the Forwarding state to the Blocking state. The trap is not sent if a newRoot trap is sent for the same transition. Implementation of this trap is optional.</p> | 1.3.6.1.2.1.17.0.2 |
| dot1agCfmFaultAlarm | <p>A MEP has a persistent defect condition. A notification (fault alarm) is sent to the management entity with the OID of the MEP that has detected the fault. Whenever a MEP has a persistent defect, it may or may not generate a Fault Alarm to warn the system administrator of the problem, as controlled by the MEP Fault Notification Generator State Machine and associated Managed Objects. Only the highest-priority defect, as shown in Table 20-1, is reported in the Fault Alarm. If a defect with a higher priority is raised after a Fault Alarm has been issued, another Fault Alarm is issued. The management entity receiving the notification can identify the system from the network source address of the notification, and can identify the MEP reporting the defect by the indices in the OID of the dot1agCfmMepHighestPrDefect variable in the notification: dot1agCfmMdIndex - Also the index of the MEP's Maintenance Domain table entry (dot1agCfmMdTable). dot1agCfmMaIndex - Also an index (with the MD table index) of the MEP's Maintenance Association network table entry (dot1agCfmMaNetTable), and (with the MD table index and component ID) of the MEP's MA component table entry (dot1agCfmMaCompTable). dot1agCfmMepIdentifier - MEP Identifier and final index into the MEP table (dot1agCfmMepTable).</p> <p>Binding: 1.dot1agCfmMepHighestPrDefect</p> | 1.3.111.2.802.1.1.8.0.1 |

| | | |
|--------------------------------|---|-------------------------------|
| dot3OamThresholdEvent | <p>A dot3OamThresholdEvent notification is sent when a local or remote threshold crossing event is detected. A local threshold crossing event is detected by the local entity, while a remote threshold crossing event is detected by the reception of an Ethernet OAM Event Notification OAMPDU that indicates a threshold event. This notification should not be sent more than once per second. The OAM entity can be derived from extracting the ifIndex from the variable bindings. The objects in the notification correspond to the values in a row instance in the dot3OamEventLogTable. The management entity should periodically check dot3OamEventLogTable to detect any missed events.</p> <p>Binding: 1.dot3OamEventLogTimestamp 2.dot3OamEventLogOui 3.dot3OamEventLogType 4.dot3OamEventLogLocation 5.dot3OamEventLogWindowHi 6.dot3OamEventLogWindowLo 7.dot3OamEventLogThresholdHi 8.dot3OamEventLogThresholdLo 9.dot3OamEventLogValue 10.dot3OamEventLogRunningTotal 11.dot3OamEventLogEventTotal</p> | 1.3.6.1.2.1.158.0.1 |
| swPktStormOccurred | <p>This trap is sent when a packet storm is detected by a packet storm mechanism and a shutdown action is taken.</p> <p>Binding: 1: swPktStormCtrlPortIndex</p> | 1.3.6.1.4.1.171.12.25.5.0.1 |
| swPktStormCleared | <p>The trap is sent when the packet storm is cleared by the packet storm mechanism.</p> <p>Binding: 1: swPktStormCtrlPortIndex</p> | 1.3.6.1.4.1.171.12.25.5.0.2 |
| swPktStormDisablePort | <p>The trap is sent when the port is disabled by the packet storm mechanism.</p> <p>Binding: 1: swPktStormCtrlPortIndex</p> | 1.3.6.1.4.1.171.12.25.5.0.3 |
| swSafeGuardChgToExhausted | <p>This trap indicates System change operation mode from normal to exhausted.</p> <p>Binding: 1: swSafeGuardCurrentStatus</p> | 1.3.6.1.4.1.171.12.19.4.1.0.1 |
| swSafeGuardChgToNormal | <p>This trap indicates System change operation mode from exhausted to normal.</p> <p>Binding: 1: swSafeGuardCurrentStatus</p> | 1.3.6.1.4.1.171.12.19.4.1.0.2 |
| swDoSAttackDetected | <p>This trap is sent when the specific DoS packet is received and trap is enabled.</p> <p>Binding: 1: swDoSCtrlType 2: swDoSNotifyVarIpAddr 3: swDoSNotifyVarPortNumber</p> | 1.3.6.1.4.1.171.12.59.4.0.1 |
| swIpMacBindingViolationTrap | <p>When the IP-MAC Binding trap is enabled, if there's a new MAC that violates the pre-defined port security configuration, a trap will be sent out.</p> <p>Binding: 1: swIpMacBindingPortIndex 2: swIpMacBindingViolationIP 3: swIpMacBindingViolationMac</p> | 1.3.6.1.4.1.171.12.23.5.0.1 |
| swIpMacBindingStopLearningTrap | <p>When the IP-MAC Binding trap is enabled, if the specific port changes from a normal state to a stop_learning state, a trap will be sent out.</p> <p>Binding: 1: swIpMacBindingPortIndex</p> | 1.3.6.1.4.1.171.12.23.5.0.2 |
| swIpMacBindingRecoverLearn | <p>When the IP-MAC Binding trap is enabled, if the</p> | 1.3.6.1.4.1.171.12.23.5.0.3 |

| | | |
|--------------------------------------|---|--|
| ningTrap | specific port changes from a stop_learning state to a normal state, a trap will be sent out. Binding: 1: swlpMacBindingPortIndex | |
| swMacBasedAccessControlLoggedSuccess | The trap is sent when a MAC-based access control host is successfully logged in. Binding: 1.swMacBasedAuthInfoMacIndex 2.swMacBasedAuthInfoPortIndex 3.swMacBasedAuthVID | 1.3.6.1.4.1.171.12.35.11.1.0.1 |
| swMacBasedAccessControlLoggedFail | The trap is sent when a MAC-based access control host login fails. Binding: 1.swMacBasedAuthInfoMacIndex 2.swMacBasedAuthInfoPortIndex 3.swMacBasedAuthVID | 1.3.6.1.4.1.171.12.35.11.1.0.2 |
| swMacBasedAccessControlAgesOut | The trap is sent when a MAC-based access control host ages out. Binding: 1.swMacBasedAuthInfoMacIndex 2.swMacBasedAuthInfoPortIndex 3.swMacBasedAuthVID | 1.3.6.1.4.1.171.12.35.11.1.0.3 |
| swERPSSFDetectedTrap | When the signal fail occurs, a trap will be generated. Binding: 1.swERPSNodeId | 1.3.6.1.4.1.171.12.78.4.0.1 |
| swERPSSFClearedTrap | When the signal fail clears, a trap will be generated. Binding: 1.swERPSNodeId | 1.3.6.1.4.1.171.12.78.4.0.2 |
| swERPSPLOwnerConflictTrap | When a conflict occurs, a trap will be generated. Binding: 1.swERPSNodeId | 1.3.6.1.4.1.171.12.78.4.0.3 |
| swBpduProtectionUnderAttackingTrap | When the BPDU Protection trap is enabled, if the specific port changes from a normal state to an under attack state, a trap will be sent out. Binding: 1.swBpduProtectionPortIndex 2.swBpduProtectionPortMode | 1.3.6.1.4.1.171.12.76.4.0.1 |
| swBpduProtectionRecoveryTrap | When the BPDU Protection trap is enabled, if the specific port changes from an under attack state to a normal state, a trap will be sent out. Binding: 1.swBpduProtectionPortIndex 2.swBpduProtectionRecoveryMethod | 1.3.6.1.4.1.171.12.76.4.0.2 |
| swL2PortSecurityViolationTrap | When the port_security trap is enabled, if there's a new MAC that violates the pre-defined port security configuration, a trap will be sent out. Binding: 1: swL2PortSecurityPortIndex 2: swL2PortSecurityViolationMac | 1.3.6.1.4.1.171.11.133.1.1.2.1 00.1.2.0.2 1.3.6.1.4.1.171.11.133.2.1.2.1 00.1.2.0.2 |
| swL2macNotification | This trap indicates the MAC address variations in the address table. Binding: 1: swL2macNotifyInfo | 1.3.6.1.4.1.171.11.133.1.1.2.1 00.1.2.0.1 1.3.6.1.4.1.171.11.133.2.1.2.1 00.1.2.0.1 |
| swPortLoopOccurred | The trap is sent when a Port loop occurs. Binding: 1.swLoopDetectPortIndex | 1.3.6.1.4.1.171.12.41.10.0.1 |
| swPortLoopRestart | The trap is sent when a Port loop restarts after the interval time. Binding: 1.swLoopDetectPortIndex | 1.3.6.1.4.1.171.12.41.10.0.2 |
| swVlanLoopOccurred | The trap is sent when a Port with a VID loop occurs. Binding: 1.swLoopDetectPortIndex 2.swVlanLoopDetectVID | 1.3.6.1.4.1.171.12.41.10.0.3 |

| | | |
|----------------------------|---|-------------------------------|
| swVlanLoopRestart | The trap is sent when a Port with a VID loop restarts after the interval time. Binding: 1.swLoopDetectPortIndex 2.swVlanLoopDetectVID | 1.3.6.1.4.1.171.12.41.10.0.4 |
| swFilterDetectedTrap | Send trap when illegal DHCP server is detected. The same illegal DHCP server IP address detected is just sent once to the trap receivers within the log ceasing unauthorized duration. Binding: 1.swFilterDetectedIP 2.swFilterDetectedport | 1.3.6.1.4.1.171.12.37.100.0.1 |
| swSingleIPMSColdStart | Commander switch will send swSingleIPMSColdStart notification to indicated host when its Member generate cold start notification. Binding: 1: swSingleIPMSID 2: swSingleIPMSMacAddr | 1.3.6.1.4.1.171.12.8.6.0.11 |
| swSingleIPMSWarmStart | Commander switch will send swSingleIPMSWarmStart notification to indicated host when its Member generate warm start notification. Binding: 1: swSingleIPMSID 2: swSingleIPMSMacAddr | 1.3.6.1.4.1.171.12.8.6.0.12 |
| swSingleIPMSLinkDown | Commander switch will send swSingleIPMSLinkDown notification to indicated host when its Member generate link down notification. Binding: 1: swSingleIPMSID 2: swSingleIPMSMacAddr 3: ifIndex | 1.3.6.1.4.1.171.12.8.6.0.13 |
| swSingleIPMSLinkUp | If Commander switch will send swSingleIPMSLinkUp notification to indicated host when its Member generate link up notification. Binding: 1: swSingleIPMSID 2: swSingleIPMSMacAddr 3: ifIndex | 1.3.6.1.4.1.171.12.8.6.0.14 |
| swSingleIPMSAuthFail | Commander switch will send swSingleIPMSAuthFail notification to indicated host when it Member generate authentication failure notification. Binding: 1: swSingleIPMSID 2: swSingleIPMSMacAddr | 1.3.6.1.4.1.171.12.8.6.0.15 |
| swSingleIPMSnewRoot | Commander switch will send swSingleIPMSnewRoot notification to indicated host when it Member generate new root notification. Binding: 1: swSingleIPMSID 2: swSingleIPMSMacAddr | 1.3.6.1.4.1.171.12.8.6.0.16 |
| swSingleIPMSTopologyChange | Commander switch will send swSingleIPMSTopologyChange notification to indicated host when it Member generate topology change notification. Binding: 1: swSingleIPMSID 2: swSingleIPMSMacAddr | 1.3.6.1.4.1.171.12.8.6.0.17 |
| swDdmAlarmTrap | The trap is sent when any parameter value exceeds the alarm threshold value or recover to normal status depending on the configuration of the trap action. | 1.3.6.1.4.1.171.12.72.4.0.1 |

| | | |
|--------------------------|--|---------------------------------|
| | <p>Binding: 1: swDdmPort 2: swDdmThresholdType 3: swDdmThresholdExceedType 4: swDdmThresholdExceedOrRecover</p> | |
| swDdmWarningTrap | <p>The trap is sent when any parameter value exceeds the warning threshold value or recover to normal status depending on the configuration of the trap action. Binding: 1: swDdmPort 2: swDdmThresholdType 3: swDdmThresholdExceedType 4: swDdmThresholdExceedOrRecover</p> | 1.3.6.1.4.1.171.12.72.4.0.2 |
| agentGratuitousARPTrap | <p>This trap is sent when there is an IP address conflict. Binding: 1: agentGratuitousARPIpAddr 2: agentGratuitousARPMacAddr 3: agentGratuitousARPPortNumber 4: agentGratuitousARPInterfaceName</p> | 1.3.6.1.4.1.171.12.1.7.2.0.5 |
| agentCfgOperCompleteTrap | <p>The trap is sent when the configuration is completely saved, uploaded or downloaded. Binding: 1: unitID 2: agentCfgOperate 3: agentLoginUserName</p> | 1.3.6.1.4.1.171.12.1.7.2.0.9 |
| agentFirmwareUpgrade | <p>This trap is sent when the process of upgrading the firmware via SNMP has finished. Binding: 1: swMultimageVersion</p> | 1.3.6.1.4.1.171.12.1.7.2.0.7 |
| swPowerStatusChg | <p>Power Status change notification. The notification is issued when the swPowerStatus changes in the following cases: lowVoltage -> overCurrent. lowVoltage -> working. lowVoltage -> disconnect. lowVoltage -> connect. overCurrent -> lowVoltage. overCurrent -> working. overCurrent -> disconnect. overCurrent -> connect. working -> lowVoltage. working -> overCurrent. working -> connect. working -> disconnect. fail -> connect. fail -> disconnect. connect -> lowVoltage. connect -> overCurrent. connect -> working. connect -> disconnect. disconnect -> lowVoltage. disconnect -> overCurrent. disconnect -> working. disconnect -> connect.</p> <p>Binding : 1: swPowerUnitIndex 2: swPowerID 3: swPowerStatus</p> | 1.3.6.1.4.1.171.12.11.2.2.2.0.1 |
| swPowerFailure | <p>Power Failure notification. The notification is issued when the swPowerStatus changes in the</p> | 1.3.6.1.4.1.171.12.11.2.2.2.0.2 |

| | | |
|--------------------------|---|---------------------------------|
| | <p>following cases: lowVoltage -> fail. overCurrent -> fail. working -> fail. connect -> fail. disconnect -> fail.</p> <p>Binding : 1: swPowerUnitIndex 2: swPowerID 3: swPowerStatus</p> | |
| swPowerRecover | <p>Power Recover notification. The notification is issued when the swPowerStatus changes in the following cases: Binding : 1: swPowerUnitIndex 2: swPowerID 3: swPowerStatus</p> | 1.3.6.1.4.1.171.12.11.2.2.2.0.3 |
| swFanFailure | <p>Fan Failure notification. Binding : 1: swFanUnitIndex 2: swFanID</p> | 1.3.6.1.4.1.171.12.11.2.2.3.0.1 |
| swFanRecover | <p>Fan Recover notification. Binding : 1: swFanUnitIndex 2: swFanID</p> | 1.3.6.1.4.1.171.12.11.2.2.3.0.2 |
| swHighTemperature | <p>High Temperature notification Binding : 1: swTemperatureUnitIndex 2: swTemperSensorID 3: swTemperatureCurrent</p> | 1.3.6.1.4.1.171.12.11.2.2.4.0.1 |
| swHighTemperatureRecover | <p>High Temperature notification Binding : 1: swTemperatureUnitIndex 2: swTemperSensorID 3: swTemperatureCurrent</p> | 1.3.6.1.4.1.171.12.11.2.2.4.0.2 |
| swLowTemperature | <p>Low Temperature notification Binding : 1: swTemperatureUnitIndex 2: swTemperSensorID 3: swTemperatureCurrent</p> | 1.3.6.1.4.1.171.12.11.2.2.4.0.3 |
| swLowTemperatureRecover | <p>Low Temperature notification Binding : 1: swTemperatureUnitIndex 2: swTemperSensorID 3: swTemperatureCurrent</p> | 1.3.6.1.4.1.171.12.11.2.2.4.0.4 |

Appendix D RADIUS Attributes Assignment

The RADIUS Attributes Assignment on the DGS-3000 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 termination). | 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 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 | Required |

| | | | |
|--|--|--|--|
| | | 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; | |
|--|--|--|--|

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**), 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.