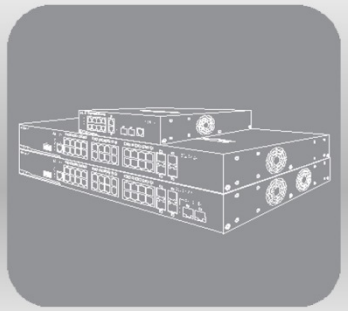
D-Link®
Building Networks for People



CLI Reference Guide

Product Model: DGS-3000-28SC
Layer 2 Managed Stackable Gigabit Switch
Release 5.00

Table of Contents

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:

- 9600 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-3000-28SC Gigabit Ethernet Switch
                           Command Line Interface

                          Firmware: Build 5.00.020
          Copyright(C) 2014 D-Link Corporation. All rights reserved.
UserName:
PassWord:

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

There is no initial username or password. Just press the **Enter** key twice to display the CLI input cursor – **DGS-3000-28SC: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                                          V5.00.003
-------------------------------------------------------------------------------

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

  MAC Address   : B0-C5-54-30-00-A0
  H/W Version   : A1

  Please Wait, Loading V5.00.020 Runtime Image ..............  100 %
  UART init .................................................  100 %
  Starting runtime image
  Device Discovery ..........................................  100 %
  Configuration init ........................................  100 %
```

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-3000-28SC: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-3000-28SC: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.

```
DGS-3000-28SC:admin# ?
Command:?
..
?
cable_diag ports
cd
cfm linktrace
cfm lock md
cfm loopback
change drive
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 historical_counters ports
clear igmp_snooping data_driven_group
clear igmp_snooping statistics counter
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-3000-28SC:admin#config account
Command: config account
Next possible completions:
<username>

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

DGS-3000-28SC: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-3000-28SC: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-3000-28SC: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-3000-28SC:admin# show
Command: show
Next possible completions:
802.1p              802.1x              aaa                 access_profile
account             accounting          acct_client         address_binding
arp_spoofing_prevention                 arpentry            asymmetric_vlan
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     broadcast_ping_reply                    cfm
command             command_history     community_encryption
config              control_pkt         cpu                 cpu_filter
cpu_protect         current_config      ddm                 device_status
dhcp_local_relay    dhcp_relay          dhcpv6_local_relay
dhcpv6_relay        dnsr                dos_prevention
dot1v_protocol_group                    dscp                duld
eee                 egress_access_profile                   egress_flow_meter
environment         erps                error               ethernet_oam
fdb                 filter              flow_meter          gratuitous_arp
greeting_message    gvrp                hol_prevention      host_name
igmp                igmp_proxy          igmp_snooping       ipfdb
ipif                ipif_ipv6_link_local_auto               iproute
ipv6                ipv6route           jumbo_frame         l2protocol_tunnel
lacp_port           led                 limited_multicast_addr
link_aggregation    lldp                lldp_med            local_loopback
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_proxy           mld_snooping        multicast           multicast_fdb
name_server         nlb                 packet              password_recovery
per_queue           port                port_group          port_security
port_security_entry                     port_vlan           ports
power_saving        pppoe               private_vlan        pvid
qinq                radius              rcp                 rmon
router_ports        rspan               safeguard_engine    scheduling
scheduling_mechanism                    serial_port         session
sflow               sftp                sim                 snmp
sntp                sred                ssh                 ssl
stack_device        stack_information   stacking_mode
storage_media_info                      stp                 surveillance_vlan
switch              syslog              system_severity     tacacs
tech_support        telnet              terminal            tftp
time                time_range          traffic
traffic_segmentation                    trap                trusted_host
utilization         vlan                vlan_counter        vlan_translation
vlan_translation_profile                vlan_trunk          voice_vlan
wac

DGS-3000-28SC: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 < >	Encloses a variable or value. Users must specify the variable or value. For example, in the command **create ipif <ipif_name 12> {<network_address>} <vlan_name 32> {secondary | state [enable | disable] | proxy_arp [enable | disable] {local [enable | disable]}}** 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.
square brackets [ ]	Encloses a required value or list of required arguments. Only one value or argument must be specified. For example, in the command **create account [admin | operator | power_user | user] <username 15> {encrypt [plain_text | sha_1] <password>}** users must specify either the admin-level, power-user-level or user-level account when entering the command. DO NOT TYPE THE SQUARE BRACKETS.
vertical bar |	Separates mutually exclusive items in a list, one of which must be entered. For example, in the command **create ipif <ipif_name 12> {<network_address>} <vlan_name 32> {secondary | state [enable | disable] | proxy_arp [enable | disable] {local [enable | disable]}}** users must specify either the community or trap receiver in the command. DO NOT TYPE THE VERTICAL BAR.
braces { }	Encloses an optional value or a list of optional arguments. One or more values or arguments can be specified. For example, in the command **reset {[config | system]} {force_agree}** users may choose to reset the configuration or the system in the command. DO NOT TYPE THE BRACES.
parentheses ( )	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 command **config bpdu_protection ports [<portlist> | all] {state [enable | disable] | mode [drop | block | shutdown]}(1)** users have the option to specify to configure the state or the mode. The **(1)** following the set of braces indicates at least one argument or value within the braces must be specified. DO NOT TYPE THE PARENTHESES.
ipif <ipif_name 12> **metric <value 1-31>**	**12** means the maximum length of the IP interface name. **1-31** means the legal range of the metric value.

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 switch
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 {capability_advertised {10_half | 10_full | 100_half | 100_full | 1000_full}} | 10_half | 10_full | 100_half | 100_full | 1000_full {[master | slave]} | 10g_full] | auto_negotiation [restart_an | remote_fault_advertised [disable | offline | link_fault | auto_negotiation_error]] | flow_control [enable | disable] | learning [enable | disable] | state [enable | disable] | mdix [auto | normal | cross] | [description <desc 1-32> | clear_description] | auto_speed_downgrade [enable | disable]}(1)
show ports {<portlist>} {[description | err_disabled | auto_negotiation | details | media_type]}
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 {unit<unit_id>}<pathname>boot_up

2-1 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-3000-28SC:admin#show switch
Command: show switch

Device Type                : DGS-3000-28SC 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 5.00.003
Firmware Version           : Build 5.00.020
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 q Quit SPACE n Next Page ENTER Next Entry a All
```

2-2 show session

Description

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

Format

show session

Parameters

None.

Restrictions

Only administrators and Operators can issue this command.

Example

To display the session entries:

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

ID  Live Time    From                                    Level Name
 --- ------------ --------------------------------------- ----- ---------------
0    00:01:46.360 10.90.90.10                              puser puser
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
```

2-3 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-3000-28SC:admin#show serial_port
Command: show serial_port

 Baud Rate     : 9600
 Data Bits     : 8
 Parity Bits   : None
 Stop Bits     : 1
 Auto-Logout   : 10 mins

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

2-4 config serial_port

Description

This command is used to configure the serial bit rate used to communicate with the management host and the idle connection auto logout time.

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 9600. **9600** - Specify the serial bit rate to be 9600. **19200** - Specify the serial bit rate to be 19200. **38400** - Specify the serial bit rate to be 38400. **115200** - Specify 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 the baud rate:

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

Success.

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

2-5 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 the “show” command output reaches the end of the page:

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

Success.

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

2-6 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 the “show” command output reaches the end of the page:

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

Success.

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

2-7 login

Description

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

Format

login

Parameters

None.

Restrictions

None.

Example

To login to the Switch using the “dlink” username:

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

UserName:dlink
PassWord:****

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

2-8 logout

Description

This command is used to logout from the command prompt.

Format

logout

Parameters

None.

Restrictions

None.

Example

To logout from the current user:

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


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

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

                           Firmware: Build 5.00.020
           Copyright(C) 2014 D-Link Corporation. All rights reserved.
UserName:
```

2-9 ?

Description

This command is used to display a description of a specific command or general command.

Format

?

Parameters

None.

Restrictions

None.

Example

To get a description for the“ping” command usage:

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

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

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

2-10 clear

Description

This command is used to clear the screen.

Format

clear

Parameters

None.

Restrictions

None.

Example

To clear the screen:

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



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

2-11 show command_history

Description

This command is used to display the command history.

Format

show command_history

Parameters

None.

Restrictions

None.

Example

To display the command history:

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

2-12 config command_history

Description

This command is used to configure the number of commands that the Switch can recall. The Switch “remembers” 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 lines shown in the command history:

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

Success.

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

2-13 config greeting_message

Description

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

Format

config greeting_message {default}

Parameters

default - (Optional) Add 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-3000-28SC:admin#config greeting_message
Command: config greeting_message

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

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

                           Firmware: Build 5.00.020
          Copyright(C) 2014 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
--------------------------------------------------------------------------------
```

2-14 show greeting_message

Description

This command is used to display a greeting message.

Format

show greeting_message

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To display the greeting message:

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

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

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

                            Firmware: Build 5.00.020
          Copyright(C) 2014 D-Link Corporation. All rights reserved.
================================================================================

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

2-15 config command_prompt

Description

This command is used to modify the command prompt.

When users issue the “reset” command, the current command prompt will remain intact. 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 - Specify the login username as the command prompt.
default - Specify 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-3000-28SC:admin#config command_prompt Prompt#
Command: config command_prompt Prompt#

Success.

Prompt#:admin#
```

2-16 config terminal width

Description

This command is used to set the current terminal width.

The usage is described as below:

1. Configure the terminal width to 120px. Enter the command "save" to apply this. Once you have logged out and logged back in, the terminal width will be 120 pixels.
2. If you didn't save the configuration or a new/another user logs into the terminal, the terminal width remains at its default value.
3. If you are running two CLI sessions concurrently, the first terminal configured to use 120px is saved will not effect the other terminal unless you logout and relogin to that terminal.

Format

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

Parameters

default - Specify the default terminal width setting. The default value is 80.
<value 80-200> - Enter the configured terminal width. The width is between 80 and 200 characters.

Restrictions

None.

Example

To configure the current terminal width:

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

Success.

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

2-17 show terminal width

Description

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

Format

show terminal width

Parameters

None.

Restrictions

None.

Example

To display the current terminal width configuration:

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

Global terminal width     : 80
Current terminal width    : 80

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

2-18 config ports

Description

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

Format

config ports [<portlist> | all] {medium_type [fiber | copper]} {speed [auto {capability_advertised {10_half | 10_full | 100_half | 100_full | 1000_full}} | 10_half | 10_full | 100_half | 100_full | 1000_full {[master | slave]} | 10g_full] | auto_negotiation [restart_an | remote_fault_advertised [disable | offline | link_fault | auto_negotiation_error]] | flow_control [enable | disable] | learning [enable | disable] | state [enable | disable] | mdix [auto | normal | cross] | [description <desc 1-32> | clear_description] | auto_speed_downgrade [enable | disable]}(1)

Parameters

<portlist> - Enter a range of ports to be configured.

all - Specify all ports in the system, you may use the “all” parameter command.

medium_type - (Optional) Specify the medium type for the combo ports. This parameter is optional. For non combo ports, the user doesn't need to specify medium_type in the command.
- **fiber** - Specify the fiber port.
- **copper** - Specify the copper port

speed - Specify the port speed.
- **auto** - Specify the port auto negotiation speed.
  - **capability_advertised** - (Optional) Specify that the capability will be advertised.
    - **10_half** - (Optional) Specify the port speed to 10_half.
    - **10_full** - (Optional) Specify the port speed to 10_full.
    - **100_half** - (Optional) Specify the port speed to 100_half.
    - **100_full** - (Optional) Specify the port speed to 100_full.
    - **1000_full** - (Optional) Specify the port speed to 1000_full. Using master or slave mode in this mode is optional.
- **10_half** - Specify the port speed to 10_half.
- **10_full** - Specify the port speed to 10_full.
- **100_half** - Specify the port speed to 100_half.
- **100_full** - Specify the port speed to 100_full.
- **1000_full** - Specify the 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** - (Optional) Specify that the port(s) will be set to master. **slave** - (Optional) Specify that the port(s) will be set to slave. **10g_full** - Specify the port speed to 10g_full.
auto_negotiation - Specify that the auto-negotiation option will be configured. **restart_an** - Specify to restart the auto-negotiation process. **remote_fault_advertised** - Specify that the remote fault advertisement option will be configured. **disable** - Specify to disable remote fault advertisement. **offline** - Specify that a local device may indicate Offline prior to powering off, running transmitter tests, or removing the local device from the active configuration. If it is set and detected offline, it will advertise at the next auto-negotiation. It interacted for 1000Mbps MAUs. **link_fault** - Specify that if set and local device was detected, a Link_Failure condition indicated by the loss of synchronization, will advertise at the next auto-negotiation. It interacted for 1000Mbps MAUs. **auto_negotiation_error** - Specify the resolution which precludes operation between a local device and link partner advertised at the next auto-negotiation. It interacted for 1000Mbps MAUs.
flow_control - Turns on or turns off the flow control on one or more ports by enabling or disabling this function. **enable** - Specify that the flow control option will be enabled. **disable** - Specify that the flow control option will be disabled.
learning - Turns on or turns off the MAC address learning on one or more ports. **enable** - Specify that the learning option will be enabled. **disable** - Specify that the learning option will be disabled.
state - Enables or disables the specified port. If the specificed ports are in error-disabled status, configure their state to enable will recover these ports from disabled to enable state. **enable** - Specify that the port state will be enabled. **disable** - Specify that the port state will be disabled.
mdix - 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** - Specify that the MDIX mode for the port will be set to auto. **normal** - Specify that the MDIX mode for the port will be set to normal. **cross** - Specify that the MDIX mode for the port will be set to cross.
description - Specify 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) Specify that the description field will be cleared.
auto_speed_downgrade - Specify to enable or disable the option to automatically downgrade the advertised speed. This setting has no effect when the port is working in the forced mode. **enable** - Specify to enable the option to automatically downgrade the advertised speed. **disable** - Specify to disable the option to automatically downgrade the advertised speed.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the Ethernet ports:

```
DGS-3000-28SC:admin# config ports 1-3 speed 10_full learning enable state
enable flow_control enable
Command: config ports 1-3 speed 10_full learning enable state enable
flow_control enable


Success.


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

2-19 show ports

Description

This command is used to display the current configuration of a range of ports. No parameter will show all ports.

Format

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

Parameters

<portlist> - (Optional) Enter a range of ports to be displayed.
description - (Optional) Specify to display the port description.
err_disabled - (Optional)Specify to display disabled information.
auto_negotiation - (Optional) Specify to display detailed auto-negotiation information.
details - (Optional) Specify if port information is included in the display.
media_type - (Optional) Displays SFP information.

Restrictions

None.

Example

To display the port details:

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

Port : 1
--------------------
Port Status                 : Link Up
Description                 :
HardWare Type               : Gigabits Ethernet
MAC Address                 : B0-C5-54-30-00-A1
Bandwidth                   : 100000Kbit
Auto-Negotiation            : Enabled
Duplex Mode                 : Full Duplex
Flow Control                : Disabled
MDI                         : Cross
Address Learning            : Enabled
Last Clear of Counter       : 3 hours 9 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
```

2-20 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-3000-28SC:admin#enable telnet 23
Command: enable telnet 23

Success.

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

2-21 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-3000-28SC:admin#disable telnet
Command: disable telnet

Success.

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

2-22 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-3000-28SC:admin#enable web 80
Command: enable web 80

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

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

2-23 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-3000-28SC:admin#disable web
Command: disable web

Success.

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

2-24 reboot

Description

This command is used to restart the Switch.

Format

reboot {force_agree}

Parameters

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

Restrictions

Only Administrators can issue this command.

Example

To reboot the Switch:

```
DGS-3000-28SC:admin#reboot
Command: reboot

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

2-25 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 immediatedly without further confirmation.

Restrictions

Only Administrators can issue this command.

Example

To reset the Switch:

```
DGS-3000-28SC: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...
```

2-26 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 {unit <unit_id>} <pathname>boot_up

Parameters

unit - Enter the firmware file unit from the device. **<unit_id>** - Enter the unit ID.
<pathname> - Enter the image pathname.
boot_up - Specify the firmware as the boot-up firmware.

Restrictions

Only Administrators can issue this command.

Example

To configure c:/ firmware.had as the boot-up image:

```
DGS-3000-28SC:admin#config firmware image c:/firmware.had boot_up
Command: config firmware image c:/firmware.had boot_up

Success.

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

Chapter 3 802.1Q VLAN Command List

create vlan <vlan_name 32> tag <vlanid 2-4094> {type [1q_vlan | private_vlan]} {advertisement}
create vlan vlanid <vidlist> {type [1q_vlan | private_vlan]} {advertisement}
delete vlan <vlan_name 32>
delete vlan vlanid <vidlist>
config vlan <vlan_name 32> {[add [tagged | untagged | forbidden] | delete] <portlist> | advertisement [enable | disable]}(1)
config vlan vlanid <vidlist> {[add [tagged | untagged | forbidden] | delete] <portlist> | advertisement [enable | disable] | name <vlan_name 32>}(1)
config port_vlan [<portlist> | all] {gvrp_state [enable | disable] | ingress_checking [enable | disable] | acceptable_frame [tagged_only | admit_all] | pvid <vlanid 1-4094>}(1)
show vlan {<vlan_name 32>}
show vlan ports {<portlist>}
show vlan vlanid <vidlist>
show port_vlan {<portlist>}
enable pvid auto_assign
disable pvid auto_assign
show pvid auto_assign
config gvrp [timer [join | leave | leave all] <value 100-100000> | nni_bpdu_add [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) Specify the type of VLAN here. **1q_vlan** - (Optional) Specify that the type of VLAN used is based on the 802.1Q standard. **private_vlan** - (Optional) Specify that the private VLAN type will be used.

advertisement - (Optional) Specify 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-3000-28SC:admin#create vlan p1 tag 2 type private_vlan advertisement
Command: create vlan p1 tag 2 type private_vlan advertisement

Success.

DGS-3000-28SC: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) Specify the type of VLAN to be created. **1q_vlan** - (Optional) Specify that the VLAN created will be a 1Q VLAN. **private_vlan** - (Optional) Specify that the private VLAN type will be used.
advertisement - (Optional) Specify 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-3000-28SC:admin#create vlan vlanid 10-30
Command: create vlan vlanid 10-30

Success.

DGS-3000-28SC: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_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-3000-28SC:admin#delete vlan v1
Command: delete vlan v1

Success.

DGS-3000-28SC: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

<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-3000-28SC:admin#delete vlan vlanid 10-30
Command: delete vlan vlanid 10-30

Success.

DGS-3000-28SC: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) Specify to add tagged, untagged or forbidden ports to the VLAN. **tagged** - Specify the additional ports as tagged. **untagged** - Specify the additional ports as untagged. **forbidden** - Specify the additional ports as forbidden.
delete - (Optional) Specify to delete ports from the VLAN.
<portlist> - (Optional) Enter the list of ports used for the configuration here.
advertisement - (Optional) Specify the GVRP state of this VLAN. **enable** - Specify to enable advertisement for this VLAN. **disable** - Specify 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-3000-28SC:admin#config vlan v2 add tagged 4-8
Command: config vlan v2 add tagged 4-8

Success.

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

3-6 config vlan vlanid

Description

This command is used 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) Specify to add tagged, untagged or forbidden ports to the VLAN. **tagged** - Specify the additional ports as tagged. **untagged** - Specify the additional ports as untagged. **forbidden** - Specify the additional ports as forbidden.
delete - (Optional) Specify to delete ports from the VLAN.
<portlist> - (Optional) Enter the list of ports used for the configuration here.
advertisement - (Optional) Specify the GVRP state of this VLAN. **enable** - Specify to enable advertisement for this VLAN. **disable** - Specify 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-3000-28SC:admin#config vlan vlanid 10-20 add tagged 4-8
Command: config vlan vlanid 10-20 add tagged 4-8

Success.

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

3-7 config port_vlan

Description

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

Format

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

Parameters

<portlist> - Enter a range of ports for which you want ingress checking. The port list is specified by listing the beginning port number on the Switch, separated by a colon. Then highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. **all** - Specify all ports for ingress checking.
gvrp_state - (Optional) Enables or disables the GVRP for the ports specified in the port list. **enable** - Specify that GVRP for the specified ports will be enabled. **disable** - Specify that GVRP for the specified ports will be disabled.
ingress_checking - (Optional) Enables or disables ingress checking for the specified portlist. **enable** - Specify that ingress checking will be enabled for the specified portlist. **disable** - Specify 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) Specify 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-3000-28SC:admin#config port_vlan 1-5 gvrp_state enable ingress_checking
enable acceptable_frame tagged_only pvid 2
Command: config port_vlan 1-5 gvrp_state enable ingress_checking enable
acceptable_frame tagged_only pvid 2


Success.


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

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

DGS-3000-28SC: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-3000-28SC: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-3000-28SC: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) Enter a range of ports to be displayed.
If no parameter is specified, system will display all ports gvrp information.

Restrictions

None.

Example

To display 802.1Q port setting:

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

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

3-12 enable pvid auto assign

Description

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

If “Auto-assign PVID” is enabled, PVID will be possibly changed by PVID or VLAN configuration. When 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-3000-28SC:admin#enable pvid auto_assign
Command: enable pvid auto_assign

Success.

DGS-3000-28SC: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-3000-28SC:admin#disable pvid auto_assign
Command: disable pvid auto_assign

Success.

DGS-3000-28SC: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-3000-28SC:admin#show pvid auto_assign
Command: show pvid auto_assign

PVID Auto-assignment: Enabled

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

3-15 config gvrp

Description

This command is used to 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 | leave | leave all] <value 100-100000> | nni_bpdu_addr [dot1d | dot1ad]]

Parameters

timer - Specify that the GVRP timer parameter will be configured.
join - (Optional) Specify the Join time will be set.
leave - (Optional) Specify the Leave time will be set.
leave all - (Optional) Specify 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 - Used 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 a user defined multicast address. **dot1d** - Specify that the NNI BPDU protocol address value will be set to Dot1d. **dot1ad** - Specify 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-3000-28SC:admin#config gvrp timer join 200
Command: config gvrp timer join 200

Success.

DGS-3000-28SC: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-3000-28SC: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-3000-28SC: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-3000-28SC:admin#enable gvrp
Command: enable gvrp

Success.

DGS-3000-28SC: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-3000-28SC:admin#disable gvrp
Command: disable gvrp

Success.

DGS-3000-28SC: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> - Enter the name of the private VLAN.
vid - Specify 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 - Specify that a secondary VLAN will be added to the private VLAN. **isolated** - Specify the secondary VLAN as isolated VLAN. **community** - Specify the secondary VLAN as community VLAN.
remove - Specify that a secondary VLAN will be removed from the private VLAN.
<vlan_name 32> - Enter the secondary VLAN name used. This name can be up to 32 characters long.
vlanid - A range of secondary 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-3000-28SC:admin#config private_vlan p1 add community vlanid 3
Command: config private_vlan p1 add community vlanid 3

Success.

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

3-20 show private_vlan

Description

This command is used to show the private VLAN information.

Format

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

Parameters

<vlan_name 32> - (Optional) Enter the name of the private VLAN or its secondary VLAN. This

name can be up to 32 characters long.
vlanid - (Optional) Specify 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-3000-28SC:admin#show private_vlan
Command: show private_vlan

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


 Total Entries: 1


DGS-3000-28SC: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 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]
config 802.1x trap 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-3000-28SC:admin#enable 802.1x
Command: enable 802.1x

Success.

DGS-3000-28SC: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-3000-28SC:admin#disable 802.1x
Command: disable 802.1x

Success.

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

Success.

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

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

 Total Entries:1


DGS-3000-28SC: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 - Specify the authentication protocol as local.
radius_eap - Specify 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-3000-28SC:admin#config 802.1x auth_protocol radius_eap
Command: config 802.1x auth_protocol radius_eap

Success.

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

Success.

DGS-3000-28SC: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 - Specify that all the ports will be used.
enable - Specify to enable forwarding EAPOL PDU receive on the ports.
disable - Specify to disable forwarding EAPOL PDU receive on the ports.

Restrictions

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

Example

To configure 802.1X fwd_pdu for ports:

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

Success.

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

4-9 config 802.1x authorization attributes radius

Description

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

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

Format

config 802.1x authorization attributes radius [enable | disable]

Parameters

enable - Specify to enable the authorization attributes. The authorization attributes (for example VLAN, 802.1p default priority, and ACL) assigned by the RADUIS server will be accepted.

This is the default.
disable - Specify 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-3000-28SC:admin#config 802.1x authorization attributes radius disable
Command: config 802.1x authorization attributes radius disable

Success.

DGS-3000-28SC: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) Specify to display 802.1X authentication state machine of some or all ports.
auth_configuration - (Optional) Specify to display 802.1X configurations of some or all ports.
port - (Optional) Specify 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-3000-28SC: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

<portlist> - Enter the list of ports used for the configuration here.
all - Specify all ports to be configured.
authenticator - Specify 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-3000-28SC:admin#config 802.1x capability ports 1-10 authenticator
Command: config 802.1x capability ports 1-10 authenticator

Success.

DGS-3000-28SC: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 - Specify 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-3000-28SC:admin#config 802.1x max_users 200
Command: config 802.1x max_users 200

Success.

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

4-13 config 802.1x auth_parameter ports

Description

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

Format

config 802.1x auth_parameter ports [<portlist> | all] [default | {direction [both | in] | port_control [force_unauth | auto | force_auth] | quiet_period <sec 0-65535> | tx_period <sec 1-65535> | supp_timeout <sec 1-65535> | server_timeout <sec 1-65535> | max_req

<value 1-10> | reauth_period <sec 1-65535> | max_users [<value 1-448> | no_limit] | enable_reauth [enable | disable]}(1)]

Parameters

<portlist> - Enter the list of ports used for the configuration here.
all - Specify that all the ports will be used.
default - Sets all parameter to be default value.
direction - Sets the direction of access control. **both** - For bidirectional access control. **in** - For unidirectional access control.
port_control - 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 - 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 - 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 - 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 - 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 - 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 - 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) Specify 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** - Specify that no limit is enforced on the maximum users used.
enable_reauth - You can enable or disable the re-authentication mechanism for a specific port. **enable** - Specify to enable the re-authentication mechanism for a specific port. **disable** - Specify 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-3000-28SC:admin#config 802.1x auth_parameter ports 1-20 direction both
Command: config 802.1x auth_parameter ports 1-20 direction both

Success.

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

4-14 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 - Specify the authentication as the port-based mode. **<portlist>** - Enter the list of ports used for the configuration here. **all** - Specify that all ports will be used.
mac_based ports - Specify the authentication as the MAC-based mode. **<portlist>** - Enter the list of ports used for the configuration here. **all** - Specify that all ports will be used.
mac_address - (Optional) Specify 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-3000-28SC:admin#config 802.1x init port_based ports all
Command: config 802.1x init port_based ports all

Success.

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

4-15 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 - Specify the authentication as the port-based mode. **<portlist>** - Enter the list of ports used for the configuration here. **all** - Specify that all ports will be used.
mac_based ports - Specify the authentication as the MAC-based mode. **<portlist>** - Enter the list of ports used for the configuration here. **all** - Specify that all ports will be used.
mac_address - (Optional) Specify 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-3000-28SC:admin#config 802.1x reauth port_based ports all
Command: config 802.1x reauth port_based ports all

Success.

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

4-16 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> - Enter 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-3000-28SC:admin#create 802.1x guest_vlan guestVLAN
Command: create 802.1x guest_vlan guestVLAN

Success.

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

4-17 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-3000-28SC:admin#delete 802.1x guest_vlan guestVLAN
Command: delete 802.1x guest_vlan guestVLAN

Success.

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

4-18 config 802.1x guest_vlan ports

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

<portlist> - Enter the list of ports used for the configuration here.
all - Specify that all the port will be included in this configuration.
state - Specify the guest VLAN port state of the configured ports. **enable** - Specify to join the guest VLAN. **disable** - Specify 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-3000-28SC: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-3000-28SC:admin#
```

4-19 config 802.1x trap state

Description

This command is used to enable or disable the sending of 802.1X traps.

Format

config 802.1x trap state [enable | disable]

Parameters

enable - Specify to enable the sending of 802.1x traps.
disable - Specify to disable the sending of 802.1x traps.

Restrictions

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

Example

This example shows how to enable the trap state for 802.1x.

```
DGS-3000-28SC:admin# config 802.1x trap state enable
Command: config 802.1x trap state enable

Success.

DGS-3000-28SC: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-3000-28SC: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-3000-28SC: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) Specify 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-3000-28SC:admin#show auth_statistics ports 1
Command: show auth_statistics ports 1

MAC Address : 00—01-02-03-04-05
 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) Specify 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-3000-28SC:admin#show auth_diagnostics ports 1
Command: show auth_diagnostics ports 1

Mac Address : 00-01-02-03-04-05
 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) Specify 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-3000-28SC:admin#show auth_session_statistics ports 1
Command: show auth_session_statistics ports 1

Mac Address : 00-01-02-03-04-05
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 authen_policy
disable authen_policy
enable authen_policy_encryption
disable authen_policy_encryption
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}(1)
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}(1)
delete authen_enable method_list_name <string 15>
show authen_enable [default | method_list_name <string 15> | all]
config authen application [console | telnet | ssh | http | all] [login | enable] [default | method_list_name <string 15>]
show authen application
create authen server_group <string 15>
config authen server_group [tacacs | xtacacs | tacacs+ | radius | <string 15>] [add | delete] server_host <ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius]
delete authen server_group <string 15>
show authen server_group {<string 15>}
create authen server_host <ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius] {port <int 1-65535> | [key [<key_string 254> | none] | encryption_key <key_string 344>] | timeout <int 1-255> | retransmit <int 1-20>}
config authen server_host <ipaddr> protocol [tacacs | xtacacs | tacacs+| radius] {port <int 1-65535> | [key [<key_string 254> | none] | encryption_key <key_string 344>] | timeout <int 1-255> | retransmit <int 1-20>}
delete authen server_host <ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius]
show authen server_host
config authen parameter response_timeout <int 0-255>
config authen parameter attempt <int 1-255>
show authen parameter
enable admin
config admin local_enable {encrypt [plain_text | sha_1] <password>}
config aaa server_group [tacacs | xtacacs | tacacs+ | radius | group_name <string 15>] [add | de lete] server_host <ipaddr> protocol [tacacs | xtacacs | tacacs+| radius]
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
show aaa server_group {<string15>}
delete aaa server_group <string15>
show aaa server_host
delete aaa server_host <ipaddr> protocol [tacacs | xtacacs | tacacs+| radius]
create tacacs server_host <ipaddr> {port <int 1-65535> | timeout <int 1-255> | retransmit <int 1-20>}
create radius server_host <ipaddr> {auth_port <int 1-65535> | acct_port <int 1-65535> | [key [<key_string 254> | none] | encryption_key <key_string 344>] | timeout <int 1-255> | retransmit <int 1-20>}
config radius server_host <ipaddr> {auth_port <int 1-65535> | acct_port <int 1-65535> | [key [<key_string 254> | none] | encryption_key <key_string 344>] | timeout <int 1-255> | retransmit <int 1-20>}
config radius source_ipif [<ipif_name 12> {<ipaddr> | <ipv6addr>} | none]
show radius source_ipif
config tacacs server_host <ipaddr> {port <int 1-65535> | timeout <int 1-255> | retransmit <int 1-20>}
config tacacs source_ipif [<ipif_name 12> {<ipaddr>} | none]
show tacacs source_ipif
config tacacs+ server_host <ipaddr> {port <int 1-65535> | [key [<key_string 254> | none] | encryption_key <key_string 344>] | timeout <int 1-255>}
config xtacacs server_host <ipaddr> {port <int 1-65535> | timeout <int 1-255> | retransmit <int 1-20>}
create xtacacs server_host <ipaddr> {port <int 1-65535> | timeout <int 1-255> | retransmit <int 1-20>}
create tacacs+ server_host <ipaddr> {port <int 1-65535> | [key [<key_string 254> | none] | encryption_key <key_string 344>] | timeout <int 1-255>}
create aaa server_group <string 15>
enable aaa_server_password_encryption
disable aaa_server_password_encryption

5-1 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-3000-28SC:admin#enable authen_policy
Command: enable authen_policy

Success.

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

5-2 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-3000-28SC:admin#disable authen_policy
Command: disable authen_policy

Success.

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

5-3 enable authen_policy_encryption

Description

This command is used to enable the authentication policy encryption. When enabled, TACACS+ and RADIUS key will be in the encrypted form.

Format

enable authen_policy_encryption

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To enable the authentication policy encryption:

```
DGS-3000-28SC:admin#enable authen_policy_encryption
Command: enable authen_policy_encryption

Success.

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

5-4 disable authen_policy_encryption

Description

This command is used to disable the authentication policy encryption. When disabled, TACACS+ and RADIUS key will be in the plain text form.

Format

disable authen_policy_encryption

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To disable the authentication policy encryption:

```
DGS-3000-28SC:admin#disable authen_policy_encryption
Command: disable authen_policy_encryption

Success.

DGS-3000-28SC: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-3000-28SC:admin#show authen_policy
Command: show authen_policy

Authentication Policy : Enabled

DGS-3000-28SC: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> - Enter the user-defined method list name. This value can be up to 15 characters long.

Restrictions

Only Administrators can issue this command.

Example

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

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

Success.

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

5-7 config authen_login

Description

This command is used to configure a user-defined or default method list of authentication methods for user login. The sequence of methods will effect the altercation 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 logins 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}(1)

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 - Specify the authentication method used. **tacacs** - Specify to authenticate by using the built-in server group called “TACACS”. **xtacacs** - Specify to authenticate by using the built-in server group called “XTACACS”. **tacacs+** - Specify to authenticate by using the built-in server group called “TACACS+”. **radius** - Specify to authenticate by using the built-in server group called “RADIUS”. **server_group** - Specify to authenticate by using the user-defined server group. **<string 15>** - Enter the server group value here. This value can be up 15 characters long. **local** - Specify to authenticate by local user account database in device. **none** - No authentication.

Restrictions

Only Administrators can issue this command.

Example

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

```
DGS-3000-28SC: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-3000-28SC: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> - Enter the user-defined method list name. This value can be up to 15 characters long.

Restrictions

Only Administrators can issue this command.

Example

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

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

Success.

DGS-3000-28SC: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-3000-28SC: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-3000-28SC: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> - Enter the user-defined method list name. This value can be up to 15 characters long.

Restrictions

Only Administrators can issue this command.

Example

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

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

Success.

DGS-3000-28SC: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 altercation 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 a TACACS group is 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}(1)

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 - Specify the authentication method used. **tacacs** - Specify to authenticate by using the built-in server group called "TACACS". **xtacacs** - Specify to authenticate by using the built-in server group called "XTACACS". **tacacs+** - Specify to authenticate by using the built-in server group called "TACACS+". **radius** - Specify to authenticate by using the built-in server group called "RADIUS". **server_group** - Specify 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** - Specify to authenticate by local enable password in device. **none** - 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-3000-28SC: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-3000-28SC: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> - Enter the user-defined method list name. This value can be up to 15 characters long.

Restrictions

Only Administrators can issue this command.

Example

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

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

Success.

DGS-3000-28SC: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 - Specify to display the default user-defined method list for promoting user's privilege to Admin level.
method_list_name - Specify to display 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 - Specify to display 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-3000-28SC: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-3000-28SC: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 15>** - 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-3000-28SC: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-3000-28SC: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-3000-28SC: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-3000-28SC: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> - Enter the user-defined server group name. This value can be up to 15 characters long.

Restrictions

Only Administrators can issue this command.

Example

To create a user-defined authentication server group:

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

Success.

DGS-3000-28SC: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> protocol [tacacs | xtacacs | tacacs+ | radius]

Parameters

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 - Specify the IP address of the server host. **<ipaddr>** - Enter the server host IPv4 address.
protocol - Specify the authentication protocol used. **tacacs** - Specify that the TACACS authentication protocol will be used. **xtacacs** - Specify that the XTACACS authentication protocol will be used. **tacacs+** - Specify that the TACACS+ authentication protocol will be used. **radius** - Specify 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-3000-28SC:admin#config authen server_group mix_1 add server_host 10.1.1.222
protocol tacacs+
Command: config authen server_group mix_1 add server_host 10.1.1.222 protocol
tacacs+


Success.


DGS-3000-28SC: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> - Enter the user-defined server group name. This value can be up to 15 characters long.

Restrictions

Only Administrators can issue this command.

Example

To delete a user-defined authentication server group:

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

Success.

DGS-3000-28SC: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) Enter the built-in or user-defined server group name. This value can be up to 15 characters long.

Restrictions

Only Administrators can issue this command.

Example

To display all authentication server groups:

```
DGS-3000-28SC: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-3000-28SC: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> protocol [tacacs | xtacacs | tacacs+ | radius] {port <int 1-65535> | [key [<key_string 254> | none] | encryption_key <key_string 344>] | timeout <int 1-255> | retransmit <int 1-20>}

Parameters

<ipaddr> - Enter the server host IP address.
protocol - Specify 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.
encryption_key - (Optional) Specify the encrypted form key string for TACACS+ and RADIUS authentication. This value is meaningless for TACACS and XTACACS. The encryption algorithm is based on DES. **<key_string 344>** - Enter the encrypted form key string for TACACS+ and RADIUS authentication.
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-3000-28SC: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-3000-28SC:admin#
```

5-21 config authen server_host

Description

This command is used to configure an authentication server host.

Format

config authen server_host <ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius] {port <int 1-65535> | [key [<key_string 254> | none] | encryption_key <key_string 344>] | timeout <int 1-255> | retransmit <int 1-20>}

Parameters

<ipaddr> - Enter the server host IP address.
protocol - Specify 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.
encryption_key - (Optional) Specify the encrypted form key string for TACACS+ and RADIUS authentication. This value is meaningless for TACACS and XTACACS. The encryption algorithm is based on DES. **<key_string 344>** - Enter the encrypted form key string for TACACS+ and RADIUS authentication.
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-3000-28SC: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-3000-28SC:admin#
```

5-22 delete authen server_host

Description

This command is used to delete an authentication server host.

Format

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

Parameters

<ipaddr> - Enter the server host's IP address.
protocol - Specify 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-3000-28SC:admin#delete authen server_host 10.1.1.222 protocol tacacs+
Command: delete authen server_host 10.1.1.222 protocol tacacs+

Success.

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

5-24 config authen parameter response_timeout

Description

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

Format

config authen parameter response_timeout <int 0-255>

Parameters

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

Restrictions

Only Administrators can issue this command.

Example

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

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

Success.

DGS-3000-28SC: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> - Enter 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-3000-28SC:admin#config authen parameter attempt 9
Command: config authen parameter attempt 9

Success.

DGS-3000-28SC: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-3000-28SC:admin#show authen parameter
Command: show authen parameter

Response Timeout : 60 seconds
User Attempts    : 9

DGS-3000-28SC: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 lever privilege:

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

PassWord:*****
Success.

DGS-3000-28SC: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) Specify the password form.
- **plain_text** - Specify the password in plain text form.
- **sha_1** - Specify the password in SHA-1 encrypted form.
  - **<password>** - Enter the password for promoting the privilege level. The length for a password in plain-text form and SHA-1 encrypted form are different.

Restrictions

Only Administrators can issue this command.

Example

To configure the administrator password:

```
DGS-3000-28SC:admin#config admin local_enable
Command: config admin local_ebable

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

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

5-29 config aaa server_group

Description

This command is used to add or remove an AAA server host to or from the specified server group. The built-in TACACS, XTACACS, TACACS+, and RADIUS server groups only accept server hosts with the same protocol, but a user-defined server group can accept server hosts with different protocols.

Format

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

Parameters

tacacs - Specify the built-in TACACS server group.
xtacacs - Specify the built-in XTACACS server group.
tacacs+ - Specify the built-in TACACS+ server group.
radius - Specify the built-in RADIUS server group.
group_name - Specify a user-defined server group. **<string 15>** - Enter the name of the server group.
add - Add a server host to the server group.
delete - Remove a server host to the server group.
server_host - Specify the server host. **<ipaddr>** - Enter the IP address of the server host.
protocol - Specify the server host protocol. **tacacs** - Specify the server host using TACACS protocol. **xtacacs** - Specify the server host using XTACACS protocol. **tacacs+** - Specify the server host using TACACS+ protocol. **radius** - Specify the server host using RADIUS protocol.

Restrictions

Only Administrator-level users can issue this command.

Example

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

```
DGS-3000-28SC:admin# config aaa server_group group_name mix_1 add server_host
10.1.1.222 protocol tacacs+
Command: config aaa server_group group_name mix_1 add server_host 10.1.1.222
protocol tacacs+

Success.

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

5-30 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> - Enter 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-3000-28SC:admin#create accounting method_list_name shell_acct
Command: create accounting method_list_name shell_acct

Success.

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

5-31 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 - Specify the default method list of accounting methods.
method_list_name - Specify the user-defined method list of accounting methods. <**string 15>** - Enter the name of the method list.
method - Specify the protocol. **tacacs+** - Specify the built-in TACACS+ server group. **radius** - Specify the built-in RADIUS server group. **server_group** - Specify 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** - Specify no accounting.

Restrictions

Only Administrators can issue this command.

Example

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

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

Success.

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

5-32 delete accounting method_list_name

Description

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

Format

delete accounting method_list_name <string 15>

Parameters

<string 15> - Enter the 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-3000-28SC:admin#delete accounting method_list_name shell_acct
Command: delete accounting method_list_name shell_acct

Success.

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

5-33 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 - Specify 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-3000-28SC: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-3000-28SC:admin#
```

5-34 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 - Specify 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-3000-28SC:admin#config accounting service command method_list_name
shell_acct
Command: config accounting service command method_list_name shell_acct

Success.

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

5-35 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, 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 - Specify the state of the specified service. **enable** - Specify to enable the specified accounting service. **radius_only** - (Optional) Specify accounting service to only use RADIUS group specified by the **config radius add** command. **method_list_name** - (Optional) Specify 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) Specify accounting service by the AAA default method list. **disable** - Specify 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-3000-28SC:admin#config accounting service shell state enable
Command: config accounting service shell state enable

Success.

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

5-36 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-3000-28SC:admin#show accounting service
Command: show accounting service

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

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

5-37 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-3000-28SC: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-3000-28SC:admin#
```

5-38 show aaa server_group

Description

This command is used to display the groups of AAA servers groups.

Format

show aaa server_group {<string 15>}

Parameters

<string 15> - (Optional) Specify the built-in or user-defined server group name.

Restrictions

Only Administrators can issue this command.

Example

To display all AAA server groups:

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

Group Name      IP Address                              Protocol
--------------- --------------------------------------- --------
mix_1           --------------------------------------- --------

radius          --------------------------------------- --------

tacacs          --------------------------------------- --------

tacacs+         --------------------------------------- --------

xtacacs         --------------------------------------- --------

Total Entries : 5

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

5-39 delete aaa server_group

Description

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

Format

delete aaa server_group <string 15>

Parameters

<string 15> - Specify the server group name to be deleted.

Restrictions

Only Administrators can issue this command.

Example

To delete a user-defined AAA server group called “mix_1”::

```
DGS-3000-28SC:admin# delete aaa server_group mix_1
Command: delete aaa server_group mix_1

Success.

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

5-40 show aaa server_host

Description

This command is used to display the AAA server hosts.

Format

show aaa server_host

Parameters

None.

Restrictions

None.

Example

To display all AAA server hosts:

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

IP Address           Protocl Port  Acct  Time Retry Key
                                   Port  out
-------------------- ------- ----- ----- ---- ----- --------------------------
10.1.1.222           RADIUS  15555 1813  10   2     abc123


Total Entries : 1

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

5-41 delete aaa server_host

Description

This command is used to delete an AAA server host.

Format

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

Parameters

<ipaddr> - Enter the IP address of the server host.
protocol - Specify the protocol. **tacacs** - Specify TACACS server host. **xtacacs** - Specify XTACACS server host. **tacacs+** - Specify TACACS+ server host.

radius - Specify RADIUS server host.

Restrictions

Only Administrators can issue this command.

Example

To tacacs | xtacacs | tacacs+| delete an AAA server host, with an IP address of 10.1.1.222, that is running the TACACS+ protocol:

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

Success.

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

5-42 create tacacs server_host

Description

This command is used to create a TACACS server host

Format

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

Parameters

<ipaddr> - Enter the IP address of the server host.
port - (Optional) The port number of the TACACS server host. **<int 1-65535>** - Enter the value between 1 and 65535. The default value is 49.
timeout - (Optional) Specify the time in second to wait for the server to reply. **<int 1-255>** - Enter the value between 1 and 255. The default value is 5.
retransmit - (Optional) Specify the count for re-transmissions. **<int 1-20>** - Enter the value between 1 and 20. The default value is 2.

Restrictions

Only Administrators can issue this command.

Example

To display AAA global configuration:

```
DGS-3000-28SC:admin# create tacacs server_host 10.1.1.223 port 15555 timeout 10
Command: create tacacs server_host 10.1.1.223 port 15555 timeout 10

Success.

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

5-43 create radius server_host

Description

This command is used to create an RADIUS server host.

Format

create radius server_host <ipaddr> {auth_port <int 1-65535> | acct_port <int 1-65535> | [key [<key_string 254> | none] | encryption_key <key_string 344>] | timeout <int 1-255> | retransmit <int 1-20>}

Parameters

<ipaddr> - Enter the IP address of the server host.
auth_port - (Optional) Specify the port of the RADIUS authentication. **<int 1-65535>** - Enter the value between 1 and 65535. The default value is 1812.
acct_port - (Optional) Specify the port of the RAIDUS accounting. **<int 1-65535>** - Enter the value between 1 and 65535. The default value is 1813.
key - (Optional) Specify the key for RADIUS. **<key_string 254>** - Enter the plain text key string for RADIUS. **none** - No encryption for RADIUS.
encryption_key - (Optional) The encrypted form key string for RADIUS. The encryption algorithm is based on DES. **<key_string 344>** - Etner the string with maximum 344 characters.
timeout - (Optional) Specify the time in second to wait for the server to reply. **<int 1-255>** - Enter the value between 1 and 255. The default value is 5.
retransmit - (Optional) Specify the count for re-transmissions. **<int 1-20>** - Enter the value between 1 and 20. The default value is 2.

Restrictions

Only Administrators can issue this command.

Example

To create an RADIUS server host:

```
DGS-3000-28SC:admin# create radius server_host 10.1.1.222 auth_port 15555
timeout 10
Command: create radius server_host 10.1.1.222 auth_port 15555 timeout 10

Key is empty for TACACS+ or RADIUS.

Success.

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

5-44 config radius server_host

Description

This command is used to config the radius server host.

Format

config radius server_host <ipaddr> {auth_port <int 1-65535> | acct_port <int 1-65535> | [key [<key_string 254> | none] | encryption_key <key_string 344>] | timeout <int 1-255> | retransmit <int 1-20>}

Parameters

<ipaddr> - Enter the IP address of the server host.
auth_port - (Optional) Specify the port of the RADIUS authentication. **<int 1-65535>** - Enter the value between 1 and 65535. The default value is 1812.
acct_port - (Optional) Specify the port of the RAIDUS accounting. **<int 1-65535>** - Enter the value between 1 and 65535. The default value is 1813.
key - (Optional) Specify the key for RADIUS. **<key_string 254>** - Enter the plain text key string for RADIUS. **none** - No encryption for RADIUS.
encryption_key - (Optional) The encrypted form key string for RADIUS. The encryption algorithm is based on DES. **<key_string 344>** - Enter the string with maximum 344 characters.
timeout - (Optional) Specify the time in second to wait for the server to reply. **<int 1-255>** - Enter the value between 1 and 255. The default value is 5.
retransmit - (Optional) Specify the count for re-transmissions. **<int 1-20>** - Enter the value between 1 and 20. The default value is 2.

Restrictions

Only Administrators can issue this command.

Example

To configure the RADIUS server host::

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

Success.

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

5-45 config radius source_ipif

Description

This command is used to specify source interface for all outgoing RADIUS packets.

Format

config radius source_ipif [<ipif_name 12> {<ipaddr> | <ipv6addr>} | none]

Parameters

<ipif_name 12> - Specify the interface name as source interface for all outgoing RADIUS packets. If there are several IPv4 addresses or IPv6 global addresses assigned to the specified source interface, the least IPv4 address or smallest IPv6 global address will be selected for RADIUS by default. **<ipaddr>** - (Optional) Specify the IP address as source IPv4 address for all outgoing RADIUS packets. **<ipv6addr>** - (Optional) Specify IP address as source IPv4 address for all outgoing RADIUS packets.
none - Revert to the default route table for all outgoing RADIUS packet.

Restrictions

Only Administrators can issue this command.

Example

To specify if_v200 as source interface for all outgoing RADIUS packets:

```
DGS-3000-28SC:admin# config radius source_ipif if_v200
Command: config radius source_ipif if_v200

Success.

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

5-46 show radius source_ipif

Description

This command is used to display specified source interface for all outgoing RADIUS packets.

Format

show radius source_ipif

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To display specified source interface for all outgoing RADIUS packets:

```
DGS-3000-28SC:admin# show radius source_ipif
Command: show radius source_ipif

IP Interface: ip_v300
IPv4 Address: 192.168.1.100
IPv6 Address: 2500::8

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

5-47 config tacacs server_host

Description

This command is used to configure a TACACS server host.

Format

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

Parameters

<ipaddr> - Enter the IP address of the server host.
port - (Optional) The port number of the TACACS server host. **<int 1-65535>** - Enter the value between 1 and 65535. The default value is 49.
timeout - (Optional) Specify the time in second to wait for the server to reply. **<int 1-255>** - Enter the value between 1 and 255. The default value is 5.
retransmit - (Optional) Specify the count for re-transmissions. **<int 1-20>** - Enter the value between 1 and 20. The default value is 2.

Restrictions

Only Administrators can issue this command.

Example

To configure the TACACS server host:

```
DGS-3000-28SC:admin# config tacacs server_host 10.1.1.223 retransmit 5
Command: config tacacs server_host 10.1.1.223 retransmit 5

 Key is meaningless for TACACS and XTACACS.

Success.

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

5-48 config tacacs source_ipif

Description

This command is used to specify source interface for all outgoing TACACS packets.

Format

config tacacs source_ipif [<ipif_name 12>{<ipaddr>} | none]

Parameters

<ipif_name 12> - Enter the interface name as a source interface for all outgoing TACACS packets. **<ipaddr>** - (Optional) Specify IP address as source IPv4 address for all outgoing TACACS packets.
none - Specify to revert to the default route table for all outgoing TACACS packets.

Restrictions

Only Administrators can issue this command.

Example

To specify **if_v200** as source interface for all outgoing TACACS packets:

```
DGS-3000-28SC:admin# config tacacs source_ipif if_v200
Command: config tacacs source_ipif if_v200

Success.

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

5-49 show tacacs source_ipif

Description

This command is used to display specified source interface for all outgoing TACACS packets.

Format

show tacacs source_ipif

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To display specified source interface for all outgoing TACACS packets:

```
DGS-3000-28SC:admin# show tacacs source_ipif
Command: show tacacs source_ipif

IP Interface: ip_v200
IPv4 Address: 172.18.1.253
IPv6 Address: 2000::15

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

5-50 config tacacs+ server_host

Description

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

Format

config tacacs+ server_host <ipaddr> {port <int 1-65535> | [key [<key_string 254> | none] | encryption_key <key_string 344>] | timeout <int 1-255>}

Parameters

<ipaddr> - Enter the IP address of the server host.
port - (Optional) The port number of the TACACS+ server host. **<int 1-65535>** - Enter the value between 1 and 65535. The default value is 49.
key - (Optional) Specify the key for TACACS+. **<key_string 254>** - Enter the plain text key string for TACACS+. **none** - No encryption for RADIUS.
encryption_key - (Optional) The encrypted form key string for TACACS+. The encryption algorithm is based on DES. **<key_string 344>** - Etner the string with maximum 344 characters.
timeout - (Optional) Specify the time in second to wait for the server to reply. **<int 1-255>** - Enter the value between 1 and 255. The default value is 5.

Restrictions

Only Administrators can issue this command.

Example

To configure the TACACS+ server host:

```
DGS-3000-28SC:admin# config tacacs+ server_host 10.1.1.211 key "abcd123"
Command: config tacacs+ server_host 10.1.1.211 key "abcd123"

Success.

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

5-51 config xtacacs server_host

Description

This command is used configure a XTACACS server host.

Format

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

Parameters

<ipaddr> - Enter the IP address of the server host.
port - (Optional) The port number of the XTACACS server host. **<int 1-65535>** - Enter the value between 1 and 65535. The default value is 49.
timeout - (Optional) Specify the time in second to wait for the server to reply. **<int 1-255>** - Enter the value between 1 and 255. The default value is 5.
retransmit - (Optional) Specify the count for re-transmissions. **<int 1-20>** - Enter the value between 1 and 20. The default value is 2.

Restrictions

Only Administrators can issue this command.

Example

To configure the XTACACS server host:

```
DGS-3000-28SC:admin# config xtacacs server_host 10.1.1.224 retransmit 5
Command: config xtacacs server_host 10.1.1.224 retransmit 5

 Key is meaningless for TACACS and XTACACS.

Success.

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

5-52 create xtacacs server_host

Description

This command is used to create a XTACACS server host.

Format

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

Parameters

<ipaddr> - Enter the IP address of the server host.
port - (Optional) The port number of the XTACACS server host. **<int 1-65535>** - Enter the value between 1 and 65535. The default value is 49.
timeout - (Optional) Specify the time in second to wait for the server to reply. **<int 1-255>** - Enter the value between 1 and 255. The default value is 5.
retransmit - (Optional) Specify the count for re-transmissions. **<int 1-20>** - Enter the value between 1 and 20. The default value is 2.

Restrictions

Only Administrators can issue this command.

Example

To create a XTACACS server host:

```
DGS-3000-28SC:admin# create xtacacs server_host 10.1.1.224 port 15555 timeout
10
Command: create xtacacs server_host 10.1.1.224 port 15555 timeout 10

Success.

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

5-53 create tacacs+ server_host

Description

This command is used to create a TACACS+ server host.

Format

create tacacs+ server_host <ipaddr> {port <int 1-65535> | [key [<key_string 254> | none] | encryption_key <key_string 344>] | timeout <int 1-255>}

Parameters

<ipaddr> - Enter the IP address of the server host.
port - (Optional) The port number of the TACACS+ server host. **<int 1-65535>** - Enter the value between 1 and 65535. The default value is 49.

key - (Optional) Specify the key for TACACS+. **<key_string 254>** - Enter the plain text key string for TACACS+. **none** - No encryption for RADIUS.
encryption_key - (Optional) The encrypted form key string for TACACS+. The encryption algorithm is based on DES. **<key_string 344>** - Etner the string with maximum 344 characters.
timeout - (Optional) Specify the time in second to wait for the server to reply. **<int 1-255>** - Enter the value between 1 and 255. The default value is 5.

Restrictions

Only Administrators can issue this command.

Example

To create a TACACS+ server host:

```
DGS-3000-28SC:admin# create tacacs+ server_host 10.1.1.211 port 15555 timeout
10
key "abc123"
Command: create tacacs+ server_host 10.1.1.211 port 15555 timeout 10 key
"abc123"

Success.

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

5-54 create aaa server_group

Description

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

Format

create aaa server_group <string 15>

Parameters

<string 15> - Specify the user-defined server group name.

Restrictions

Only Administrators can issue this command.

Example

To create a user-defined AAA server group called “mix_1”:

```
DGS-3000-28SC:admin# create aaa server_group mix_1
Command: create aaa server_group mix_1

Success.

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

5-55 enable aaa_server_password_encryption

Description

This command is used to enable AAA server password encryption.

Format

enable aaa_server_password_encryption

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To enable AAA server password encryption:

```
DGS-3000-28SC:admin# enable aaa_server_password_encryption
Command: enable aaa_server_password_encryption

Success.

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

5-56 disable aaa_server_password_encryption

Description

This command is used to disable AAA server password encryption.

Format

disable aaa_server_password_encryption

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To disable AAA server password encryption:

```
DGS-3000-28SC:admin#disable aaa_server_password_encryption
Command: disable aaa_server_password_encryption

Success.

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

Chapter 6 Access Control List (ACL) Command List

create access_profile profile_id <value 1-6> profile_name <name1-32> [ethernet {vlan {<hex0x0-0x0fff>} | source_mac <macmask000000000000-ffffffffffff> | destination_mac <macmask000000000000-ffffffffffff> | 802.1p | ethernet_type} | ip {vlan {<hex0x0-0x0fff>} | source_ip_mask <netmask> | destination_ip_mask <netmask> | dscp | [icmp {type | code} | igmp {type} | tcp {src_port_mask <hex0x0-0xffff> | dst_port_mask <hex0x0-0xffff> | flag_mask [all| {urg | ack | psh | rst | syn | fin}]} | udp {src_port_mask <hex0x0-0xffff> | dst_port_mask <hex0x0-0xffff>} | protocol_id_mask <hex0x0-0xff> {user_define_mask <hex0x0-0xffffffff>}]} | packet_content_mask {offset_chunk_1 <value0-31> <hex0x0-0xffffffff> | offset_chunk_2 <value0-31> <hex0x0-0xffffffff> | offset_chunk_3 <value0-31> <hex0x0-0xffffffff> | offset_chunk_4 <value0-31> <hex0x0-0xffffffff>} | ipv6 {class | flowlabel | source_ipv6_mask <ipv6mask> | destination_ipv6_mask <ipv6mask> | [tcp {src_port_mask <hex0x0-0xffff> | dst_port_mask <hex0x0-0xffff>} | udp {src_port_mask <hex0x0-0xffff> | dst_port_mask <hex0x0-0xffff>} | icmp {type | code}]}]
delete access_profile [profile_id <value 1-6> | profile_name <name1-32> | all]
config access_profile [profile_id <value 1-6> | profile_name <name1-32>] [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 0x0-0xfffff> | source_ipv6 <ipv6addr> {mask <ipv6mask>} | destination_ipv6 <ipv6addr> {mask <ipv6mask>} | [tcp {src_port <value 0-65535> {mask <hex 0x0-0xffff>} | dst_port <value 0-65535> {mask <hex0x0-0xffff>}} | udp {src_port <value 0-65535> {mask <hex 0x0-0xffff>} | dst_port <value 0-65535> {mask <hex 0x0-0xffff>}} | icmp {type <value 0-255> | code <value 0-255>}]}] [port [<portlist> | all] | vlan_based [vlan <vlan_name 32> | vlan_id <vlanid 1-4094>]] [permit {priority <value 0-7> {replace_priority} | [replace_dscp_with <value 0-63> | replace_tos_precedence_with <value 0-7>] | counter [enable | disable]} | mirror | {group_id <value 1-4>} | deny] {time_range <range_name 32>} | delete access_id <value 1-256>]
show access_profile {[profile_id <value 1-6> | profile_name <name 1-32>]}
config flow_meter [profile_id <value 1-6> | profile_name <name 1-32>] access_id <value 1-256> [rate [<value 0-1048576>] {burst_size [<value 0-131072>]} rate_exceed [drop_packet | remark_dscp <value 0-63>] | tr_tcmcir <value 0-1048576> {cbs <value 0-131072>} pir <value 0-1048576> {pbs <value 0-131072>} {[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_tcmcir <value 0-1048576> cbs <value 0-131072> ebs <value 0-131072> {[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 1-6> | profile_name <name 1-32>] {access_id <value 1-256>}}
show current_config access_profile

6-1 create access_profile profile_id

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_prfile** 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
6. Packet Content.
7. Source IPv6 Address, Class, IPv6 Protocol (Next Header)
8. Destination IPv6 Address, Class, IPv6 Protocol (Next Header)

Format

create access_profile profile_id <value 1-6> profile_name <name1-32> [ethernet {vlan {<hex0x0-0x0fff>} | source_mac <macmask000000000000-ffffffffffff> | destination_mac <macmask000000000000-ffffffffffff> | 802.1p | ethernet_type} | ip {vlan {<hex0x0-0x0fff>} | source_ip_mask <netmask> | destination_ip_mask <netmask> | dscp | [icmp {type | code} | igmp {type} | tcp {src_port_mask <hex0x0-0xffff> | dst_port_mask <hex0x0-0xffff> | flag_mask [all| {urg | ack | psh | rst | syn | fin}]} | udp {src_port_mask <hex0x0-0xffff> | dst_port_mask <hex0x0-0xffff>} | protocol_id_mask <hex0x0-0xff> {user_define_mask <hex0x0-0xffffffff>}]} | packet_content_mask {offset_chunk_1 <value0-31> <hex0x0-0xffffffff> | offset_chunk_2 <value0-31> <hex0x0-0xffffffff> | offset_chunk_3 <value0-31> <hex0x0-0xffffffff> | offset_chunk_4 <value0-31> <hex0x0-0xffffffff>} | ipv6 {class | flowlabel | source_ipv6_mask <ipv6mask> | destination_ipv6_mask <ipv6mask> | [tcp {src_port_mask <hex0x0-0xffff> | dst_port_mask <hex0x0-0xffff>} | udp {src_port_mask <hex0x0-0xffff> | dst_port_mask <hex0x0-0xffff>} | icmp {type | code}]}]

Parameters

<value 1-6> - Enter the profile ID here. This value must be between 1 and 6.
profile_name - The name of the profile must be specified. The maximum length is 32 characters. **<name1-32>** - Enter the profile name here.
ethernet - Specify this is an ethernet mask. **vlan** - (Optional) Specify 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) Specify the source MAC mask. **<macmask>** - Enter the source MAC address used here. **destination_mac** - (Optional) Specify the destination MAC mask. **<macmask>** - Enter the destination MAC address used here. **802.1p** - (Optional) Specify the 802.1p priority tag mask. **ethernet_type** - (Optional) Specify the Ethernet type mask.

ip - Specify this is a IPv4 mask.
- **vlan** - (Optional) Specify 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) Specify a source IP address mask.
  - **<netmask>** - Enter the source IP address mask here.
- **destination_ip_mask** - (Optional) Specify a destination IP address mask.
  - **<netmask>** - Enter the destination IP address mask here.
  - **dscp** - (Optional) Specify the DSCP mask.
  - **icmp** - (Optional) Specify that the rule applies to ICMP traffic.
  - **type** - Specify the type of ICMP traffic.
  - **code** - Specify the code of ICMP traffic
  - **igmp** - (Optional) Specify that the rule applies to IGMP traffic.
  - **type** - Specify the type of IGMP traffic.
  - **tcp** - (Optional) Specify that the rule applies to TCP traffic.
  - **src_port_mask** - (Optional) Specify the TCP source port mask.
    - **<hex 0x0-0xffff>** - Enter the TCP source port mask here.
  - **dst_port_mask** - (Optional) Specify the TCP destination port mask.
    - **<hex 0x0-0xffff>** - Enter the TCP destination port mask here.
  - **flag_mask** - (Optional) Specify the TCP flag field mask.
    - **all** – Specify that all the flags will be used for the TCP mask.
    - **urg** – (Optional) Specify that the TCP flag field will be set to 'urg'.
    - **ack** - (Optional) Specify that the TCP flag field will be set to 'ack'.
    - **psh** - (Optional) Specify that the TCP flag field will be set to 'psh'.
    - **rst** - (Optional) Specify that the TCP flag field will be set to 'rst'.
    - **syn** - (Optional) Specify that the TCP flag field will be set to 'syn'.
    - **fin** - (Optional) Specify that the TCP flag field will be set to 'fin'.
- **udp** - (Optional) Specify that the rule applies to UDP traffic.
  - **src_port_mask** - (Optional) Specify the UDP source port mask.
    - **<hex 0x0-0xffff>** - Enter the UDP source port mask here.
  - **dst_port_mask** - (Optional) Specify the UDP destination port mask.
    - **<hex 0x0-0xffff>** - Enter the UDP destination port mask here.
- **protocol_id_mask** - (Optional) Specify that the rule applies to IP protocol ID traffic.
  - **<0x0-0xff>** - Enter the protocol ID mask here.
  - **user_define_mask** - (Optional) Specify 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 - Specify the packet content mask. Only one packet_content_mask profile can be created.
- **offset_chunk_1** - (Optional) Specify 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) Specify 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) Specify 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) Specify 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 - Specify this is the IPv6 mask.
- **class** - (Optional) Specify the IPv6 class.
- **flowlabel** - (Optional) Specify the IPv6 flow label.
- **source_ipv6_mask** - (Optional) Specify an IPv6 source sub-mask.
  - **<ipv6mask>** - Enter the source IPv6 mask value here.
- **destination_ipv6_mask** - (Optional) Specify an IPv6 destination sub-mask.
  - **<ipv6mask>** -Enter the destination IPv6 mask value here.
- **tcp** - (Optional) Specify that the rule applies to TCP traffic.
  - **src_port_mask** - (Optional) Specify an IPv6 TCP source port mask.
    - **<hex 0x0-0xffff>** - Enter the TCP source port mask value here.

dst_port_mask - (Optional) Specify an IPv6 TCP destination port mask.
<hex 0x0-0xffff> - Enter the TCP destination port mask value here.
udp - (Optional) Specify that the rule applies to UDP traffic.
src_port_mask - Specify the UDP source port mask.
<hex 0x0-0xffff> - Enter the UDP source port mask value here.
dst_port_mask - Specify the UDP destination port mask.
<hex 0x0-0xffff> - Enter the UDP destination port mask value here.
icmp - (Optional) Specify a mask for ICMP filtering.
type - (Optional) Specify the inclusion of the ICMP type field in the mask.
code - (Optional) Specify 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-3000-28SC: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-3000-28SC: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-3000-28SC: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-3000-28SC: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 1-6> | profile_name <name1-32> | all]

Parameters

profile_id - Specify the index of the access list profile. **<value 1-6>** - Enter the profile ID value here. This value must be between 1 and 6.
profile_name - Specify the name of the profile. **<name1-32>** - Enter the profile name. The maximum length is 32 characters.
all - Specify 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-3000-28SC:admin#delete access_profile profile_id 1
Command: delete access_profile profile_id 1

Success.

DGS-3000-28SC: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 1-6> | profile_name <name1-32>] [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 0x0-0xfffff> | source_ipv6 <ipv6addr> {mask <ipv6mask>} | destination_ipv6 <ipv6addr> {mask <ipv6mask>} | [tcp {src_port <value 0-65535> {mask <hex 0x0-0xffff>} | dst_port <value 0-65535> {mask <hex0x0-0xffff>}}

| udp {src_port <value 0-65535> {mask <hex 0x0-0xffff>} | dst_port <value 0-65535> {mask <hex 0x0-0xffff>}} | icmp {type <value 0-255> | code <value 0-255>}]}] [port [<portlist> | all] | vlan_based [vlan <vlan_name 32> | vlan_id <vlanid 1-4094>]] [permit {priority <value 0-7> {replace_priority} | [replace_dscp_with <value 0-63> | replace_tos_precedence_with <value 0-7>] | counter [enable | disable]} | mirror | {group_id <value 1-4>} | deny] {time_range <range_name 32>} | delete access_id <value 1-256>]

Parameters

profile_id - Specify the index of the access list profile.
- **<value 1-6>** - Enter the profile ID value here. This value must be between 1 and 512.

profile_name - Specify the name of the profile.
- **<name1-32>** - Enter the profile name here. This name can be up to 32 characters long.

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

access_id - Specify 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** - Specify 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 - Specify to configure the ethernet access profile.
- **vlan** - (Optional) Specify 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) Specify the VLAN ID used.
  - **<vlanid 1-4094>** - Enter the VLAN ID used here. This value must be between 1 and 4094.
  - **mask** - (Optional) Specify an additional mask parameter that can be configured.
    - **<hex 0x0-0x0fff>** - Enter the mask value here.
- **source_mac** - (Optional) Specify the source MAC address.
  - **<macaddr>** - Enter the source MAC address used for this configuration here.
  - **mask** - (Optional) Specify an additional mask parameter that can be configured.
    - **<macmask>** - Enter the source MAC mask used here.
- **destination_mac** - (Optional) Specify the destination MAC address.
  - **<macaddr>** - Enter the destination MAC address used for this configuration here.
  - **mask** - (Optional) Specify an additional mask parameter that can be configured.
    - **<macmask>** - Enter the destination MAC mask here.
- **802.1p** - (Optional) Specify 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) Specify the Ethernet type.
  - **<hex 0x0-0xffff>** - Enter the Ethernet type mask here.

ip - Specify to configure the IP access profile.
- **vlan** - (Optional) Specify 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) Specify that VLAN ID used.
  - **<vlanid 1-4094>** - Enter the VLAN ID used here. This value must be between 1 and 4094.
  - **mask** – (Optional) Specify an additional mask parameter that can be configured.
    - **<hex 0x0-0x0fff>** - Enter the mask value here.
- **source_ip** - (Optional) Specify an IP source address.
  - **<ipaddr>** - Enter the source IP address used for this configuration here.
  - **mask** - (Optional) Specify an additional mask parameter that can be configured.
    - **<netmask>** - Enter the source netmask used here.
- **destination_ip** - (Optional) Specify an IP destination address.
  - **<ipaddr>** - Enter the destination IP address used for this configuration here.
  - **mask** - (Optional) Specify an additional mask parameter that can be configured.
    - **<netmask>** - Enter the destination netmask used here.
- **dscp** - (Optional) Specify the value of DSCP. The DSCP value ranges from 0 to 63.
  - **<value 0-63>** - Enter the DSCP value here.
- **icmp** - (Optional) Specify to configure the ICMP parameters.
  - **type** - (Optional) Specify 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) Specify 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) Specify to configure the IGMP parameters.
type - (Optional) Specify 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 - Specify to configure the TCP parameters.
src_port - (Optional) Specify 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) Specify an additional mask parameter that can be configured.
<hex 0x0-0xffff> - Enter the source port mask here.
dst_port - (Optional) Specify 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) Specify an additional mask parameter that can be configured.
<hex 0x0-0xffff> - Enter the destination port mask here.
flag - (Optional) Specify the TCP flag fields.
all - Specify that all the TCP flags will be used in this configuration.
urg - (Optional) Specify that the TCP flag field will be set to 'urg'.
ack - (Optional) Specify that the TCP flag field will be set to 'ack'.
psh - (Optional) Specify that the TCP flag field will be set to 'psh'.
rst - (Optional) Specify that the TCP flag field will be set to 'rst'.
syn - (Optional) Specify that the TCP flag field will be set to 'syn'.
fin - (Optional) Specify that the TCP flag field will be set to 'fin'.
udp - Specify to configure the UDP parameters.
src_port - (Optional) Specify 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) Specify an additional mask parameter that can be configured.
<hex 0x0-0xffff> - Enter the source port mask here.
dst_port - (Optional) Specify 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) Specify an additional mask parameter that can be configured.
<hex 0x0-0xffff> - Enter the destination port mask here.
protocol_id - Specify 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) Specify 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 - Specify 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) Specify 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) Specify 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) Specify 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) Specify 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 - Specify that the rule applies to IPv6 fields.
- **class** - (Optional) Specify 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) Specify the value of the IPv6 flow label.
  - **<hex 0x0-0xffff>** - Enter the IPv6 flow label mask used here.
- **source_ipv6** - (Optional) Specify the value of the IPv6 source address.
  - **<ipv6addr>** - Enter the source IPv6 address used for this configuration here.
  - **mask** - (Optional) Specify an additional mask parameter that can be configured.
    - **<ipv6mask>** - Enter the source IPv6 mask here.
- **destination_ipv6** - (Optional) Specify the value of the IPv6 destination address.
  - **<ipv6addr>** - Enter the destination IPv6 address used for this configuration here.
  - **mask** - (Optional) Specify an additional mask parameter that can be configured.
  - **<ipv6mask>** - Enter the destination IPv6 mask here.
- **tcp** - (Optional) Specify to configure the TCP parameters.
  - **src_port** - Specify 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** - Specify an additional mask parameter that can be configured.
      - **<hex 0x0-0xffff>** - Enter the TCP source port mask value here.
  - **dst_port** - (Optional) Specify 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** - Specify an additional mask parameter that can be configured.
      - **<hex 0x0-0xffff>** - Enter the TCP destination port mask value here.
- **udp** - (Optional) Specify to configure the UDP parameters.
  - **src_port** - Specify 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** - Specify an additional mask parameter that can be configured.
      - **<hex 0x0-0xffff>** - Enter the UDP source port mask value here.
  - **dst_port** - Specify 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** - Specify an additional mask parameter that can be configured.
      - **<hex 0x0-0xffff>** - Enter the UDP destination port mask value here.
- **icmp** - (Optional) Specify to configure the ICMP parameters used.
  - **type** - (Optional) Specify 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) Specify 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 - Specify the port list used for this configuration.
- **<portlist>** - Enter a list of ports used for the configuration here.
- **all** - Specify that all the ports will be used for this configuration.
- **vlan_based** - Specify that the rule will be VLAN based.
  - **vlan** - Specify the VLAN name used for this configuration.
    - **<vlan_name>** - Enter the VLAN name used for this configuration here.
  - **vlan_id** - Specify 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 - Specify that packets matching the access rule are permitted by the Switch.
- **priority** - (Optional) Specify 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) Specify that the 802.1p priority of the outgoing packet will be replaced.
- **replace_dscp_with** - (Optional) Specify 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) Specify 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) Specify 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** - Specify that the ACL counter feature will be enabled. **disable** - Specify that the ACL counter feature will be disabled.
mirror - Specify that packets matching the access rules are copied to the mirror port. **group_id** - (Optional) Specify the groupd ID. **<value 1-4>** - Enter the value between 1 and 4.
deny - Specify that packets matching the access rule are filtered by the Switch.
time_range - (Optional) Specify 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 - Specify that a profile or a rule will be deleted.
access_id - Specify 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-3000-28SC: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-3000-28SC: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 1-6> | profile_name <name 1-32>]}

Parameters

profile_id - (Optional) Specify the index of the access list profile.

	<value 1-6> - Enter the profile ID used here. This value must be between 1 and 6.
profile_name - (Optional) Specify the name of the profile.	
	<name 1-32> - 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-3000-28SC: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-3000-28SC:admin#
```

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

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

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

```
DGS-3000-28SC: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-3000-28SC: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 1-6> | profile_name <name 1-32>] access_id <value 1-256> [rate [<value 0-1048576>] {burst_size [<value 0-131072>]} rate_exceed [drop_packet | remark_dscp <value 0-63>] | tr_tcmcir <value 0-1048576> {cbs <value 0-131072>} pir <value 0-1048576> {pbs <value 0-131072>} {[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_tcmcir <value 0-1048576> cbs <value 0-131072> ebs <value 0-131072> {[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 - Specify the profile ID.
- **<value 1-6>** - Enter the profile ID here. This value must be between 1 and 6. A lower value denotes a higher priority.

profile_name - Specify the name of the profile. The maximum length is 32 characters.
- **<name 1-32>** - Enter the profile name used here.

access_id - Specify the access ID.
- **<value 1-256>** - Enter the access ID used here. This value must be between 1 and 256. A lower value denotes a higher priority.

rate - This specifies the rate for single rate two color mode. Specify the committed bandwidth in Kbps for the flow. The value m and n are determined by the project.
- **<value 0-1048576>** - Enter the rate for single rate two color mode here. This value must be between 0 and 1048576.

burst_size - (Optional) This specifies the burst size for the single rate two color mode. The unit is Kbytes.
- **<value 0-131072>** - Enter the burst size value here. This value must be between 0 and 131072.

rate_exceed - This specifies the action for packets that exceeds the committed rate in single rate, two color mode.
- **drop_packet** - Drop the packet immediately.
- **remark_dscp** - Mark the packet with a specified DSCP. The packet is set to have a high drop precedence.
  - **<value 0-63>** - Enter the remark DSCP value here. This value must be between 0 and 63.

tr_tcm - Specify the “two rate three color mode”.
- **cir** - Specify the Committed Information Rate. The unit is in Kbps. CIR should always be equal or less than PIR.
  - **<value 0-1048576>** - Enter the commited information rate value here. This value must be between 0 and 1048576.
- **cbs** - (Optional) Specify 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 0-1048576>** - Enter the commited burst size value here. This value must be between 0 and 1048576.
- **pir** - Specify the “Peak Information Rate”. The unit is in Kbps. PIR should always be equal to or greater than CIR.
  - **<value 0-1048576>** - Enter the peak information rate value here. This value must be between 0 and 1048576.
- **pbs** - (Optional) Specify the “Peak Burst Size”. The unit is in Kbytes. This parameter is an optional parameter. The default value is 4*1024.
  - **<value 0-131072>** - Enter the peak burst size value here. This value must be between 0

and 131072.
color_blind - (Optional) Specify the meter mode as color-blind. The default is color-blind mode.
color_aware - (Optional) Specify 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) Specify 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) Specify 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 - Specify that the ACL counter option will be enabled.
disable - Specify that the ACL counter option will be disabled.
exceed - Specify 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) Specify 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 - Specify that the ACL counter option will be enabled.
disable - Specify that the ACL counter option will be disabled.
violate - Specify 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) Specify 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 - Specify that the ACL counter option will **disable** - Specify that the ACL counter option will be disabled.be enabled.

sr_tcm - Specify “single rate three color mode”.
cir - Specify 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 - Specify the “Committed Burst Size” The unit is Kbytes.
<value 0-131072> - Enter the commited burst size value here. This value must be between 0 and 131072.
ebs - Specify 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) Specify the meter mode as color-blind. The default is color-blind mode.
color_aware - (Optional) Specify 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) Specify 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) Specify 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 - Specify that the ACL counter option will be enabled.

disable - Specify that the ACL counter option will be disabled.
exceed - Specify 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) Specify 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 - Specify that the ACL counter option will be enabled.
disable - Specify that the ACL counter option will be disabled.
violate - Specify 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) Specify 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 - Specify that the ACL counter option will be enabled.
disable - Specify that the ACL counter option will be disabled.
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-3000-28SC: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-3000-28SC: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 1-6> | profile_name <name 1-32>] {access_id <value 1-256>}}

Parameters

profile_id - (Optional) Specify the profile ID. **<value 1-6>** - Enter the profile ID used here. This value must be between 1 and 6.
profile_name - (Optional) Specify the name of the profile. **<name 1-32>** - Enter the profile name used here. The maximum length is 32 characters.
access_id - (Optional) Specify 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-3000-28SC:admin#show flow_meter
Command: show flow_meter

Flow Meter Information
------------------------------------------------------------------------------
Profile ID:1     Aceess 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-3000-28SC:admin#
```

6-7 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-3000-28SC: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-3000-28SC:admin#
```

Chapter 7 Access Control List (ACL) Egress Command List

create egress_access_profile profile_id <value 1-4> profile_name <name 1-32> [ethernet {vlan {<hex 0x0-0x0fff>} | source_mac <macmask 000000000000-ffffffffffff> | destination_mac <macmask 000000000000-ffffffffffff> | 802.1p | ethernet_type} | ip {vlan {<hex 0x0-0x0fff>} | source_ip_mask <netmask> | destination_ip_mask <netmask> | dscp | [icmp {type | code} | igmp {type} | tcp {src_port_mask <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>}]} | ipv6 {class | 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}]}]
config egress_access_profile [profile_id <value 1-4> | profile_name <name 1-32>] [add access_id [auto_assign | <value 1-128>] [ethernet {[vlan <vlan_name 32> | vlan_id <vlanid 1-4094>] {mask <hex 0x0-0x0fff>} | source_mac <macaddr> {mask <macmask>} | destination_mac <macaddr> {mask <macmask>} | 802.1p <value 0-7> | ethernet_type <hex 0x0-0xffff>} | ip {[vlan <vlan_name 32> | vlan_id <vlanid 1-4094>] {mask <hex 0x0-0x0fff>} | source_ip <ipaddr> {mask <netmask>} | destination_ip <ipaddr> {mask <netmask>} | dscp <value 0-63> | [icmp {type <value 0-255> | code <value 0-255>} | igmp {type <value 0-255>} | tcp {src_port <value 0-65535> {mask <hex 0x0-0xffff>} | dst_port <value 0-65535> {mask <hex 0x0-0xffff>} | flag [all | {urg | ack | psh | rst | syn | fin}]} | udp {src_port <value 0-65535> {mask <hex 0x0-0xffff>} | dst_port <value 0-65535> {mask <hex 0x0-0xffff>}} | protocol_id <value 0-255> {user_define <hex 0x0-0xffffffff> {mask <hex 0x0-0xffffffff>}}]} | ipv6 {class <value 0-255> | 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>}]}] [vlan_based [vlan <vlan_name 32> | vlan_id <vlanid 1-4094>] | port_group [id <value 1-64> | name <name 16>] | port <port>] [permit {replace_priority_with <value 0-7> | replace_dscp_with <value 0-63> | counter[enable | disable]} | deny] {time_range <range_name 32>} | delete access_id <value 1-128>]
config egress_flow_meter [profile_id <value 1-4> | profile_name <name 1-32>] access_id <value 1-128> [rate <value 0-1048576> {burst_size <value 0-131072>} rate_exceed [drop_packet | remark_dscp <value 0-63>] | tr_tcm cir <value 0-1048576> {cbs <value 0-131072>} pir <value 0-1048576> {pbs <value 0-131072>} {[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 0-1048576> cbs <value 0-131072> ebs <value 0-131072> {[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 <value0-63>} | drop] {counter [enable | disable]} | delete]
config port_group [id <value 1-64> | name <name 16>] [add | delete] [<portlist> | all]
show current_config egress_access_profile
show egress_access_profile {[profile_id <value 1-4> | profile_name <name 1-32>]}
show egress_flow_meter {[profile_id <value 1-4> | profile_name <name 1-32>] {access_id <value 1-128>}}
create port_group id <value 1-64> name <name 16>
show port_group {id <value 1-64> | name<name 16>}
delete egress_access_profile [profile_id <value 1-4> | profile_name <name 1-32> | all]
delete port_group [id <value 1-64> | name <name 16>]

7-1 create egress_access_profile profile_id

Description

This command is used to create an egress access list profile. For example, for some hardware, it may be invalid to specify destination IPv6 address and source IPv6 address at the same time. The user will be prompted for these limitations.

Format

create egress_access_profile profile_id <value 1-4> profile_name <name 1-32> [ethernet {vlan {<hex 0x0-0x0fff>} | source_mac <macmask 000000000000-ffffffffffff> | destination_mac <macmask 000000000000-ffffffffffff> | 802.1p | ethernet_type} | ip {vlan {<hex 0x0-0x0fff>} | source_ip_mask <netmask> | destination_ip_mask <netmask> | dscp | [icmp {type | code} | igmp {type} | tcp {src_port_mask <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>}]} | ipv6 {class | source_ipv6_mask <ipv6mask> | destination_ipv6_mask <ipv6mask> | [tcp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | udp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | icmp {type | code}]}]

Parameters

<value 1-4> - Enter the profile ID used here. This value must be between 1 and 4. A lower value denotes a higher priority.
profile_name - The name of the profile must be specified. The maximum length is 32 characters. **<name 1-32>** - Enter the profile name used here. This name can be up to 32 characters long.
ethernet - Specify this is an Ethernet mask.
vlan - (Optional) Specify a VLAN mask. **<hex 0x0-0x0fff>** - Enter the VLAN mask used here.
source_mac - (Optional) Specify the source MAC mask. **<macmask>** - Enter the source MAC mask used here.
destination_mac - (Optional) Specify the destination MAC mask. **<macmask>** - Enter the destination MAC mask used here.
802.1p - (Optional) Specify 802.1p priority tag mask.
ethernet_type - (Optional) Specify the Ethernet type mask.
ip - Specify this is an IPv4 mask.
vlan - (Optional) Specify a VLAN mask. **<hex 0x0-0x0fff>** - Enter the VLAN mask used here.
source_ip_mask - (Optional) Specify a source IP address mask. **<netmask>** - Enter the source network mask used here.
destination_ip_mask - (Optional) Specify a destination IP address mask. **<netmask>** - Enter the destination network mask used here.
dscp - (Optional) Specify the DSCP mask.
icmp - (Optional) Specify that the rule applies to ICMP traffic. **type** - Specify the type of ICMP traffic. **code** - Specify the code of ICMP traffic.
igmp - (Optional) Specify that the rule applies to IGMP traffic. **type** - Specify the type of IGMP traffic.
tcp - (Optional) Specify that the rule applies to TCP traffic. **src_port_mask** - Specify the TCP source port mask. **<hex 0x0-0xffff>** - Enter the TCP source port mask value here. **dst_port_mask** - Specify the TCP destination port mask. **<hex 0x0-0xffff>** - Enter the TCP source port mask value here.
flag_mask - (Optional) Specify the TCP flag field mask. **all** - Specify that the TCP flag field mask will be set to 'all'. **urg** - Specify that the TCP flag field mask will be set to 'urg'.

ack - Specify that the TCP flag field mask will be set to 'ack'. **psh** - Specify that the TCP flag field mask will be set to 'psh'. **rst** - Specify that the TCP flag field mask will be set to 'rst'. **syn** - Specify that the TCP flag field mask will be set to 'syn'. **fin** - Specify that the TCP flag field mask will be set to 'fin'.
udp - (Optional) Specify that the rule applies to UDP traffic. **src_port_mask** - Specify the UDP source port mask. **<hex 0x0-0xffff>** - Enter the UDP source port mask value here. **dst_port_mask** - Specify the UDP destination port mask. **<hex 0x0-0xffff>** - Enter the UDP destination port mask value here.
protocod_id_mask - (Optional) Specify that the rule applies to IP protocol ID traffic. **<hex 0x0-0xff>** - Enter the protocol ID mask value here.
user_define_mask - (Optional) Specify that the rule applies to the IP protocol ID, and that the mask option behind the IP header length is 20 bytes. **<hex 0x0-0xffffffff>** - Enter the user-defined mask value here.
ipv6 - (Optional) Specify this is an IPv6 mask.
class - (Optional) Specify the IPv6 class.
source_ipv6_mask - (Optional) Specify an IPv6 source sub-mask. **<ipv6mask>** - Enter the IPv6 source sub-mask value here. **destination_ipv6_mask** - Specify an IPv6 destination sub-mask. **<ipv6mask>** - Enter the IPv6 destination sub-mask value here.
tcp - (Optional) Specify that the following parameter are application to the TCP configuration. **src_port_mask** - Specify an IPv6 Layer 4 TCP source port mask. **<hex 0x0-0xffff>** - Enter the Ipv6 TCP source port mask value here. **dst_port_mask** - Specify an IPv6 Layer 4 TCP destination port mask. **<hex 0x0-0xffff>** - Enter the Ipv6 TCP destination port mask value here.
udp - (Optional) Specify that the following parameter are application to the UDP configuration. **src_port_mask** - Specify an IPv6 Layer 4 UDP source port mask. **<hex 0x0-0xffff>** - Enter the Ipv6 UDP source port mask value here. **dst_port_mask** - Specify an IPv6 Layer 4 UDP destination port mask. **<hex 0x0-0xffff>** - Enter the Ipv6 UDP destination port mask value here.
icmp - (Optional) Specify that the rule applies to ICMP traffic. **type** - Specify the type of ICMP traffic. **code** - Specify the code of ICMP traffic.

Restrictions

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

Example

To create an egress access list profile with the name “eap-eth-bc” and assign the profile ID to be 1:

```
DGS-3000-28SC:admin#  create egress_access_profile profile_id 1 profile_name
eap-eth-bc ethernet source_mac FF-FF-FF-FF-FF-FF
Command: create egress_access_profile profile_id 1 profile_name eap-eth-bc
ethernet source_mac FF-FF-FF-FF-FF-FF


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

7-2 config egress_access_profile

Description

This command is used to configure egress access list entries.

Format

config egress_access_profile [profile_id <value 1-4> | profile_name <name 1-32>] [add access_id [auto_assign | <value 1-128>] [ethernet {[vlan <vlan_name 32> | vlan_id <vlanid 1-4094>] {mask <hex 0x0-0x0fff>} | source_mac <macaddr> {mask <macmask>} | destination_mac <macaddr> {mask <macmask>} | 802.1p <value 0-7> | ethernet_type <hex 0x0-0xffff>} | ip {[vlan <vlan_name 32> | vlan_id <vlanid 1-4094>] {mask <hex 0x0-0x0fff>} | source_ip <ipaddr> {mask <netmask>} | destination_ip <ipaddr> {mask <netmask>} | dscp <value 0-63> | [icmp {type <value 0-255> | code <value 0-255>} | igmp {type <value 0-255>} | tcp {src_port <value 0-65535> {mask <hex 0x0-0xffff>} | dst_port <value 0-65535> {mask <hex 0x0-0xffff>} | flag [all | {urg | ack | psh | rst | syn | fin}]} | udp {src_port <value 0-65535> {mask <hex 0x0-0xffff>} | dst_port <value 0-65535> {mask <hex 0x0-0xffff>}} | protocol_id <value 0-255> {user_define <hex 0x0-0xffffffff> {mask <hex 0x0-0xffffffff>}}]} | ipv6 {class <value 0-255> | 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>}]}] [vlan_based [vlan <vlan_name 32> | vlan_id <vlanid 1-4094>] | port_group [id <value 1-64> | name <name 16>] | port <port>] [permit {replace_priority_with <value 0-7> | replace_dscp_with <value 0-63> | counter[enable | disable]} | deny] {time_range <range_name 32>} | delete access_id <value 1-128>]

Parameters

profile_id - Specify the index of the egress access list profile.
- **<value 1-4>** - Enter the profile ID used here. This value must be between 1 and 4. A lower value denotes a higher priority.

profile_name - Specify the name of the profile.
- **<name 1-32>** - Enter the profile name here. This name can be up to 32 characters long.

add - Specify to add a profile or rule.

access_id - Specify the index of the access list entry. If the auto_assign option is selected, the access ID is automatically assigned.
- **auto assign** - Specify that the access ID will be configured automatically.
- **<value 1-128>** - Enter the access ID used here. This value must be between 1 and 128.

ethernet - Specify an Ethernet egress ACL rule.

vlan - (Optional) Specify the VLAN name.
- **<vlan_name 32>** - Enter the VLAN name used for this configuration here. This name can be up to 32 characters long.

vlanid - Specify a VLAN ID.
- **<vlanid 1-4094>** - Enter the VLAN ID used for this congfiguration here. This value must be between 1 and 4094.

source_mac - (Optional) Specify the source MAC address.
- **<macaddr>** - Enter the source MAC address used here.
- **mask** - Specify that source MAC mask used.
  - **<macmask>** - Enter the source MAC mask value here.

destination_mac - Specify the destination MAC address.
- **<macaddr>** - Enter the destination MAC address used here.
- **mask** - Specify that destination MAC mask used.
  - **<macmask>** - Enter the destination MAC mask value here.

802.1p - (Optional) Specify the value of the 802.1p priority tag. The priority tag ranges from 1 to 7.
- **<value 0-7>** - Enter the 802.1p priority tag used here.

ethernet_type - (Optional) Specify the Ethernet type.
- **<hex 0x0-0xffff>** - Enter the Ethernet type mask used here.

ip - Specify an IP egress ACL rule.

vlan - (Optional) Specify the VLAN name.
- **<vlan_name 32>** - Enter the VLAN name used for this configuration here. This name can be up to 32 characters long.

vlanid - Specify a VLAN ID.

<vlanid 1-4094> - Enter the VLAN ID used for this congfiguration here. This value must be between 1 and 4094.
mask - (Optional) Specify the mask used. **<hex 0x0-x0fff>** - Enter the mask value used here.
source_ip - (Optional) Specify an IP source address. **<ipaddr>** - Enter the source IP address used here. **mask** - Specify the source IP address used here. **<netmask>** - Enter the source network mask here.
destination_ip - (Optional) Specify an IP destination address. **<ipaddr>** - Enter the destination IP address used here. **mask** - Specify the destination IP address used here. **<netmask>** - Enter the destination network mask here.
dscp - (Optional) Specify the value of DSCP. The DSCP value ranges from 0 to 63. **<value 0-63>** - Enter the DSCP value used here. This value must be between 0 and 63.
icmp - (Optional) Specify that the following parameters configured will apply to the ICMP configuration. **type** - Specify that the rule will apply to the ICMP type traffic value. **<value 0-255>** - Enter the ICMP traffic type value here. This value must be between 0 and 255. **code** - Specify 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) Specify that the following parameters configured will apply to the IGMP configuration. **type** - Specify 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 - (Optional) Specify that the following parameters configured will apply to the TCP configuration. **src_port** - Specify that the rule will apply to a range of TCP source ports. **<value 0-65535>** - Enter the source port value here. This value must be between 0 and 65535. **mask** - Specify the TCP source port mask here. **<hex 0x0-0xffff>** - Enter the TCP source port mask value here. **dst_port** - Specify that the rule will apply to a range of TCP destination ports. **<value 0-65535>** - Enter the destination port value here. This value must be between 0 and 65535. **mask** - Specify the TCP destination port mask here. **<hex 0x0-0xffff>** - Enter the TCP destination port mask value here.
flag - (Optional) Specify the TCP flag fields. **all** - Specify that the TCP flag field will be set to 'all'. **urg** - Specify that the TCP flag field will be set to 'urg'. **ack** - Specify that the TCP flag field will be set to 'ack'. **psh** - Specify that the TCP flag field will be set to 'psh'. **rst** - Specify that the TCP flag field will be set to 'rst'. **syn** - Specify that the TCP flag field will be set to 'syn'. **fin** - Specify that the TCP flag field will be set to 'fin'.
udp - (Optional) Specify that the following parameters configured will apply to the UDP configuration. **src_port** - Specify the UDP source port range. **<value 0-65535>** - Enter the UDP source port range value here. **mask** - Specify the UDP source port mask here. **<hex 0x0-0xffff>** - Enter the UDP source port mask value here. **dst_port** - Specify the UDP destination port range. **<value 0-65535>** - Enter the UDP destination port range value here. **mask** - Specify the UDP destination port mask here. **<hex 0x0-0xffff>** - Enter the UDP destination port mask value here.
protocod_id - (Optional) Specify that the rule will apply to the value of IP protocol ID traffic. **<value 0-255>** - Enter the protocol ID used here. This value must be between 0 and 255.
user_define - (Optional) Specify that the rule will apply to the IP protocol ID and that the mask

options behind the IP header, which has a length of 20 bytes. **<hex 0x0-0xffffffff>** - Enter the user-defined mask value here. **mask** - Specify the user-defined mask here. **<hex 0x0-0xffffffff>** - Enter the user-defined mask value here.
ipv6 - Specify the rule applies to IPv6 fields.
class - (Optional) Specify the value of IPv6 class. **<value 0-255>** - Enter the IPv6 class value here. This value must be between 0 and 255.
source_ipv6 - (Optional) Specify the value of IPv6 source address. **<ipv6addr>** - Enter the source IPv6 source address here. **mask** - Specify the IPv6 source address mask here. **<ipv6mask>** - Enter the IPv6 source address mask value here.
destination_ipv6 - (Optional) Specify the value of IPv6 destination address. **<ipv6addr>** - Enter the source IPv6 destination address here. **mask** - Specify the IPv6 destination address mask here. **<ipv6mask>** - Enter the IPv6 destination address mask value here.
tcp - (Optional) Specify the TCP protocol **src_port** - Specify the value of the IPv6 layer 4 TCP source port. **<value 0-65535>** - Enter the IPv6 TCP source port value here. This value must be between 0 and 65535. **mask** - Specify the IPv6 TCP source port mask here. **<hex 0x0-0xffff>** - Enter the IPv6 TCP source port mask value here. **dst_port** - Specify the value of the IPv6 layer 4 TCP destination port. **<value 0-65535>** - Enter the IPv6 TCP destination port value here. This value must be between 0 and 65535. **mask** - Specify the IPv6 TCP destination port mask here. **<hex 0x0-0xffff>** - Enter the IPv6 TCP destination port mask value here.
udp - (Optional) Specify the UDP protocol. **src_port** - Specify the value of the IPv6 layer 4 UDP source port. **<value 0-65535>** - Enter the IPv6 UDP source port value here. This value must be between 0 and 65535. **mask** - Specify the IPv6 UDP source port mask here. **<hex 0x0-0xffff>** - Enter the IPv6 UDP source port mask value here. **dst_port** - Specify the value of the IPv6 layer 4 UDP destination port. **<value 0-65535>** - Enter the IPv6 UDP destination port value here. This value must be between 0 and 65535. **mask** - Specify the IPv6 UDP destination port mask here. **<hex 0x0-0xffff>** - Enter the IPv6 UDP destination port mask value here.
icmp - (Optional) Specify that the following parameters configured will apply to the ICMP configuration. **type** - Specify that the rule will apply to the ICMP type traffic value. **<value 0-255>** - Enter the ICMP traffic type value here. This value must be between 0 and 255. **code** - Specify 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.
vlan_based - The rule applies on the specified VLAN.
vlan - Specify the VLAN name. **<vlan_name 32>** - Enter the VLAN name used for this configuration here. This name can be up to 32 characters long. **vlanid** - Specify a VLAN ID. **<vlanid 1-4094>** - Enter the VLAN ID used for this congfiguration here. This value must be between 1 and 4094.
port_group - Specify the port group value here. **id** - Specify the ID of the port group which the rule applies. **<value 1-64>** - Enter the group ID value here. This value must be between 1 and 64. **name** - Specify the name of the port group which the rule applies. **<name_string 16>** - Enter the port group name here. This name can be up to 16 characters long.
permit - Specify that packets matching the egress access rule are permitted by the Switch.
replace_priority_with - (Optional) Specify the packets that match the egress access rule are

changed the 802.1p priority tag field by the Switch. **<value 0-7>** - Enter the replace priority with value here. This value must be between 0 and 7. **replace_dscp_with** - (Optional) Specify the packets that match the egress access rule are changed the DSCP value by the Switch. **<value 0-63>** - Enter the replace DSCP with value here. This value must be between 0 and 63.
counter - (Optional) Specify 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** - Specify that the ACL counter feature will be enabled. **disable** - Specify that the ACL counter feature will be disabled.
deny - Specify the packets that match the egress access rule are filtered by the Switch.
time_range - (Optional) Specify the name of the time range entry. **<range_name 32>** - Enter the time range value here. This name can be up to 32 characters long.
delete - Specify to delete a profile or rule.
access_id - Specify the index of the access list entry. If the auto_assign option is selected, the access ID is automatically assigned. **<value 1-128>** - Enter the access ID used here. This value must be between 1 and 128. A lower value denotes a higher priority.

Restrictions

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

Example

To configure a port-base egress access rule that when the packet go out switch which match the specified source IP, DSCP and destination IP field, it will not be dropped:

```
DGS-3000-28SC:admin#  config egress_access_profile profile_id 2 add access_id
auto_assign ip source_ip 10.0.0.1 dscp 25 destination_ip 10.90.90.90 port_group
id 1 permit
Command: config egress_access_profile profile_id 2 add access_id auto_assign ip
source_ip 10.0.0.1 dscp 25 destination_ip 10.90.90.90 port_group id 1 permit


Success.


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

To configure a vlan-base egress access rule that when the packet go out switch which match the specified source MAC field, it will be dropped:

```
DGS-3000-28SC:admin#  config egress_access_profile profile_id 2 add access_id 1
ethernet source_mac 11-22-33-44-55-66 vlan_based vlan_id 1 deny
Command: config egress_access_profile profile_id 2 add access_id 1 ethernet
source_mac 11-22-33-44-55-66 vlan_based vlan_id 1 deny


Success.


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

7-3 config egress_flow_meter

Description

This command is used to configure the packet flow-based metering based on an egress access profile and rule.

Format

config egress_flow_meter [profile_id <value 1-4> | profile_name <name 1-32>] access_id <value 1-128> [rate <value 0-1048576> {burst_size <value 0-131072>} rate_exceed [drop_packet | remark_dscp <value 0-63>] | tr_tcm cir <value 0-1048576> {cbs <value 0-131072>} pir <value 0-1048576> {pbs <value 0-131072>} {[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 0-1048576> cbs <value 0-131072> ebs <value 0-131072> {[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 <value0-63>} | drop] {counter [enable | disable]} | delete]

Parameters

profile_id - Specify the index of the egress access list profile.
- **<value 1-4>** - Enter the profile ID used here. This value must be between 1 and 4. A lower value denotes a higher priority.

profile_name - Specify the name of the profile.
- **<name 1-32>** - Enter the profile name here. This name can be up to 32 characters long.

access_id - Specify the index of the access list entry. If the auto_assign option is selected, the access ID is automatically assigned.
- **<value 1-128>** - Enter the access ID used here. This value must be between 1 and 128.

rate - Specify the rate for single rate two-color mode.
- **<value 0-1048576>** Enter the rate ID used here.

burst_size - (Optional) Specify the burst size for the single rate “two color” mode. The unit is Kbytes.
- **<value 0-131072>** - Enter the burst size here.

rate_exceed - Specify the action for packets that exceed the committed rate in single rate “two color” mode.
- **drop_packet** - (Optional) Specify to drop the packet immediately.
- **remark_dscp** - (Optional) Specify the packet with DSCP. The packet is set to have the higher drop precedence.
  - **<value 0-63>** - Enter a packet value.

tr_tcm - Specify the “two rate three color mode”.
- **cir** - Specify the Committed Information Rate.
  - **<value 0-1048576>** - Enter the Committed Information Rate in Kbps. The maximum rate is determined by the project. CIR should always be equal or less than.
- **cbs** - Specify the “Committed Burst Size”. The unit is Kbytes. That is to say, 1 means 1Kbytes
  - **<value 0-131072>** - Enter the Committed Burst Size here.
- **pir** - Specify the “Peak Information Rate”. The unit is in Kbps. The maximum rate is determined by the project. PIR should always be equal to or greater than CIR.
  - **<value 0-1048576>** - Enter the PIR value here.
- **pbs** – (Optional) Specify the “Peak Burst Size”. The unit is in Kbytes. . The default value is 4*1024
  - **<value 0-131072>** - Enter the PBZ value here.

color_blind - Specify the meter mode: color-blind. The default is color-blind mode.

color_aware - Specify the meter mode: color-aware. The final color of packet is determined by the initial color of packet and the metering result.

conform - Specify the action when packet is in “green color”.

permit - Specify to permit the packet.
replace_dsp - Specify to change the DSCP of the packet.
<value 0-63> - Enter a DSCP packet value.

counter - (Optional) Specify the ACL counter. The resource may be limited so that a counter cannot be turned on. The limitation is project dependent. Counters will be cleared when the function is disabled.
enable - Specify to enable the ACL counter.
disable - Specify to disable the ACL counter.

exceed - Specify the action when packet is in “yellow color”.
permit - Specify to permit the packet.
replace_dsp - Specify to change the DSCP of the packet.
<value 0-63> - Enter a packet value between 0 and 63.
drop - Specify to drop the packet.

counter – (Optional) Specify the ACL counter. The resource may be limited so that a counter cannot be turned on. The limitation is project dependent. Counters will be cleared when the function is disabled.
enable - Specify to enable the ACL counter.
disable - Specify to disable the ACL counter.

violate - (Optional) Specify an IP destination address.
permit - Specify to permit the packet.
replace_dsp - Specify to change the DSCP of the packet.
<value 0-63> - Enter a packet value between 0 and 63.

drop - (Optional) Specify to drop the packet.
counter – (Optional) Specify the ACL counter. The resource may be limited so that a counter cannot be turned on. The limitation is project dependent. Counters will be cleared when the function is disabled.
enable - Specify to enable the ACL counter.
disable - Specify to disable the ACL counter.

sr_tcm - (Optional) Specify the “single rate three color mode”.
cir - Specify the “committed information rate”. The unit is Kbps.
<value 0-1048576> - Enter the single rate three color mode value here.
cbs - Specify the “committed burst size”. The unit is Kbytes
<value 0-131072> - Enter the commited burst size rate here.
ebs - Specify the “Excess Burst Size”. The unit is Kbytes.
<value 0-131072> - Enter the excess burst size here.
color_blind - Specify the meter mode: color-blind. The default is color-blind mode.
color_aware - Specify the meter mode: color-aware. The final color of packet is determined by the initial color of packet and the metering result.
conform - Specify the action when packet is in “green color”.
permit - Specify to permit the packet.
replace_dsp - Specify to change the DSCP of the packet.
<value 0-63> - Enter a DSCP packet value.
counter - (Optional) Specify the ACL counter. The resource may be limited so that a counter cannot be turned on. The limitation is project dependent. Counters will be cleared when the function is disabled.
enable - Specify to enable the ACL counter.
disable - Specify to disable the ACL counter

exceed - (Specify the action when packet is in “yellow color”.
permit - Specify to permit the packet.
replace_dsp - Specify to change the DSCP of the packet.
<value 0-63> - Enter a DSCP packet value.

drop - (Optional) Specify to drop the packet.
counter – (Optional) Specify the ACL counter. The resource may be limited so that a counter cannot be turned on. The limitation is project dependent. Counters will be cleared when the function is disabled.
enable - Specify to enable the ACL counter.
disable - Specify to disable the ACL counter.

violate - (Optional) Specify an IP destination address.
permit - Specify to permit the packet.
replace_dsp - Specify to change the DSCP of the packet.

<value 0-63> - Enter a packet value between 0 and 63.
drop - (Optional) Specify to drop the packet.
counter – (Optional) Specify the ACL counter. The resource may be limited so that a counter cannot be turned on. The limitation is project dependent. Counters will be cleared when the function is disabled. **enable** - Specify to enable the ACL counter. **disable** - Specify to disable the ACL counter.
delete – Specify to delete the specified “flow_meter”.
permit - Specify that packets matching the egress access rule are permitted by the Switch.

Restrictions

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

Example

To configure a “two rates three color” flow meter:

```
DGS-3000-28SC:admin# config egress_flow_meter profile_id 1 access_id 1
tr_tcm cir 1000 cbs 200 pir 2000 pbs 200 exceed permit replace_dscp 21 violate
drop
command: config egress_flow_meter profile_id 1 access_id 1
tr_tcm cir 1000 cbs 200 pir 2000 pbs 200 exceed permit replace_dscp 21 violate
drop


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

7-4 config port_group

Description

This command is used to add or delete a port list to a port group.

Format

config port_group [id <value 1-64> | name <name 16>] [add | delete] [<portlist> | all]

Parameters

id - Specify the port group ID, the max ID is depended by project. **<value 1-64>** - Enter the profile ID here. This value must be between 1 and 64. A lower value denotes a higher priority.
name - Specify the port group name. The maximum length is 16 characters. **<name 16>** - Enter the profile name here. This name can be up to 16 characters long.
add - Specify to add a port list to this port group.
delete - Specify to delete a port list from this port group.
portlist - Specify the port list.
all - Specify all the ports.

Restrictions

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

Example

To add a port list “1-3” to the port group which ID is “2”:

```
DGS-3000-28SC:admin# config port_group id 2 add 1-3
Command: config port_group id 2 add 1-3

Success.

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

7-5 show current_config egress_access_profile

Description

This command is used to display the egress ACL part of current configuration in user level of privilege.

The overall current configuration can be displayed by “show config” command which is accessible in administrator level of privilege.

Format

show current_config egress_access_profile

Parameters

None.

Restrictions

None.

Example

To display current configuration of egress access list table:

```
DGS-3000-28SC:admin# show current_config egress_access_profile
Command: show current_config egress_access_profile

#------------------------------------------------------------------------

# Egress ACL

create egress_access_profile profile_id 1 profile_name 1 ethernet source_mac
FF-
FF-FF-FF-FF-FF
config egress_access_profile profile_id 1 add access_id 1 ethernet source_mac
00
-00-00-00-01 vlan_based vlan_id 1 permit
create egress_access_profile profile_id 2 profile_name 2 ip source_ip_mask
255.2
55.255.255 destination_ip_mask 255.255.255.255 dscp
config egress_access_profile profile_id 2 add access_id auto_assign ip
source_ip
 10.0.0.2 destination_ip 10.90.90.90 dscp 25 port_group id 1 permit counter
enable
config egress_access_profile profile_id 2 add access_id auto_assign ip
source_ip
 10.0.0.1 destination_ip 10.90.90.90 dscp 25 port_group id 1  permit

#------------------------------------------------------------------------

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

7-6 show egress_access_profile

Description

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

Format

show egress_access_profile {[profile_id <value 1-4> | profile_name <name 1-32>]}

Parameters

profile_id - (Optional) Specify the index of the egress access list profile. **<value 1-4>** - Enter the profile ID here. This value must be between 1 and 4. A lower value denotes a higher priority.
profile_name - (Optional) Specify the name of the profile. The maximum length is 32 characters. **<name 1-32>** - Enter the profile name here. This name can be up to 32 characters long.
If no parameter is specified, will show the all egress access profile.

Restrictions

None.

Example

To display current egress access list table:

```
DGS-3000-28SC:admin#show egress_access_profile
Command: show egress_access_profile

Egress Access Profile Table

Total User Set Rule Entries : 3
Total Used HW Entries       : 4
Total Available HW Entries  : 508

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

MASK on
    VLAN            : 0xFFF
    802.1p

Available HW Entries : 127
--------------------------------------------------------------------------------
Rule ID : 1    (auto assign)    Ports: 1:1

Match on
    802.1p          : 0

Action:
    Permit

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


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

MASK on
    DSCP
    ICMP

Available HW Entries : 127
--------------------------------------------------------------------------------
Rule ID : 1    (auto assign)    Ports: 1:3

Match on
    DSCP            : 3

Action:
    Permit

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


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

```
MASK on
    Class

Available HW Entries : 126
-------------------------------------------------------------------------------
Rule ID : 1    (auto assign)    Ports: 1:4

Match on
    Class           : 10

Action:
    Permit

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



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

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

```
DGS-3000-28SC:admin#show egress_access_profile profile_id 1
Command: show egress_access_profile profile_id 1

Egress Access Profile Table

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

MASK on
    VLAN            : 0xFFF
    802.1p

Available HW Entries : 127
-------------------------------------------------------------------------------
Rule ID : 1    (auto assign)    Ports: 1:1

Match on
    802.1p          : 0

Action:
    Permit

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


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

7-7 show egress_flow_meter

Description

This command is used to display the egress flow-based metering configuration.

Format

show egress_flow_meter {[profile_id <value 1-4> | profile_name <name 1-32>] {access_id <value 1-128>}}

Parameters

profile_id - (Optional) Specify the index of access list profile. **<value 1-4>** - Enter the profile ID used here. This value must be between 1 and 4. A lower value denotes a higher priority.
profile_name - (Optional) Specify the name of the profile. **<name 1-32>** - Enter the profile name used here. This name can be up to 32 characters long.
access_id - (Optional) Specify the access ID. **<value 1-128>** - Enter the access ID used here. This value must be between 1 and 128. A lower value denotes a higher priority.

Restrictions

None.

Example

To display current egress flow meter table:

```
DGS-3000-28SC:admin#  show egress_flow_meter
Command: show egress_flow_meter

Flow Meter Information
------------------------------------------------------------------------------
Profile ID:1     Aceess ID:1     Mode : trTCM / ColorAware
CIR(Kbps):1000     CBS(Kbyte):1000     PIR(Kbps):2000     PBS(Kbyte):2000
Action:
      Conform : Permit                        Counter: Enabled
       Exceed : Drop                          Counter: Enabled
      Violate : Drop                          Counter: Disabled
------------------------------------------------------------------------------
Profile ID:1     Aceess ID:2     Mode : srTCM / ColorBlind
CIR(Kbps):1000     CBS(Kbyte):100      EBS(Kbyte):200
Action:
      Conform : Permit                        Counter: Enabled
       Exceed : Permit     Replace DSCP: 60   Counter: Enabled
      Violate : Drop                          Counter: Disabled
------------------------------------------------------------------------------

Total Entries: 2

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

7-8 create port_group id

Description

This command is used to create a port group.

Format

create port_group id <value 1-64> name <name 16>

Parameters

<value 1-64> - Enter the port group ID here. This value must be between 1 and 64.
name - Specify the port group name. **<name 16>** - Enter the port group name here. This name can be up to 16 characters long.

Restrictions

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

Example

To create a port group:

```
DGS-3000-28SC:admin#  create port_group id 2 name group2
Command: create port_group id 2 name group2

Success.

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

7-9 show port_group

Description

This command is used to display the port group information.

Format

show port_group {id <value 1-64> | name <name 16>}

Parameters

id - (Optional) Specify the port group ID. **<value 1-64>** - Enter the port group ID used here. This value must be between 1 and 64.
name - (Optional) Specify the port group name. **<name 16>** - Enter the port group name here. This name can be up to 16 characters long.
If no parameter is specified, all the port groups will be displayed.

Restrictions

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

Example

To show all the port group information:

```
DGS-3000-28SC:admin#  show port_group
Command: show port_group

Port Group Table
--------------------------------------------
Port Group ID     Port Group Name      Ports
2                  group2               1:1-1:3

Total Entries :1

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

7-10 delete egress_access_profile

Description

This command is used to delete egress access profile command can only delete the profile which is created by egress ACL module.

Format

delete egress_access_profile [profile_id <value 1-4> | profile_name <name 1-32> | all]

Parameters

profile_id - Specify the index of the egress access list profile. **<value 1-4>** - Enter the profile ID used here. This value must be between 1 and 4.
profile_name - Specify the name of the profile. The maximum length is 32 characters. **<name 1-32>** - Enter the profile name used here. This name can be up to 32 characters long.
all - Specify that the whole egress access list profile will be deleted.

Restrictions

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

Example

To delete egress access list profile ID 1:

```
DGS-3000-28SC:admin#  delete egress_access_profile profile_id 1
Command: delete egress_access_profile profile_id 1

Success.

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

7-11 delete port_group

Description

This command is used to delete a port group.

Format

delete port_group [id <value 1-64> | name <name 16>]

Parameters

id - Specify the port group ID. **<value 1-64>** - Enter the port group ID used here. This value must be between 1 and 64.
name - Specify the port group name. **<name 16>** - Enter the port group name here. This name can be up to 16 characters long.

Restrictions

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

Example

To delete egress access list profile ID 1:

```
DGS-3000-28SC:admin#  delete port_group id 2
Command: delete port_group id 2

Success.

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

Chapter 8 Address Resolution Protocol (ARP) Command List

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

8-1 create arpentry

Description

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

Format

create arpentry <ipaddr> <macaddr>

Parameters

<ipaddr> - Enter the end node or station IP address.
<macaddr> - Enter the corresponding MAC address of 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-3000-28SC:admin#create arpentry 10.48.74.121 00-50-BA-00-07-36
Command: create arpentry 10.48.74.121 00-50-BA-00-07-36

Success.

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

8-2 delete arpentry

Description

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

Format

delete arpentry [<ipaddr> | all]

Parameters

<ipaddr> - Enter the end node or station IP address.
all - Specify 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-3000-28SC:admin#delete arpentry 10.48.74.121
Command: delete arpentry 10.48.74.121

Success.

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

8-3 config arpentry

Description

This command is used to configure a static entry's MAC address in the ARP table. Specify the IP address and MAC address of the entry.

Format

config arpentry <ipaddr> <macaddr>

Parameters

<ipaddr> - Enter the end node or station IP address.
<macaddr> - Enter the corresponding MAC address of 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-3000-28SC: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-3000-28SC:admin#
```

8-4 config arp_aging time

Description

This command is used to set the maximum amount of time, in minutes, that a dynamic ARP entry can remain in the Switch's ARP table, without being accessed, before it is dropped from the table.

Format

config arp_aging time <min 0-65535>

Parameters

<min 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-3000-28SC:admin#config arp_aging time 30
Command: config arp_aging time 30

Success.

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

8-5 clear arptable

Description

This command is used to clear all the dynamic entries from ARP table.

Format

clear arptable

Parameters

None.

Restrictions

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

Example

To clear the ARP table:

```
DGS-3000-28SC:admin#clear arptable
Command: clear arptable

Success.

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

8-6 show arpentry

Description

This command is used to display the ARP table. You can filter the display by IP address, MAC address, Interface name, or static entries.

Format

show arpentry {ipif <ipif_name 12> | ipaddress <ipaddr> | static | mac_address <macaddr>}

Parameters

ipif - (Optional) 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-3000-28SC: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-3000-28SC:admin#
```

Chapter 9 ARP Spoofing Prevention Command List

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

9-1 config arp_spoofing_prevention

Description

This command is used to configure the spoofing prevention entry to prevent spoofing of MAC 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 - Specify to add an ARP spoofing prevention entry. **gateway_ip** - Specify a gateway IP address to be configured. **<ipaddr>** - Enter the IP address used for this configuration here. **gateway_mac** - Specify a gateway MAC address to be configured. **<macaddr>** - Enter the MAC address used for this configuration here. **ports** - Specify a range of ports to be configured. **<portlist>** - Enter a list of ports used for the configuration here. **all** - Specify all of ports to be configured.
delete - Specify to delete an ARP spoofing prevention entry. **gateway_ip** - Specify a gateway ip to be configured. **<ipaddr>** - Enter the IP address used for this configuration here.

Restrictions

Only Administrators, Operators and Power User's can issue this command.

Example

To configure the ARP spoofing prevention entry:

```
DGS-3000-28SC:admin#config arp_spoofing_prevention add gateway_ip
10.254.254.251gateway_mac 00-00-00-11-11-11 ports 1-2
Command: config arp_spoofing_prevention add gateway_ip 10.254.254.251
gateway_mac 00-00-00-11-11-11 ports 1-2

Success.

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

9-2 show arp_spoofing_prevention

Description

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

Format

show arp_spoofing_prevention

Parameters

None.

Restrictions

None.

Example

To display the ARP spoofing prevention entries:

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

Chapter 10 Asymmetric VLAN Command List

enable asymmetric_vlan
disable asymmetric_vlan
show asymmetric_vlan

10-1 enable asymmetric_vlan

Description

This command is used to enable the asymmetric VLAN function on the Switch.

Format

enable asymmetric_vlan

Parameters

None.

Restrictions

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

Example

To enable asymmetric VLANs:

```
DGS-3000-28SC:admin# enable asymmetric_vlan
Command: enable asymmetric_vlan

Success.

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

10-2 disable asymmetric_vlan

Description

This command is used to disable the asymmetric VLAN function on the Switch.

Format

disable asymmetric_vlan

Parameters

None.

Restrictions

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

Example

To disable asymmetric VLANs:

```
DGS-3000-28SC:admin# disable asymmetric_vlan
Command: disable asymmetric_vlan

Success.

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

10-3 show asymmetric_vlan

Description

This command is used to display the asymmetric VLAN state on the Switch.

Format

show asymmetric_vlan

Parameters

None.

Restrictions

None.

Example

To display the asymmetric VLAN state currently set on the Switch:

```
DGS-3000-28SC:admin# show asymmetric_vlan
Command: show asymmetric_vlan

Asymmetric VLAN: Enabled

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

Chapter 11 Auto-Configuration Command List

enable autoconfig
disable autoconfig
show autoconfig

11-1 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-3000-28SC:admin#enable autoconfig
Command: enable autoconfig

Success.

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

11-2 disable autoconfig

Description

This command is used to disable auto configuration. When disabled, the Switch will configure itself using the local configuration file

Format

disable autoconfig

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To disable autoconfig:

```
DGS-3000-28SC:admin#disable autoconfig
Command: disable autoconfig

Success.

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

11-3 show autoconfig

Description

This command is used to display if the auto-configuration is enabled or disabled.

Format

show autoconfig

Parameters

None.

Restrictions

None.

Example

To show autoconfig status:

```
DGS-3000-28SC:admin#show autoconfig
Command: show autoconfig

Autoconfig State: Disabled

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

Chapter 12 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>}}

12-1 config bpdu_protection ports

Description

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

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

Format

config bpdu_protection ports [<portlist> | all] {state [enable | disable] | mode [drop | block | shutdown]}(1)

Parameters

<portlist> - Enter a range of ports to be configured (port number).
all - Specify that all the port will be configured.
state - Specify the BPDU protection state. The default state is disable. **enable** - Specify to enable BPDU protection. **disable** - Specify to disable BPDU protection.
mode - Specify the BPDU protection mode. The default mode is shutdown. **drop** - Specify to drop all received BPDU packets when the port enters under_attack state. **block** - Specify to drop all packets including BPDU and normal packets when the port enters under_attack state. **shutdown** - Specify to shut down the port when the port enters under_attack state.

Restrictions

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

Example

To set the port state enable and drop mode:

```
DGS-3000-28SC:admin#config bpdu_protection ports 1 state enable mode drop
Commands: config bpdu_protection ports 1 state enable mode drop

Success.

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

12-2 config bpdu_protection recovery_timer

Description

This command is used to configure BPDU protection recovery timer. When a port enters the 'under attack' state, it can be disabled or blocked based on the configuration. The state can be recovered manually or by the auto recovery mechanism. To manually recover the port, the user needs to disable and re-enable the port.

Format

config bpdu_protection recovery_timer [<sec 60-1000000> | infinite]

Parameters

<sec 60 –1000000> - Enter the timer (in seconds) used by the Auto-Recovery mechanism to recover the port. The valid range is 60 to 1000000.
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-3000-28SC:admin#config bpdu_protection recovery_timer 120
Commands: config bpdu_protection recovery_timer 120

Success.

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

12-3 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 - Specify the trap state.
log - Specify 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-3000-28SC:admin#config bpdu_protection trap both
Commands: config bpdu_protection trap both

Success.

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

12-4 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-3000-28SC:admin#enable bpdu_protection
Commands: enable bpdu_protection

Success.

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

12-5 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-3000-28SC:admin#disable bpdu_protection
Commands: disable bpdu_protection

Success.

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

12-6 show bpdu_protection

Description

This command is used to display BPDU protection global configuration or per port configuration and current status.

Format

show bpdu_protection {ports {<portlist>}}

Parameters

ports - (Optional) Specify 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-3000-28SC: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-3000-28SC:admin#
```

To show the bpdu_protection status ports 1-12:

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

Chapter 13 Cable Diagnostics Command List

cable_diag ports [<portlist> | all]

13-1 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 l**ink partner is powered down with no errors** and the **link is down**, this command cannot detect the cable length
- When the **link partner is powered down with errors**, this command can detect whether the error is open, short, or crosstalk. In this case this command can also detect the distance of the error
- When there is **no link partner** with **no errors** and the **link is up**, this command can detect the cable length
- When there is **no link partner with errors**, this command can detect whether the error is open, short, or crosstalk. In this case this command can also detect the distance of the error

When the link partner is Gigabit Ethernet ports:

- Where the **link partner is powered on with no errors** and the **link is up**, this command can detect the cable length
- Where the **link partner is powered on with errors**, this command can detect whether the error is open, short, or crosstalk. In this case this command can also detect the distance of the error
- Where the **link partner is powered down with no errors** and the **link is down**, this command cannot detect the cable length
- When the **link partner is powered down with errors**, this command can detect whether the error is open, short, or crosstalk. In this case this command can also detect the distance of the error
- When there is **no link partner with no errors** and the **link is up**, this command can detect the cable length
- When there is **no link partner with errors**, this command can detect whether the error is open, short, or crosstalk. In this case this command can also detect the distance of the error

NOTE: This test is only for copper cable. The fiber port is not tested. For the combo ports, only the copper media will be tested. The cable diagnosis does not support on the Pair 1 and 4 if the link partner is FE port. If the link partner is FE port, the target port's link will be down after the test.

Format

cable_diag ports [<portlist> | all]

Parameters

<portlist> - Enter a list of ports used for the configuration here.
all - Specify 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-3000-28SC: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-3000-28SC:admin#
```

Chapter 14 Command Logging Command List

enable command logging
disable command logging
show command logging

14-1 enable command logging

Description

This command is used to enable the command logging function. This is disabled by default.

NOTE: When the Switch is under booting procedure, all configuration command should not be logged. When the user under AAA authentication, the user name should not changed if user uses “enable admin” command to replace its privilege.

Format

enable command logging

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To enable the command logging function:

```
DGS-3000-28SC:admin#enable command logging
Command: enable command logging

Success.

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

14-2 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-3000-28SC:admin#disable command logging
Command: disable command logging

Success.

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

14-3 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

None.

Example

To show the command logging configuration status:

```
DGS-3000-28SC:admin#show command logging
Command: show command logging

Command Logging State : Disabled

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

Chapter 15 Compound Authentication Command List

create authentication guest_vlan [vlan <vlan_name 32> | vlanid <vlanid 1-4094>]
enable authorization attributes
delete authentication guest_vlan [vlan <vlan_name 32> | vlanid <vlanid 1-4094>]
disable authorization attributes
config authentication guest_vlan [vlan <vlan_name 32> | vlanid <vlanid 1-4094>] [add | delete] ports [<portlist> | all]
config authentication mac_format {case [lowercase | uppercase] | delimiter {[hyphen | colon | dot | none] | number [1 | 2 | 5]}(1)} (1)
config authentication ports [<portlist> | all] {auth_mode [port_based | host_based {vlanid <vid_list> state [enable | disable]}] | multi_authen_methods [none | any | dot1x_impb | impb_wac | mac_impb | mac_wac]}(1)
config authentication server failover [local | permit | block]
show authorization
show authentication
show authentication guest_vlan
show authentication mac_format
show authentication ports {<portlist>}

15-1 create authentication guest_vlan

Description

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

Format

create authentication guest_vlan [vlan <vlan_name 32> | vlanid <vlanid 1-4094>]

Parameters

vlan - Specify the guest VLAN by VLAN name. **<vlan_name 32>** - Enter the guest VLAN by VLAN name. The VLAN name can be up to 32 characters long.
vlanid - Specify the guest VLAN by VLAN ID. **<vlanid 1-4094>** - Enter the guest VLAN by VLAN ID. The VLAN ID value must be between 1 and 4094.

Restrictions

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

Example

To assign a static VLAN to be a guest VLAN:

```
DGS-3000-28SC:admin#create authentication guest_vlan vlan guestVLAN
Command: create authentication guest_vlan vlan guestVLAN

Success.

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

15-2 enable authorization attributes

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-3000-28SC:admin#enable authorization attributes
Command: enable authorization attributes

Success.

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

15-3 delete authentication guest_vlan

Description

This command is used to delete guest VLAN setting, but won't delete the static VLAN.

All ports which enable guest VLAN will move to original VLAN after deleting guest VLAN.

Format

delete authentication guest_vlan [vlan <vlan_name 32> | vlanid <vlanid 1-4094>]

Parameters

vlan - Specify the guest VLAN by VLAN name. **<vlan_name 32>** - Enter the VLAN name here. This name can be up to 32 characters long.
vlanid - Specify the guest VLAN by VLAN ID. **<vlanid 1-4094>** - Enter the VLAN ID here. This ID must be between 1 and 4094.

Restrictions

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

Example

To delete guest VLAN configuration:

```
DGS-3000-28SC:admin# delete authentication guest_vlan vlan guestVLAN
Command: delete authentication guest_vlan vlan guestVLAN

Success.

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

15-4 disable authorization attributes

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-3000-28SC:admin#disable authorization attributes
Command: disable authorization attributes

Success.

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

15-5 config authentication guest_vlan

Description

This command is used to assign or remove ports to or from a guest VLAN.

Format

config authentication guest_vlan [vlan <vlan_name 32> | vlanid <vlanid 1-4094>] [add | delete] ports [<portlist> | all]

Parameters

vlan - Specify the guest VLAN name. **<vlan_name 32>** - Enter the guest VLAN name. The VLAN name can be up to 32 characters long.
vlanid - Specify the guest VLAN VID. **<vlanid 1-4094>** - Enter the guest VLAN VID. The VLAN ID value must be between 1 and 4094.
add - Specify to add a port list to the guest VLAN.
delete - Specify to delete a port list from the guest VLAN.
ports - Specify a port or range of ports to configure. **<portlist>** - Enter a range of ports to configure. **all** - Specify to configure all ports.

Restrictions

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

Example

To configure authentication for all ports for a guest VLAN called “gv”:

```
DGS-3000-28SC:admin#config authentication guest_vlan vlan gv add ports all
Command: config authentication guest_vlan vlan gv add ports all

Success.

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

15-6 config authentication mac_format

Description

This command is used to set the MAC address format that will be used for authentication username via the RADIUS server.

Format

config authentication mac_format {case [lowercase | uppercase] | delimiter {[hyphen | colon | dot | none] | number [1 | 2 | 5]}(1)}(1)

Parameters

case - Specify the case format used. **lowercase** - Specify using the lowercase format, the RADIUS authentication username will be formatted as: aa-bb-cc-dd-ee-ff. **uppercase** - Specify using the uppercase format, the RADIUS authentication username will be formatted as: AA-BB-CC-DD-EE-FF.
delimiter - Specify the delimiter format used. **hyphen** - Specify using the "-" as delimiter, the format is: AA-BB-CC-DD-EE-FF **colon** - Specify using the ":" as delimiter, the format is: AA:BB:CC:DD:EE:FF **dot** - Specify using the "." as delimiter, the format is: AA.BB.CC.DD.EE.FF **none** - Specify not using any delimiter, the format is: AABBCCDDEEFF
number - Specify the delimiter number used. **1** - Single delimiter, the format is: AABBCC.DDEEFF **2** - Double delimiter, the format is: AABB.CCDD.EEFF **5** - Multiple delimiter, the format is: AA.BB.CC.DD.EE.FF

Restrictions

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

Example

To configure the MAC address format to IETF style:

```
DGS-3000-28SC:admin#config authentication mac_format case uppercase delimiter
hyphen number 5
Command: config authentication mac_format case uppercase delimiter hyphen
number 5

Success.

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

15-7 config authentication ports

Description

This command is used to configure authorization mode and authentication method on ports.

Format

config authentication ports [<portlist> | all] {auth_mode [port_based | host_based {vlanid <vid_list> state [enable | disable]}] | multi_authen_methods [none | any | dot1x_impb | impb_wac | mac_impb| | mac_wac]}(1)

Parameters

<portlist> - Enter a port or range of ports to configure.

all - Specify to configure all ports.

auth_mode - The authorization mode is port-based or host-based.

- **port-based** - If one of the attached hosts pass the authentication, all hosts on the same port will be granted access to the network. If the user fails the authentication, this port will keep trying the next authentication.
- **host-based** - Specify to allow every user to be authenticated individually. The "vlanid" can authenticate the client on a specific authenticated VLAN(s).If the "vlanid" is not specified, or all the VLANs are disabled, it means the host does not care which VLAN the client comes from. The client will be authenticated if the client's MAC address (regardless of the VLAN) is not authenticated.
  - **vlanid** - (Optional) Specify the VLAN ID used for this configuration.
    - **<vid_list>** - Enter the VLAN ID used for this configuration here.
  - **state** - (Optional) Specify whether the authentication mode will be enabled or disabled on a specified VLAN.
    - **enable** - Specify that the authentication mode will be enabled on the specified VLAN.
    - **disable** - Specify that the authentication mode will be disabled on the specified VLAN.

multi_authen_methods - Specify the compound authentication method. (If the compound authentication method selected includes IMPB(ex: dot1x_impb, impb_wac, mac_impb) and the other method (802.1X, WAC or MAC) is globally disabled, only IMPB will be used. If the mac_wac option is selected, both authentication methods will be applied. If one of the authentication methods fails or is globally disabled, then access will be denied.)

- **none** - Specify that compound authentication is not enabled.
- **any** - Specify if any of the authentication methods (802.1X, MAC, and WAC) pass, then pass.
- **dot1x_impb** – 802.1X will be verified first, and then IMPB will be verified. Both authentications need to be passed.
- **impb_wac** - WAC will be verified first, and then IMPB will be verified. Both authentications need to be passed.
- **mac_impb** - MAC will be verified first, and then IMPB will be verified. Both authentications need to be passed.
- **mac_wac** - MAC will be verified first followed by WAC. Both authentication methods need to be passed.

Restrictions

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

Example

The following example sets the authentication mode of all ports to host-based:

```
DGS-3000-28SC:admin#config authentication ports all auth_mode host_based
Command: config authentication ports all auth_mode host_based

Success.

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

The following example sets the compound authentication method of all ports to “any”:

```
DGS-3000-28SC:admin#config authentication ports all multi_authen_methods any
Command: config authentication ports all multi_authen_methods any

Success.

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

15-8 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-3000-28SC:admin#config authentication server failover local
Command: config authentication server failover local

Success.

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

15-9 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-3000-28SC:admin#show authorization
Command: show authorization

Authorization for Attributes: Enabled.

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

15-10 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-3000-28SC:admin#show authentication
Command: show authentication

Authentication Server Failover: Block.

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

15-11 show authentication guest_vlan

Description

This command is used to display guest VLAN information.

Format

show authentication guest_vlan

Parameters

None.

Restrictions

None.

Example

To display the guest VLAN setting:

```
DGS-3000-28SC:admin#show authentication guest_vlan
Command: show authentication guest_vlan

Guest VLAN VID         :
Guest VLAN Member Ports:

 Total Entries: 0

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

15-12 show authentication mac_format

Description

This command is used to display the authentication MAC format setting.

Format

show authentication mac_format

Parameters

None.

Restrictions

None.

Example

To display the authentication MAC format setting:

```
DGS-3000-28SC:admin#show authentication mac_format
Command: show authentication mac_format

 Case              : Uppercase
 Delimiter         : None
 Delimiter Number  : 5

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

15-13 show authentication ports

Description

This command is used to display the authentication method and authorization mode on ports.

Format

show authentication ports {<portlist>}

Parameters

<portlist> - (Optional) Enter to display compound authentication on specific port(s).

Restrictions

None.

Example

To display the authentication settings for ports 1 to 3:

```
DGS-3000-28SC:admin#show authentication ports 1-3
Command: show authentication ports 1-3

 Port  Methods        Auth Mode  Authentication VLAN(s)
 ---- -------------- ----------- ----------------------
 1    None           Host-based
 2    None           Host-based
 3    None           Host-based

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

Chapter 16 Configuration Command List

show config [effective | modified | current_config | boot_up | information | file <pathname>] {[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 {unit <unit_id>} <pathname> [boot_up | active]
save config {[config <pathname> | log | all]}
show boot_file
config configuration trap {save [enable | disable] | upload [enable | disable] | download [enable | disable]}

16-1 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 | information | file <pathname>] {[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.

modified - Shows only the commands which are not default setting.
current_config - Specify the current configuration.
boot_up - Specify the list of the boot-up configuration.
information - Specify the current config information.
file - Specify to display the configuration file. **<pathname>** - Enter an absolute pathname on the device file system. If pathname is not specified, the boot-up configuration is implied.
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-3000-28SC:admin#show config modified
Command: show config modified

#------------------------------------------------------------------------
#                    DGS-3000-28SC Gigabit Ethernet Switch
#                                Configuration
#
#                           Firmware: Build 5.00.020
#           Copyright(C) 2014 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
```

16-2 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 {unit <unit_id>} <pathname> [boot_up | active]

Parameters

unit - (Optional) Specify which unit on the stacking system. If it is not specified, it refers to the master unit. **<unit_id>** - Enter the unit ID value. This value must be between 1 and 6.
<pathname> - Specify a configuration file on the device file system.
boot_up - Specify it as a boot up file.
active - Specify to apply the configuration.

Restrictions

Only Administrators can issue this command.

Example

To configure the Switch's configuration file as boot-up:

```
DGS-3000-28SC:admin# config configuration config.cfg boot_up
Command: config configuration config.cfg boot_up

Success.

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

16-3 save configuration

Description

This command is used to save the current configuration to a file.

Format

save config {[config <pathname> | log | all]}

Parameters

config - (Optional) Specify the configuration file name. **<pathname>** - Enter a configuration file on the device file system.
log - (Optional) Specify the log to save the configuration
all - (Optional) Specify all to apply the configuration.

Restrictions

Only Administrators can issue this command.

Example

To save the current configuration to a file:

```
DGS-3000-28SC:admin# save config
Command: save config

Saving configurations.......... Done.

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

16-4 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-3000-28SC:admin#show boot_file
Command: show boot_file

  Boot-up Firmware       : /c:/runtime.had
  Boot-up Configuration  : /c:/config.cfg

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

16-5 config configuration trap

Description

This command is used to configure the trap status of configuration saving completed, configuration uploading completed and configuration downloading completed.When set to enabled, the SNMP Agent will send a trap while the related operation (save / upload / download the configuration) is successfully completed.

Format

config configuration trap {save [enable | disable] | upload [enable | disable] | download [enable | disable]}

Parameters

save - (Optional) Enable or disable sending the trap by the SNMP agent when the configuration is saved in NVRAM. **enable** - Send the trap by the SNMP agent when the configuration is saved in NVRAM. **disable** - No trap will be send.
upload - (Optional) Enable or disable sending the trap by the SNMP agent when successfully uploading configuration. **enable** - Send the trap by the SNMP agent when successfully uploading configuration. **disable** - No trap will be send.
download - (Optional) Enable or disable sending the trap by the SNMP agent when successfully downloading configuration. **enable** - Send the trap by the SNMP agent when successfully downloading configuration. **disable** - No trap will be send.

Restrictions

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

Example

To enable the trap of a configuration saving completed:

```
DGS-3000-28SC:admin#config configuration trap save enable
Command: config configuration trap save enable

Success.

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

Chapter 17 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]}(1)
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 [100ms | 1sec | 10sec | 1min | 10min] | mepid_list [add | delete] <mepid_list 1-8191>}(1)
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>}(1)
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 port <port> {level <int 0-7> | direction [inward | outward] | vlanid <vlanid 1-4094>}
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]}

17-1 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) Specify the maintenance domain index. **<uint 1-4294967295>** - Enter the maintenance domain index value here. This value must be between 1 and 4294967295.
level - Specify 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-3000-28SC:admin#create cfm md op_domain level 2
Command: create cfm md op_domain level 2

Success.

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

17-2 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]}(1)

Parameters

<string 22> - Enter the maintenance domain name. This name can be up to 22 characters long.
md_index - Specify the maintenance domain index. **<uint 1-4294967295>** - Enter the maintenance domain index value here. This value must be

between 1 and 4294967295.
mip - Specify to configure MIPs. **none** - Specify 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 - Specify the control transmission of the sender ID TLV. **none** - Specify 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-3000-28SC:admin#config cfm md op_domain mip explicit
Command: config cfm md op_domain mip explicit

Success.

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

17-3 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) Specify the maintenance association index. **<uint 1-4294967295>** - Enter the maintenance association index value here. This value must be between 1 and 4294967295.
md - Specify the maintenance domain name. **<string 22>** - Enter the maintenance domain name here. This name can be up to 22 characters long. **md_index** - Specify 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-3000-28SC:admin#create cfm ma op1 md op_domain
Command: create cfm ma op1 md op_domain

Success.

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

17-4 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 [100ms | 1sec | 10sec | 1min | 10min] | mepid_list [add | delete] <mepid_list 1-8191>}(1)

Parameters

<string 22> - Enter the maintenance association name. This name can be up to 22 characters long.

ma_index - Specify the maintenance association index.
- **<uint 1-4294967295>** - Enter the maintenance association index value here. This value must be between 1 and 4294967295.

md - Specify the maintenance domain name.
- **<string 22>** - Enter the maintenance domain name here. This name can be up to 22 characters long.
- **md_index** - Specify the maintenance domain index.
  - **<uint 1-4294967295>** - Enter the maintenance domain index value here. This value must be between 1 and 4294967295.

vlanid - Specify 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 - Specify to configure MIPs.
- **none** - Specify 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 - This is the control transmission of the sender ID TLV. **none** - Specify 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 - Specify the CCM interval. **100ms** - Specify that the CCM interval will be set to 100 milliseconds. Not recommended. **1sec** - Specify that the CCM interval will be set to 1 second. **10sec** - Specify that the CCM interval will be set to 10 seconds. This is the default value. **1min** - Specify that the CCM interval will be set to 1 minute. **10min** - Specify that the CCM interval will be set to 10 minutes.
mepid_list - Specify the MEPIDs contained in the maintenance association. The range of the MEPID is 1-8191. **add** - Specify to add MEPID(s). **delete** - Specify to delete MEPID(s). By default, there is no MEPID in a newly created maintenance association. **<mepid_list 1-8191>** - Enter the MEP ID list here.

Restrictions

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

Example

To configure a CFM MA:

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

17-5 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 - Specify 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 - Specify the maintenance domain name. **<string 22>** - Enter the maintenance domain name used here. This name can be up to 22 characters long. **md_index** - Specify the maintenance domain index. **<uint 1-4294967295>** - Enter the maintenance domain index value here. This value must be between 1 and 4294967295.
ma - Specify the maintenance association name. **<string 22>** - Enter the maintenance association name used here. This name can be up to 22 characters long. **ma_index** - Specify the maintenance association index. **<uint 1-4294967295>** - Enter the maintenance association index value here. This value must be between 1 and 4294967295.
direction - Specify the MEP direction. **inward** - Specify the inward facing (up) MEP. **outward** - Specify the outward facing (down) MEP.
port - Specify 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-3000-28SC:admin#create cfm mep mep1 mepid 1 md op_domain ma op1 direction
inward port 2
Command: create cfm mep mep1 mepid 1 md op_domain ma op1 direction inward port
2

Success.

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

17-6 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>}(1)

Parameters

mepname - Specify the MEP name.
- **<string 32>** - Enter the MEP name used here. This name can be up to 32 characters long.

mepid - Specify the MEP ID.
- **<int 1-8191>** - Enter the MEP ID used here. This value must be between 1 and 8191.
- **md** - Specify the maintenance domain name.
  - **<string 22>** - Enter the maintenance domain name used here. This name can be up to 22 characters long.
  - **md_index** - Specify the maintenance domain index.
    - **<uint 1-4294967295>** - Enter the maintenance domain index value here. This value must be between 1 and 4294967295.
- **ma** - Specify the maintenance association name.
  - **<string 22>** - Enter the maintenance association name used here. This name can be up to 22 characters long.
  - **ma_index** - Specify the maintenance association index.
    - **<uint 1-4294967295>** - Enter the maintenance association index value here. This value must be between 1 and 4294967295.

state - Specify the MEP administrative state.
- **enable** - Specify that the MEP will be enabled.
- **disable** - Specify that the MEP will be disabled. This is the default value.

ccm - Specify the CCM transmission state.
- **enable** - Specify that the CCM transmission will be enabled.
- **disable** - Specify that the CCM transmission will be disabled. This is the default value.

pdu_priority - 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 - Specify 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 - Specify 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 - Specify 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-3000-28SC:admin#config cfm mep mepname mep1 state enable ccm enable
Command: config cfm mep mepname mep1 state enable ccm enable

Success.

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

17-7 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 - Specify the MEP name. **<string 32>** - Enter the MEP name used here. This name can be up to 32 characters long.
mepid - Specify the MEP ID. **<int 1-8191>** - Enter the MEP ID used here. This value must be between 1 and 8191. **md** - Specify the maintenance domain name. **<string 22>** - Enter the maintenance domain name used here. This name can be up to 22 characters long. **md_index** - Specify the maintenance domain index. **<uint 1-4294967295>** - Enter the maintenance domain index value here. This value must be between 1 and 4294967295. **ma** - Specify the maintenance association name. **<string 22>** - Enter the maintenance association name used here. This name can be up to 22 characters long. **ma_index** - Specify 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-3000-28SC:admin#delete cfm mep mepname mep1
Command: delete cfm mep mepname mep1

Success.

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

17-8 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 - Specify the maintenance association index. **<uint 1-4294967295>** - Enter the maintenance association index value here. This value must be between 1 and 4294967295.
md - Specify the maintenance domain name. **<string 22>** - Enter the maintenance domain name used here. This name can be up to 22 characters long. **md_index** - Specify 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-3000-28SC:admin#delete cfm ma op1 md op_domain
Command: delete cfm ma op1 md op_domain

Success.

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

17-9 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 - Specify 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-3000-28SC:admin#delete cfm md op_domain
Command: delete cfm md op_domain

Success.

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

17-10 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-3000-28SC:admin#enable cfm
Command: enable cfm

Success.

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

17-11 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-3000-28SC:admin#disable cfm
Command: disable cfm

Success.

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

17-12 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 - Specify that the the CFM function will be enabled or disabled. **enable** - Specify that the CFM function will be enabled. **disable** - Specify 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-3000-28SC:admin#config cfm ports 2-5 state enable
Command: config cfm ports 2-5 state enable

Success.

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

17-13 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-3000-28SC:admin#show cfm ports 1:3-1:6
Command: show cfm ports 1:3-1:6

Port   State
-----  --------
1:3      Enabled
1:4      Enabled
1:5      Enabled
1:6      Disabled

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

17-14 show cfm port

Description

This command is used to show MEPs and MIPs created on a port.

Format

show cfm port <port> {level <int 0-7> | direction [inward | outward] | vlanid <vlanid 1-4094>}

Parameters

<port> - Enter the port number used here.
level - (Optional) Specify 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) Specify the MEP direction. **inward** - Specify that the MEP direction will be inward facing. **outward** - Specify that the MEP direction will be outward facing. If not specified, both directions and the MIP are shown.
vlanid - (Optional) Specify 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-3000-28SC:admin#show cfm port 1:2
Command: show cfm port 1:2

MAC Address: 00-01-02-03-04-02
MD Name      MA Name      MEPID  Level  Direction  VID
-----------  -----------  -----  -----  ---------  ----
op_domain    op1          1      2      Inward     1

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

17-15 cfm linktrace

Description

This command is used to issue a CFM link track message.

Format

cfm linktrace <macaddr> [mepname <string 32> | mepid <int 1-8191> md [<string 22> | md_index <uint 1-4294967295>] ma [<string 22> | ma_index <uint 1-4294967295>]] {ttl <int 2-255> | pdu_priority <int 0-7>}

Parameters

<macaddr> - Enter the destination MAC address.

mepname - Specify the MEP name used.
- **<string 32>** - Enter the MEP name used here. This name can be up to 32 characters long.

mepid - Specify the MEP ID used.
- **<int 1-8191>** - Enter the MEP ID used here. This value must be between 1 and 8191.
- **md** - Specify the maintenance domain name.
  - **<string 22>** - Enter the maintenance domain name her. This name can be up to 22 characters long.
  - **md_index** - Specify the maintenance domain index.
    - **<uint 1-4294967295>** - Enter the maintenance domain index value here. This value can be between 1 and 4294967295.
- **ma** - Specify the maintenance association name.
  - **<string 22>** - Enter the maintenance association name her. This name can be up to 22 characters long.
  - **ma_index** - Specify the maintenance association index.
    - **<uint 1-4294967295>** - Enter the maintenance association index value here. This value can be between 1 and 4294967295.

ttl - (Optional) Specify 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-3000-28SC: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-3000-28SC:admin#
```

17-16 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 - Specify the MEP name used. **<string 32>** - Enter the MEP name used here. This name can be up to 32 characters long.
mepid - Specify the MEP ID used. **<int 1-8191>** - Enter the MEP ID used here. This value must be between 1 and 8191. **md** - Specify the maintenance domain name. **<string 22>** - Enter the maintenance domain name her. This name can be up to 22 characters long. **md_index** - Specify the maintenance domain index. **<uint 1-4294967295>** - Enter the maintenance domain index value here. This value must between 1 and 4294967295. **ma** - Specify the maintenance association name. **<string 22>** - Enter the maintenance association name her. This name can be up to 22 characters long. **ma_index** - Specify the maintenance association index. **<uint 1-4294967295>** - Enter the maintenance association index value here. This value must between 1 and 4294967295.
trans_id - (Optional) Specify 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-3000-28SC: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    : 2014-01-31 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-3000-28SC:admin#"
```

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

```
DGS-3000-28SC: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-3000-28SC:admin#"
```

17-17 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) Specify the maintenance domain name.
- **<string 22>** - Enter the maintenance domain name her. This name can be up to 22 characters long.
- **md_index** - Specify the maintenance domain index.
  - **<uint 1-4294967295>** - Enter the maintenance domain index value here. This value must be between 1 and 4294967295.
- **ma** - (Optional) Specify the maintenance association name.
  - **<string 22>** - Enter the maintenance association name her. This name can be up to 22 characters long.
  - **ma_index** - Specify the maintenance association index.
    - **<uint 1-4294967295>** - Enter the maintenance association index value here. This value must be between 1 and 4294967295.
  - **mepid** - (Optional) Specify the MEP ID used.
    - **<int 1-8191>** - Enter the MEP ID used here. This value must be between 1 and 8191.

mepname - (Optional) Specify 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-3000-28SC:admin#delete cfm linktrace mepname mep1
Command: delete cfm linktrace mepname mep1

Success.

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

17-18 show cfm mipccm

Description

This command is used to show the MIP CCM database entries. All entries in the MIP CCM database will be shown. A MIP CCM entry is similar to a FDB which keeps the forwarding port information of a MAC entry.

Format

show cfm mipccm

Parameters

None.

Restrictions

None.

Example

To show MIP CCM database entries:

```
DGS-3000-28SC:admin#show cfm mipccm
Command: show cfm mipccm

MA          VID   MAC Address        Port
----------  ----  -----------------  -----
opma        1     00-11-22-33-44-55  1:2
opma        1     01-23-45-67-89-10  1:3

Total: 2

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

17-19 config cfm mp_ltr_all

Description

This command is used to enable or disable the "all MPs reply LTRs" function. It can make all MPs on an LTM’s forwarding path reply with LTRs, whether they are on a Bridge or not.

Format

config cfm mp_ltr_all [enable | disable]

Parameters

enable - Specify 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-3000-28SC:admin#config cfm mp_ltr_all enable
Command: config cfm mp_ltr_all enable

Success.

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

17-20 show cfm mp_ltr_all

Description

This command is used to show the current configuration of the "all MPs reply LTRs" function.

Format

show cfm mp_ltr_all

Parameters

None.

Restrictions

None.

Example

To show the configuration of the "all MPs reply LTRs" function:

```
DGS-3000-28SC:admin#show cfm mp_ltr_all
Command: show cfm mp_ltr_all

All MPs reply LTRs: Disabled

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

17-21 show cfm remote_mep

Description

This command is used to show remote MEPs.

Format

show cfm remote_mep [mepname <string 32> | md [<string 22> | md_index <uint 1-4294967295>] ma [<string 22> | ma_index <uint 1-4294967295>] mepid <int 1-8191>] remote_mepid <int 1-8191>

Parameters

mepname - Specify the MEP name used. **<string 32>** - Enter the MEP name used here. This name can be up to 32 characters long.
md - Specify the maintenance domain name. **<string 22>** - Enter the maintenance domain name here. This name can be up to 22 characters long. **md_index** - Specify the maintenance domain index. **<uint 1-4294967295>** - Enter the maintenance domain index value here. This value must between 1 and 4294967295. **ma** - Specify the maintenance association name. **<string 22>** - Enter the maintenance association name here. This name can be up to 22 characters long. **ma_index** - Specify the maintenance association index. **<uint 1-4294967295>** - Enter the maintenance association index value here. This value must between 1 and 4294967295. **mepid** - Specify the MEP ID used. **<int 1-8191>** - Enter the MEP ID used here. This value must be between 1 and 8191.
remote_mepid - Specify 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-3000-28SC: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-3000-28SC:admin#
```

17-22 show cfm pkt_cnt

Description

This command is used to show the CFM packet's RX/TX counters.

Format

show cfm pkt_cnt {[ports <portlist> {[rx | tx]} | [rx | tx] | ccm]}

Parameters

ports - (Optional) Specify 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) Specify to display the RX counter. **tx** - (Optional) Specify to display the TX counter. If not specified, both of them will be shown.
rx - (Optional) Specify to display the RX counter.
tx - (Optional) Specify to display the TX counter. If not specified, both of them will be shown.
ccm - (Optional) Specify the CCM RX counters.

Restrictions

None.

Example

To show the CFM packet's RX/TX counters:

```
DGS-3000-28SC: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
1:1     0        0        0        0        0        0        0        0
1:2     0        0        0        0        0        0        0        0
1:3     0        0        0        0        0        0        0        0
1:4     0        0        0        0        0        0        0        0
1:5     0        0        0        0        0        0        0        0
1:6     0        0        0        0        0        0        0        0
1:7     0        0        0        0        0        0        0        0
1:8     0        0        0        0        0        0        0        0
1:9     0        0        0        0        0        0        0        0
1:10    0        0        0        0        0        0        0        0
1:11    0        0        0        0        0        0        0        0
1:12    0        0        0        0        0        0        0        0
1:13    0        0        0        0        0        0        0        0
1:14    0        0        0        0        0        0        0        0
1:15    0        0        0        0        0        0        0        0
1:16    0        0        0        0        0        0        0        0
1:17    0        0        0        0        0        0        0        0
1:18    0        0        0        0        0        0        0        0
1:19    0        0        0        0        0        0        0        0
1:20    0        0        0        0        0        0        0        0
1:21    0        0        0        0        0        0        0        0
1:22    0        0        0        0        0        0        0        0
1:23    0        0        0        0        0        0        0        0
1:24    0        0        0        0        0        0        0        0
1:25    0        0        0        0        0        0        0        0
1:26    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
1:1     0        0        0        0        0        0
1:2     0        0        0        0        0        0
1:3     0        0        0        0        0        0
1:4     0        0        0        0        0        0
1:5     0        0        0        0        0        0
1:6     0        0        0        0        0        0
1:7     0        0        0        0        0        0
1:8     0        0        0        0        0        0
1:9     0        0        0        0        0        0
1:10    0        0        0        0        0        0
1:11    0        0        0        0        0        0
1:12    0        0        0        0        0        0
1:13    0        0        0        0        0        0
1:14    0        0        0        0        0        0
1:15    0        0        0        0        0        0
1:16    0        0        0        0        0        0
1:17    0        0        0        0        0        0
1:18    0        0        0        0        0        0
```

```
1:19    0         0         0         0         0         0
1:20    0         0         0         0         0         0
1:21    0         0         0         0         0         0
1:22    0         0         0         0         0         0
1:23    0         0         0         0         0         0
1:24    0         0         0         0         0         0
1:25    0         0         0         0         0         0
1:26    0         0         0         0         0         0

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

17-23 clear cfm pkt_cnt

Description

This command is used to clear the CFM packet's RX/TX counters.

Format

clear cfm pkt_cnt {[ports <portlist> {[rx | tx]} | [rx | tx] | ccm]}

Parameters

ports - (Optional) The ports which require need the counters clearing. If not specified, all ports will be cleared. **<portlist>** - Enter the list of ports used for this configuration here. **rx** - (Optional) Specify to clear the RX counter. **tx** - (Optional) Specify to clear the TX counter. If not specified, both of them will be cleared.
rx - (Optional) Specify to clear the RX counter.
tx - (Optional) Specify to clear the TX counter. If not specified, both of them will be cleared.
ccm - (Optional) Specify 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-3000-28SC:admin#clear cfm pkt_cnt
Command: clear cfm pkt_cnt

Success.

DGS-3000-28SC:admin#clear cfm pkt_cnt ccm
Command: clear cfm pkt_cnt ccm

Success.

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

Chapter 18 Connectivity Fault Management (CFM) Extension Command List

config cfm ais md [<string 22> | md_index <uint 1-4294967295>] ma [<string 22> | ma_index <uint 1-4294967295>] mepid <int 1-8191> {period [1sec | 1min] | level <int 0-7> | state [enable | disable]}(1)
config cfm lock md [<string 22> | md_index <uint 1-4294967295>] ma [<string 22> | ma_index <uint 1-4294967295>] mepid <int 1-8191> {period [1sec | 1min] | level <int 0-7> | state [enable | disable]}(1)
config cfm trap [ais | lock] state [enable | disable]
show cfm {[md [<string 22> | md_index <uint 1-4294967295>] {ma [<string 22> | ma_index <uint 1-4294967295>] {mepid <int 1-8191>}} | mepname <string 32>]}
show cfm fault {md [<string 22> | md_index <uint 1-4294967295>] {ma [<string 22> | ma_index <uint 1-4294967295>]}}
cfm lock md [<string 22> | md_index <uint 1-4294967295>] ma [<string 22> | ma_index <uint 1-4294967295>] mepid <int 1-8191> remote_mepid <int 1-8191> action [start | stop]
cfm loopback <macaddr> [mepname <string 32> | mepid <int 1-8191> md [<string 22> | md_index <uint 1-4294967295>] ma [<string 22> | ma_index <uint 1-4294967295>]] {num <int 1-65535> | [length <int 0-1500> | pattern <string 1500>] | pdu_priority <int 0-7>}

18-1 config cfm ais md

Description

This command is used to configure the parameters of the AIS function on a MEP.

Format

config cfm ais md [<string 22> | md_index <uint 1-4294967295>] ma [<string 22> | ma_index <uint 1-4294967295>] mepid <int 1-8191> {period [1sec | 1min] | level <int 0-7> | state [enable | disable]}(1)

Parameters

<string 22> - Enter the maintenance domain name. The maximum length is 22 characters.
md_index - Specify the maintenance domain index. **<uint 1-4294967295>** - Enter the maintenance domain index value here. This value must be between 1 and 4294967295.
ma - Specify the maintenance association name. **<string 22>** - Enter the maintenance association name. The maximum length is 22 characters. **ma_index** - Specify the maintenance association index. **<uint 1-4294967295>** - Enter the maintenance association index value here. This value must be between 1 and 4294967295.
mepid - Specify the MEPID. **<int 1-8191>** - Enter the MEP MEPID between 1 and 8191.
period - Specify the transmitting interval of the AIS PDU. **1sec** - Specify that the transmitting interval period will be set to 1 second. **1min** - Specify that the transmitting interval period will be set to 1 minute.
level - Specify the client level ID to which the MEP sends AIS PDU. The default client MD level is

the MD level that the most immediate client layer MIPs and MEPs exist on. **<int 0-7>** - Enter the client level ID used here. This value must be between 0 and 7.
state - Specify the AIS function state used. **enable** - Specify that AIS function state will be enabled. **disable** - Specify that AIS function state will be disabled.

Restrictions

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

Example

To configure the AIS function so that it is enabled and has a client level of 5:

```
DGS-3000-28SC:admin# config cfm ais md op-domain ma op-ma mepid 1 state enable
level 5
Command: config cfm ais md op-domain ma op-ma mepid 1 state enable level 5

Success.

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

18-2 config cfm lock md

Description

This command is used to configure the parameters of the LCK function on a MEP.

Format

config cfm lock md [<string 22> | md_index <uint 1-4294967295>] ma [<string 22> | ma_index <uint 1-4294967295>] mepid <int 1-8191> {period [1sec | 1min] | level <int 0-7> | state [enable | disable]}(1)

Parameters

<string 22> - Enter the maintenance domain name. The maximum length is 22 characters.
md_index - Specify the maintenance domain index. **<uint 1-4294967295>** - Enter the maintenance domain index value here. This value must be between 1 and 4294967295.
ma - Specify the maintenance association name. **<string 22>** - Enter the maintenance association name. The maximum length is 22 characters. **ma_index** - Specify the maintenance association index. **<uint 1-4294967295>** - Enter the maintenance association index value here. This value must be between 1 and 4294967295.
mepid - Specify the MEPID. **<int 1-8191>** - Enter the MEP MEPID between 1 and 8191.
period - Specify the transmitting interval of the LCK PDU. **1sec** - Specify that the transmitting interval period will be set to 1 second. **1min** - Specify that the transmitting interval period will be set to 1 minute.
level - Specify the client level ID to which the MEP sends LCK PDU. The default client MD level is the MD level that the most immediate client layer MIPs and MEPs exist on. **<int 0-7>** - Enter the client level ID used here. This value must be between 0 and 7.
state - Specify the LCK function state used.

enable - Specify that LCK function state will be enabled. **disable** - Specify that LCK function state will be disabled.

Restrictions

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

Example

To configure the LCK function state as enabled and specify a client level of 5:

```
DGS-3000-28SC:admin# config cfm lock md op-domain ma op-ma mepid 1 state enable
level 5
Command: config cfm lock md op-domain ma op-ma mepid 1 state enable level 5

Success.

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

18-3 config cfm trap

Description

This command is used to configure the state of the CFM trap.

Format

config cfm trap [ais | lock] state [enable | disable]

Parameters

ais - Specify the AIS trap status to be configured. If the trap status of AIS is enabled, a trap will be sent out when an ETH-AIS event occurs or clears.
lock - Specify the LCK trap status that to be configured. If the trap status of LCK is enabled, a trap will be sent out wnen an ETH-LCK event occurs or clears.
state – Specify the state of the CFM trap. **enable** – Enable the CFM trap state. This is the default. **disable** – Disable the CFM trap state.

Restrictions

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

Example

To configure the CFM ports:

```
DGS-3000-28SC:admin# config cfm trap ais state enable
Command: config cfm trap ais state enable

Success.

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

18-4 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) Specify 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) Specify the maintenance domain index.
  - **<uint 1-4294967295>** - Enter the maintenance domain index value here. This value must be between 1 and 4294967295.
- **ma** - (Optional) Specify the maintenance association name.
  - **<string 22>** - Enter the maintenance association name used here. This name can be up to 22 characters long.
  - **ma_index** - Specify the maintenance association index.
    - **<uint 1-4294967295>** - Enter the maintenance association index value here. This value must be between 1 and 4294967295.
  - **mepid** - (Optional) Specify the MEP ID.
    - **<int 1-8191>** - Enter the MEP ID used here. This value must be between 1 and 8191.

mepname - (Optional) Specify 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-3000-28SC:admin#show cfm
Command: show cfm

CFM State: Enabled

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

```
DGS-3000-28SC: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-3000-28SC: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     1:2      mep1         00-01-02-03-04-02


DGS-3000-28SC:admin#show cfm mepname mep1
Command: show cfm mepname mep1

Name                : mep1
MEPID               : 1
Port                : 1:1
Direction           : Inward
CFM Port Status     : Enabled
MAC Address         : 78-54-2E-B6-6C-01
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
AIS State           : Disabled
AIS Period          : 1 Second
AIS Client Level    : Invalid
AIS Status          : Not Detected
LCK State           : Disabled
LCK Period          : 1 Second
```

```
LCK Client Level    : Invalid
LCK Status          : Not Detected
Out-of-Sequence CCMs: 0 received
Cross-connect CCMs  : 0 received
Error CCMs          : 0 received
Normal CCMs         : 2 received
Port Status CCMs    : 0 received
If Status CCMs      : 0 received
CCMs transmitted    : 14
In-order LBRs       : 0 received
Out-of-order LBRs   : 0 received
Next LTM Trans ID   : 0
Unexpected LTRs     : 0 received
LBMs Transmitted    : 0
AIS PDUs            : 0 received
AIS PDUs Transmitted: 0
LCK PDUs            : 0 received
LCK PDUs Transmitted: 0

Remote
MEPID  MAC Address       Status RDI PortSt  IfSt       LCK Detect Time
------ ----------------- ------ --- ------- ---------- --- -------------------
2      B8-A3-86-F4-1C-99 OK     No  Up      Up         No  2014-05-19 02:50:01

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

18-5 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) Specify 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) Specify the maintenance domain index.
  - **<uint 1-4294967295>** - Enter the maintenance domain index value here. This value must be between 1 and 4294967295.
- **ma** - (Optional) Specify the maintenance association name.
  - **<string 22>** - Enter the maintenance association name used here. This name can be up to 22 characters long.
  - **ma_index** - Specify 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-3000-28SC:admin#show cfm fault
Command: show cfm fault
MD Name     MA Name     MEPID  Status                AIS Status   LCK Status
----------- ----------- ----- ---------------------- ------------ ------------
op_domain   op1         1     Error CCM Received     AIS Received Normal


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

18-6 cfm lock md

Description

This command is used to start/stop cfm management lock. This command will result in the MEP sends a LCK PDU to client level MEP.

Format

cfm lock md [<string 22> | md_index <uint 1-4294967295>] ma [<string 22> | ma_index <uint 1-4294967295>] mepid <int 1-8191> remote_mepid <int 1-8191> action [start | stop]

Parameters

<string 22> - Enter the maintenance domain name here. This name can be up to 22 characters long.
md_index - Specify the MD index value used. **<uint 1-4294967295>** - Enter the MD index value used here. This value must be between 1 and 4294967295.
ma - Specify the maintenance association name. **<string 22>** - Enter the maintenance association name here. This name can be up to 22 characters long. **ma_index** - Specify the MA index value used. **<uint 1-4294967295>** - Enter the MA index value used here. This value must be between 1 and 4294967295.
mepid - The MEP ID in the MD which sends LCK frame. **<int 1-8191>** - Enter the MEP ID value here. This value must be between 1 and 8191.
remote_mepid - The peer MEP is the target of management action. **<int 1-8191>** - Enter the remote MEP ID used here. This value must be between 1 and 8191.
action - Specify to start or to stop the management lock function. **start** - Specify to start the management lock function. **stop** - Specify to stop the management lock function.

Restrictions

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

Example

To start management lock:

```
DGS-3000-28SC:admin# cfm lock md op-domain ma op-ma mepid 1 remote_mepid 2
action start
Command: cfm lock md op-domain ma op-ma mepid 1 remote_mepid 2 action start

Success.

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

18-7 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. If the MAC address is multicast, all remote MEPs should reply to this message. 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. This MAC address can be unicast or multicast.

mepname - Specify the MEP name used.
- **<string 32>** - Enter the MEP name used here. This name can be up to 32 characters long.

mepid - Specify the MEP ID used.
- **<int 1-8191>** - Enter the MEP ID used here. This value must be between 1 and 8191.
- **md** - Specify the maintenance domain name.
  - **<string 22>** - Enter the maintenance domain name here. This name can be up to 22 characters long.
  - **md_index** - Specify the maintenance domain index.
    - **<uint 1-4294967295>** - Enter the maintenance domain index value here. This value must be between 1 and 4294967295.
- **ma** - Specify the maintenance association name.
  - **<string 22>** - Enter the maintenance association name here. This name can be up to 22 characters long.
  - **ma_index** - Specify 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-3000-28SC: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-3000-28SC:admin#”
```

Chapter 19 CPU Interface Filtering Command List

create cpu access_profile profile_id <value 1-5> [ethernet {vlan | source_mac <macmask 000000000000-ffffffffffff> | destination_mac <macmask 000000000000-ffffffffffff> | 802.1p | ethernet_type} | ip {vlan | source_ip_mask <netmask> | destination_ip_mask <netmask> | dscp | [icmp {type | code} | igmp {type} | tcp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff> | flag_mask [all | {urg | ack | psh | rst | syn | fin}]} | udp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | protocol_id_mask <hex 0x0-0xff> {user_define_mask <hex 0x0-0xffffffff>}]} | packet_content_mask {offset_0-15 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_16-31 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_32-47 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_48-63 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_64-79 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff>} | ipv6 {class | flowlabel | source_ipv6_mask <ipv6mask> | destination_ipv6_mask <ipv6mask>}]
delete cpu access_profile [profile_id <value 1-5> | all]
config cpu access_profile profile_id <value 1-5> [add access_id [auto_assign | <value 1-100>] [ethernet {[vlan <vlan_name 32> | vlan_id <vlanid 1-4094>] | source_mac <macaddr> | destination_mac <macaddr> | 802.1p <value 0-7> | ethernet_type <hex 0x0-0xffff>} | ip {[vlan <vlan_name 32> | vlan_id <vlanid 1-4094>] | source_ip <ipaddr> | destination_ip <ipaddr> | dscp <value 0-63> | [icmp {type <value 0-255> | code <value 0-255>} | igmp {type <value 0-255>} | tcp {src_port <value 0-65535> | dst_port <value 0-65535> | flag [all | {urg | ack | psh | rst | syn | fin}]} | udp {src_port <value 0-65535> | dst_port <value 0-65535>} | protocol_id <value 0-255> {user_define <hex 0x0-0xffffffff>}]} | packet_content {offset_0-15 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_16-31 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_32-47 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_48-63 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_64-79 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff>} | ipv6 {class <value 0-255> | flowlabel <hex 0x0-0xfffff> | source_ipv6 <ipv6addr> | destination_ipv6 <ipv6addr>}] port [<portlist> | all] [permit | deny] {time_range <range_name 32>} | delete access_id <value 1-100>]
enable cpu_interface_filtering
disable cpu_interface_filtering
show cpu access_profile {profile_id <value 1-5>}

19-1 create cpu access_profile profile_id

Description

This command is used to create CPU access list profiles.

Format

create cpu access_profile profile_id <value 1-5> [ethernet {vlan | source_mac <macmask 000000000000-ffffffffffff> | destination_mac <macmask 000000000000-ffffffffffff> | 802.1p | ethernet_type} | ip {vlan | source_ip_mask <netmask> | destination_ip_mask <netmask> | dscp | [icmp {type | code} | igmp {type} | tcp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff> | flag_mask [all | {urg | ack | psh | rst | syn | fin}]} | udp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | protocol_id_mask <hex 0x0-0xff> {user_define_mask <hex 0x0-0xffffffff>}]} | packet_content_mask {offset_0-15 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_16-31 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_32-47

<hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_48-63 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_64-79 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff>} | ipv6 {class | flowlabel | source_ipv6_mask <ipv6mask> | destination_ipv6_mask <ipv6mask>}]

Parameters

<value 1-5> - Enter the profile ID value here. This value must be between 1 and 5.

ethernet - Specify that the profile type will be Ethernet.
- **vlan** - (Optional) Specify a VLAN mask.
- **source_mac** - (Optional) Specify the source MAC mask.
  - **<macmask>** - Enter the source MAC mask here.
- **destination_mac** - (Optional) Specify the destination mac mask.
  - **<macmask>** - Enter the destination MAC mask here.
- **802.1p** - (Optional) Specify 802.1p priority tag mask.
- **ethernet_type** - (Optional) Specify the ethernet type mask.

ip - Specify that the profile type will be IP.
- **vlan** - (Optional) Specify a VLAN mask.
- **source_ip_mask** - (Optional) Specify an IP source submask.
  - **<netmask>** - Enter the IP source submask here.
- **destination_ip_mask** - (Optional) Specify an IP destination submask.
  - **<netmask>** - Enter the IP destination submask here.
- **dscp** - (Optional) Specify the DSCP mask.
- **icmp** - (Optional) Specify that the rule applies to ICMP traffic.
  - **type** - (Optional) Specify that the rule applies to ICMP type traffic.
  - **code** - (Optional) Specify that the rule applies to ICMP code traffic.
- **igmp** - (Optional) Specify that the rule applies to IGMP traffic.
  - **type** - (Optional) Specify that the rule applies to IGMP type traffic.
- **tcp** - Specify that the rule applies to TCP traffic.
  - **src_port_mask** - (Optional) Specify the TCP source port mask.
    - **<hex 0x0-0xffff>** - Enter the source TCP port mask here.
  - **dst_port_mask** - (Optional) Specify the TCP destination port mask.
    - **<hex 0x0-0xffff>** - Enter the destination TCP port mask here.
  - **flag_mask** - (Optional) Specify the TCP flag field mask.
    - **all** - Specify that the TCP flag field mask will be set to all.
    - **urg** - (Optional) Specify that the TCP flag field mask will be set to urg.
    - **ack** - (Optional) Specify that the TCP flag field mask will be set to ack.
    - **psh** - (Optional) Specify that the TCP flag field mask will be set to psh.
    - **rst** - (Optional) Specify that the TCP flag field mask will be set to rst.
    - **syn** - (Optional) Specify that the TCP flag field mask will be set to syn.
    - **fin** - (Optional) Specify that the TCP flag field mask will be set to fin.
- **udp** - (Optional) Specify that the rule applies to UDP traffic.
  - **src_port_mask** - (Optional) Specify the UDP source port mask.
    - **<hex 0x0-0xffff>** - Enter the source UDP port mask here.
  - **dst_port_mask** - (Optional) Specify the UDP destination port mask.
    - **<hex 0x0-0xffff>** - Enter the destination UDP port mask here.
- **protocol_id_mask** - (Optional) Specify that the rule applies to the IP protocol ID traffic.
  - **<hex 0x0-0xff>** - Enter the IP protocol ID mask here.
  - **user_define_mask** - (Optional) Specify 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 - Specify 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) Specify 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) Specify 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) Specify 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) Specify 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) Specify 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 - Specify IPv6 filtering mask.	**class** - (Optional) Specify the IPv6 class. **flowlabel** - (Optional) Specify the IPv6 flowlabel. **source_ipv6_mask** - (Optional) Specify an IPv6 source submask. **<ipv6mask>** - Enter the IPv6 source submask here. **destination_ipv6_mask** - (Optional) Specify 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-3000-28SC: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-3000-28SC: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-3000-28SC:admin#
```

19-2 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 - Specify the index of access list profile. **<value 1-5>** - Enter the profile ID value here. This value must be between 1 and 5. **all** - Specify that al 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-3000-28SC:admin#delete cpu access_profile profile_id 1
Command: delete cpu access_profile profile_id 1

Success.

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

19-3 config cpu access_profile profile_id

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 0x0-0xfffff> | source_ipv6 <ipv6addr> | destination_ipv6 <ipv6addr>}] port [<portlist> | all] [permit | deny] {time_range <range_name 32>} | delete access_id <value 1-100>]

Parameters

<value 1-5> - Enter the profile ID value here. This value must be between 1 and 5.
add - Specify that a profile or a rule will be added.
access_id - Specify the index of access list entry. The range of this value is 1-100. **auto_assign** - Specify that the access ID will automatically be assigned. **<value 1-100>** - Enter the access ID here. This value must be between 1 and 100.
ethernet - Specify that the profile type will be Ethernet. **vlan** - (Optional) Specify 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) Specify the VLAN ID used.
<vlanid 1-4094> - Enter the VLAN ID used here.
source_mac - (Optional) Specify the source MAC address.
<macaddr> - Enter the source MAC address used for this configuration here.
destination_mac - (Optional) Specify the destination MAC.
<macaddr> - Enter the destination MAC address used for this configuration here.
802.1p - (Optional) Specify 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) Specify the Ethernet type.
<hex 0x0-0xffff> - Enter the Ethernet type value here.

ip - Specify that the profile type will be IP.
vlan - (Optional) Specify 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) Specify the VLAN ID used.
<vlanid 1-4094> - Enter the VLAN ID used here.
source_ip - (Optional) Specify an IP source address.
<ipaddr> - Enter the source IP address used for this configuration here.
destination_ip - (Optional) Specify an IP destination address.
<ipaddr> - Enter the destination IP address used for this configuration here.
dscp - (Optional) Specify the value of DSCP, the value can be configured 0 to 63.
<value 0-63> - Enter the DSCP value used here.
icmp - (Optional) Specify that the rule applies to ICMP traffic.
type - (Optional) Specify 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) Specify 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) Specify that the rule applies to IGMP traffic.
type - (Optional) Specify 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) Specify that the rule applies to TCP traffic.
src_port - (Optional) Specify 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) Specify 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) Specify the TCP flag fields .
all - Specify that the TCP flag field mask will be set to all.
urg - (Optional) Specify that the TCP flag field mask will be set to urg.
ack - (Optional) Specify that the TCP flag field mask will be set to ack.
psh - (Optional) Specify that the TCP flag field mask will be set to psh.
rst - (Optional) Specify that the TCP flag field mask will be set to rst.
syn - (Optional) Specify that the TCP flag field mask will be set to syn.
fin - (Optional) Specify that the TCP flag field mask will be set to fin.
udp - Specify that the rule applies to UDP traffic.
src_port - (Optional) Specify 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) Specify 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 - Specify 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) Specify 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 - Specify 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) Specify 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) Specify 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) Specify 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) Specify 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) Specify 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 - Specify the rule applies to IPv6 fields. **class** - (Optional) Specify the value of IPv6 class. **<value 0-255>** - Enter the IPv6 class value here. This value must be between 0 and 255. **flowlabel** - (Optional) Specify the value of IPv6 flowlabel. **<hex 0x0-0xffff>** - Enter the IPv6 flowlabel here. **source_ipv6** - (Optional) Specify the value of IPv6 source address. **<ipv6addr>** - Enter the IPv6 source address used for this configuration here. **destination_ipv6** - (Optional) Specify the value of IPv6 destination address. **<ipv6addr>** - Enter the IPv6 destination address used for this configuration here.
port - Specify the list of ports to be included in this configuration. **<portlist>** - Enter a list of ports used for the configuration here. **all** - Specify that all the ports will be used for this configuration.
permit - Specify the packets that match the access profile are permit by the Switch.
deny - Specify the packets that match the access profile are filtered by the Switch.
time_range - (Optional) Specify name of this time range entry. **<range_name 32>** - Enter the time range here.
delete - Specify to delete a rule from the profile ID entered.
access_id - Specify 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-3000-28SC: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-3000-28SC:admin#
```

19-4 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-3000-28SC:admin#enable cpu_interface_filtering
Command: enable cpu_interface_filtering

Success.

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

19-5 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-3000-28SC:admin#disable cpu_interface_filtering
Command: disable cpu_interface_filtering

Success.

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

19-6 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) Specify 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-3000-28SC: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-3000-28SC:admin#
```

Chapter 20 CPU Protect Command List

enable cpu_protect
disable cpu_protect
config cpu_protect type {arp | bpdu | icmp | igmp |snmp} pps [<value 0-1024> | no_limit]
show cpu_protect

20-1 enable cpu_protect

Description

This command is used to enable CPU protection of rate limit state.

Format

enable cpu_protect

Parameters

None.

Restrictions

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

Example

To enable the rate limit state:

```
DGS-3000-28SC:admin# enable cpu_protect
Command: enable cpu_protect

Success.

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

20-2 disable cpu_protect

Description

This command is used to disable CPU protection of rate limit state.

Format

disable cpu_protect

Parameters

None.

Restrictions

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

Example

To disable the rate limit state:

```
DGS-3000-28SC:admin# disable cpu_protect
Command: disable cpu_protect

Success.

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

20-3 config cpu_protect type

Description

This command is used to configure the rate-limit of traffic destined to CPU by protocol type. The CPU can handle certain packets, routing protocols, Layer 2 protocols, and packets for management. When the CPU traffic overloads, the CPU will spend a lot of time processing unnecessary traffic, and the routing processes are impacted. To mitigate the impact, the user can use this command to control the threshold of individual protocol packets. If the specific packet that sends it to the CPU exceeds the above threshold, the packets will be dropped.

Format

config cpu_protect type {arp | bpdu | icmp | igmp |snmp} pps [<value 0-1024> | no_limit]

Parameters

arp - (Optional) Specify the IP Address Resolution Protocol (ARP).
bpdu - (Optional) Specify the BPDU packets sent to the CPU with the address 01-80-c2-00-00-XX, such as STP BPDU, 1X BPDU, GVRP BPDU and so on.
icmp - (Optional) Specify the Internet Control Message Protocol.
igmp - (Optional) Specify the Internet Group Management Protocol.
snmp - (Optional) Specify the Simple Network Management Protocol.
pps - Specify the threshold as packet count per second at which traffic is received on the CPU port. **<value 0-1024>** - Enter the threshold as packet count per second at which traffic is received on the CPU port. The range is 0 to 1024, when the threshold is set to 0, all packets of the specified type will be dropped. **no_limit** - No threshold is specified when traffic is received on the CPU port

Restrictions

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

Example

To display how to set a 100 pps ARP limit:

```
DGS-3000-28SC:admin# config cpu_protect type arp pps 100
Command: config cpu_protect type arp pps 100

Success.

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

20-4 show cpu_protect

Description

This command is used to display the CPU protect configuration.

Format

show cpu_protect

Parameters

None.

Restrictions

None.

Example

To display the CPU protect configuration:

```
DGS-3000-28SC:admin# show cpu_protect
Command: show cpu_protect

CPU Protect State: Enabled

CPU Protect Type Rate Limit(pps)
---------------- --------------
ARP                  100
BPDU                 100
ICMP                 200
IGMP                 200
SNMP                 100

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

Chapter 21 Debug Software Command List

debug address_binding [event | dhcp | all] state [enable | disable]
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 clear cpu port counter [<portlist> | all]
debug show cpu port counter [<portlist> | all] [by_cos | by_reason | by_protocol [L2 | ARP | IPv4 [ICMP | TCP | UDP | multicast-protocol | unicast-protocol | all] | IPv6 [ICMP | TCP | UDP | OSPFV3 | all] | STACK] | by_priority]
debug show error_reboot state
debug show error ports box_id [<value 1-6> | all] {sio 1 | sio 2}(1)
debug show packet ports box_id [<value 1-6> | all] {sio1 | sio 2}(1)
debug show status {module <module_list>}
debug show address_binding binding_state_table [nd_snooping | dhcpv6_snooping]
debug dhcpv6_relay hop_count state [enable | disable]
debug dhcpv6_relay output [buffer | console]
debug dhcpv6_relay packet [all | receiving | sending] state [enable | disable]
debug dhcpv6_relay state disable
debug dhcpv6_relay state enable
debug dhcpv6_client state [enable | disable]
debug dhcpv6_client output [buffer | console]
debug dhcpv6_client packet [all | receiving | sending] state [enable | disable]
debug show cpu utilization
no debug address_binding

21-1 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 - Specify the IMPB debug state to be enabled or disabled. **enable** - Specify to enable the state. **disable** - Specify to disable the state.

Restrictions

Only Administrator users can issue this command.

Example

To print out all debug IMPB messages:

```
DGS-3000-28SC:admin#debug address_binding all state enable
Command: debug address_binding all state enable

Success.

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

21-2 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 - Specify to upload the debug log to a TFTP server specified by IP address. **<ipaddr>** - (Optional) Enter the IPv4 address of the TFTP server. **<path_filename 64>** - (Optional) Enter the DOS pathname on the TFTP server. It can be a relative pathname or an absolute pathname. This value can be up to 64 characters long.

Restrictions

Only Administrators can issue this command.

Example

To dump the error log:

```
DGS-3000-28SC:admin#debug error_log dump
Command: debug error_log dump

********************************************************************************
# debug log: 1
# level: fatal
# clock: 10000ms
# time : 2014/11/11 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-3000-28SC:admin#debug error_log clear
Command: debug error_log clear

Success.

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

To upload the error log to TFTP server:

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

21-3 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 - Specify to upload the debug buffer to a TFTP server specified by IP address. **<ipaddr>** - Enter the IPv4 address of the TFTP server. **<path_filename 64>** - Enter the DOS pathname on the TFTP server. It can be a relative pathname or an absolute pathname. This value can be up to 64 characters long.

Restrictions

Only Administrator users can issue this command.

Example

To show the debug buffer's state:

```
DGS-3000-28SC:admin#debug buffer utilization
Command: debug buffer utilization

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

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

To clear the debug buffer:

```
DGS-3000-28SC:admin#debug buffer clear
Command: debug buffer clear

Success.

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

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

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

21-4 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 - Specify 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-3000-28SC:admin#debug output all console
Command: debug output all console

Success.

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

21-5 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 - Specify that the Switch will reboot when a fatal error happens.
disable - Specify that the Switch will not reboot when a fatal error happens, system will hang-up for debug and enter the debug shell mode for debug.

Restrictions

Only Administrators can issue this command.

Example

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

```
DGS-3000-28SC:admin#debug config error_reboot disable
Command: debug config error_reboot disable

Success.

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

21-6 debug config state

Description

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

Format

debug config state [enable | disable]

Parameters

enable - Specify to enable the debug state.
disable - Specify to disable the debug state.

Restrictions

Only Administrators can issue this command.

Example

To set the debug state to disabled:

```
DGS-3000-28SC:admin#debug config state disable
Command: debug config state disable

Success.

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

21-7 debug clear cpu port counter

Description

This command is used to clear cpu port counter.

Format

debug clear cpu port counter [<portlist> | all]

Parameters

<portlist> - Specify a range of ports.
all - Specify all ports.

Restrictions

Only Administrators can issue this command.

Example

To clear cpu port counter of all ports:

```
DGS-3000-28SC:admin# debug clear cpu port counter all
Command: debug clear cpu port counter all

Success.

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

21-8 debug show cpu port counter

Description

This command is used to show debug cpu port counter.

Format

debug show cpu port counter [<portlist> | all] [by_cos | by_reason | by_protocol [L2 | ARP | IPv4 [ICMP | TCP | UDP | multicast-protocol | unicast-protocol | all] | IPv6 [ICMP | TCP | UDP | OSPFV3 | all] | STACK] | by_priority]

Parameters

<portlist> - Specify a range of ports.
all - Specify all ports.
by_cos - Display by Cos.
by_reason - Display by reason.
by_protocol - Display by protocol types.
L2 - Display by L2 protocol.
ARP - Display by ARP protocol.
IPv4 - Display by IPv4 protocol.
ICMP - Display by ICMP.
TCP - Display by TCP.
UDP - Display by UDP.
multicast-protocol - Display by multicast protocol.
unicast-protocol - Display by unicast protocol
all - Display by all IPv4 protocols.
IPv6 - Display by IPv6 protocol

	ICMP - Display by ICMP. **TCP** - Display by TCP. **UDP** - Display by UDP. **OSPFV3** - Display by OSPFv3. **all** - Display by all IPv6 protocol.
STACK - Display by stacking.	
by_priority - Display by priority.	

Restrictions

Only Administrators can issue this command.

Example

To show debug cpu port counter by CoS on port 1:1 and 1:2:

```
DGS-3000-28SC:admin# debug show cpu port counter 1:1-1:2 by_cos
Command: debug show cpu port counter 1:1-1:2 by_cos

Ports:1
 CoS 0 rx:0 tx:0
      1 rx:0 tx:0
      2 rx:0 tx:0
      3 rx:0 tx:0
      4 rx:0 tx:0
      5 rx:0 tx:0
      6 rx:0 tx:0
      7 rx:0 tx:0
      unknown rx:0 tx:0
      total rx:0 tx:0
Ports:2
 CoS 0 rx:0 tx:0
      1 rx:0 tx:0
      2 rx:0 tx:0
      3 rx:0 tx:0
      4 rx:0 tx:0
      5 rx:0 tx:0
      6 rx:0 tx:0
      7 rx:0 tx:0
      unknown rx:0 tx:0
      total rx:0 tx:0

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

21-9 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-3000-28SC:admin#debug show error_reboot state
Command: debug show error_reboot state

Error Reboot: Enabled

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

21-10 debug show error ports box_id

Description

This command is used to show the error statistics information of the selected sio port.

Format

debug show error ports box_id [<value 1-6> | all] {sio1 | sio2}(1)

Parameters

<value 1-6> - Specify a value for debugging the error ports..
all - Specify all ports.
sio1 - Specify SIO1 port.
sio2 - Specify SIO2 port

Restrictions

Only Administrators can issue this command.

Example

To show the debug error statistics information of the selected sio port:

```
DGS-3000-28SC:admin#debug show error ports box_id all sio1
Command: debug show error ports box_id all sio1

Current stacking mode is disabled

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

21-11 debug show packet ports box_id

Description

This command is used to show the packet statistics information of the selected sio port.

Format

debug show packet ports box_id [<value 1-6> | all] {sio1 | sio2}(1)

Parameters

<value 1-6> - Specify a value for debugging the packet statistics for a selected sio port.
all - Specify all ports.
sio1 - Specify SIO1 port.
sio2 - Specify SIO2 port

Restrictions

Only Administrators can issue this command.

Example

To show the debug error statistics information of the selected sio port:

```
DGS-3000-28SC:admin#debug show error ports box_id all sio1
Command: debug show error ports box_id all sio1

Current stacking mode is disabled

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

21-12 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) Specify 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-3000-28SC:admin#debug show status module MSTP
Command: debug show status module MSTP

Debug Global State  : Enabled

MSTP                : Disabled

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

To show the debug state:

```
DGS-3000-28SC:admin#debug show status
Command: debug show status

Debug Global State  : Enabled

MSTP                : Disabled
IMPB                : Disabled
DHCPv6_RELAY        : Disabled
DHCPv6_SERVER       : Disabled
ERPS                : Disabled

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

21-13 debug show address_binding binding_state_table

Description

This command is used to display the ND snooping and DHCPv6 binding state table.

Format

debug show address_binding binding_state_table [nd_snooping | dhcpv6_snooping]

Parameters

nd_snooping - Display the ND Snooping binding state table.
dhcpv6_snooping - Display the DHCPv6 binding state table.

Restrictions

Only Administrators can issue this command.

Example

To display the DHCPv6 snooping binding state of entries in BST:

```
DGS-3000-28SC:admin# debug show address_binding binding_state_table
dhcpv6_snooping
Command: debug show address_binding binding_state_table dhcpv6_snooping

 S (State) - S: Start, L: Live, D :Detection, R: Renew, B: Bound
 Time - Expiry Time (sec)

 IP Address                                MAC Address       S  Time       Port
 ----------------------------------------- ----------------- -- ---------- -----
2001:2222:1111:7777:5555:6666:7777:8888  00-00-00-00-00-02 S  50          5
2001::1                                   00-00-00-00-03-02 B  100         6

Total entries : 2

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

21-14 debug dhcpv6_relay hop_count state

Description

This command is used to enable or disable debug information flag about the hop count.

Format

debug dhcpv6_relay hop_count state [enable | disable]

Parameters

enable - Specify that the hop count state will be enabled.
disable - Specify that the hop count state will be disabled.

Restrictions

Only Administrators can issue this command.

Example

To enable debug information flag about the hop count:

```
DGS-3000-28SC:admin# debug dhcpv6_relay hop_count state enable
Command: debug dhcpv6_relay hop_count state enable

Success.

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

21-15 debug dhcpv6_relay output

Description

This command is used to set debug message to output to buffer or console.

Format

debug dhcpv6_relay output [buffer | console]

Parameters

buffer - Let the debug message output to buffer.
console - Let the debug message output to console.

Restrictions

Only Administrators can issue this command.

Example

To set debug information to output to console:

```
DGS-3000-28SC:admin#  debug dhcpv6_relay output console
Command: debug dhcpv6_relay output console

Success.

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

21-16 debug dhcpv6_relay packet

Description

This command is used to enable or disable debug information flag for DHCPv6 relay packet, including packet receiving and sending.

Format

debug dhcpv6_relay packet [all | receiving | sending] state [enable | disable]

Parameters

all - Set packet receiving and sending debug flags.
receiving - Set packet receiving debug flag.

sending - Set packet sending debug flag.
state - Specify if the designated flags function will be enabled or disabled. **enable** - Enable the designated flags. **disable** - Disable the designated flags.

Restrictions

Only Administrators can issue this command.

Example

To enabled DHCPv6 relay packet sending debug:

```
DGS-3000-28SC:admin#  debug dhcpv6_relay packet sending state enable
Command: debug dhcpv6_relay packet sending state enable

Success.

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

21-17 debug dhcpv6_relay state disable

Description

This command is used to disable the DHCPv6 relay Debug function.

Format

debug dhcpv6_relay state disable

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To disabled DHCPv6 relay debug function:

```
DGS-3000-28SC:admin#  debug dhcpv6_relay state disable
Command:   debug dhcpv6_relay state disable

Success.

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

21-18 debug dhcpv6_relay state enable

Description

This command is used to enable the DHCPv6 relay Debug function.

Format

debug dhcpv6_relay state enable

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To enabled DHCPv6 relay debug function:

```
DGS-3000-28SC:admin#  debug dhcpv6_relay state enable
Command:   debug dhcpv6_relay state enable

Success.

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

21-19 debug dhcpv6_client state

Description

This command is used to enable or disable the DHCPv6 client debug function.

Format

debug dhcpv6_client state [enable | disable]

Parameters

enable - Specify to enable the DHCPv6 client debug function.
disable - Specify to disable the DHCPv6 client debug function.

Restrictions

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

Example

To enabled the DHCPv6 client debug function:

```
DGS-3000-28SC:admin# debug dhcpv6_client state enable
Command:   debug dhcpv6_client state enable

Success.

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

21-20 debug dhcpv6_client output

Description

This command is used to set the debug message to output the buffer or console.

Format

debug dhcpv6_client output [buffer | console]

Parameters

buffer - Specify the debug message output to buffer.
console - Specify the debug message output to console.

Restrictions

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

Example

To display debug information to output to the console:

```
DGS-3000-28SC:admin# debug dhcpv6_client output console
Command: debug dhcpv6_client output console

Success.

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

21-21 debug dhcpv6_client packet

Description

This command is used to enable or disable the DHCPv6 client packets debug information flag, including packet receiving and sending.

Format

debug dhcpv6_client packet {all | receiving | sending} state [enable | disable]

Parameters

all - (Optional) Specify the set packet receiving and sending debug flags.
receiving - (Optional) Specify the set packet receiving debug flag.
sending - (Optional) Specify the set packet sending debug flag.
state - Specify the DHCPv6 client packet debug state. **enable** - Specify to enable the designated flags. **disable** - Specify to disable the designated flags.

Restrictions

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

Example

To enable DHCPv6client packet sending debug flags:

```
DGS-3000-28SC:admin# debug dhcpv6_client packet sending state enable
Command: debug dhcpv6_client packet sending state enable

Success.

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

21-22 debug show cpu utilization

Description

This command is used to display the total CPU utilization and CPU utilization per process.

Format

debug show cpu utilization

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To shows how to turn on debugging for the show CPU utilization command:

```
DGS-3000-28SC:admin#debug show cpu utilization
Command: debug show cpu utilization

Five seconds -  12 %        One minute -  13 %  Five minutes -  13 %

Process Name       5Sec     1Min     5Min
-----------------   ------   ------   ------
OS_UTIL              86 %         86 %     86 %
GBIC_Pooling          5 %          5 %      5 %
DDM_TIC               3 %          3 %      3 %
bcmCNTR.0             1 %          1 %      1 %
bcmLINK.0             0 %          0 %      0 %
HISR1                 0 %          0 %      0 %
bcmL2X.0              0 %          0 %      0 %
MAUMIB_TASK           0 %          0 %      0 %
socdmadesc.0          0 %          0 %      0 %
Sflow                 0 %          0 %      0 %
FAN_Pooling           0 %          0 %      0 %
bcmRX                 0 %          0 %      0 %
radius_reader         0 %          0 %      0 %
CNT_TASK              0 %          0 %      0 %
IP-Msg                0 %          0 %      0 %
DLKtimer              0 %          0 %      0 %
IP6-Tic               0 %          0 %      0 %
SYS_Ctr               0 %          0 %      0 %
CLI                   0 %          0 %      0 %
LOOPBACK_TASK         0 %          0 %      0 %
IP-Tic                0 %          0 %      0 %
EthFwd6               0 %          0 %      0 %
ST_PERI               0 %          0 %      0 %
8021xCtrl             0 %          0 %      0 %
OS_TIMER              0 %          0 %      0 %
ST_Qchk               0 %          0 %      0 %
DHCP6Relay            0 %          0 %      0 %
ADDRBINDDHCP          0 %          0 %      0 %
DHCP6                 0 %          0 %      0 %
l2pt_tick             0 %          0 %      0 %
Telnetv6              0 %          0 %      0 %
MbaAuth               0 %          0 %      0 %
LacpTick              0 %          0 %      0 %
web_v6                0 %          0 %      0 %
ST_Tic                0 %          0 %      0 %
PacketStorm           0 %          0 %      0 %
RMON                  0 %          0 %      0 %
web                   0 %          0 %      0 %
FT_TIC                0 %          0 %      0 %
DLS_Agent_v6          0 %          0 %      0 %
Telnet                0 %          0 %      0 %
1X_Timer              0 %          0 %      0 %
SYSLOG-TICK           0 %          0 %      0 %
oam_sync_task         0 %          0 %      0 %
AcctTask              0 %          0 %      0 %
```

```
FWD-ETH                0 %          0 %       0 %
AcctCtrl               0 %          0 %       0 %
SEC_MON                0 %          0 %       0 %
FDB_R                  0 %          0 %       0 %
cpuprotect             0 %          0 %       0 %
DoSPrevention          0 %          0 %       0 %
FDB_S                  0 %          0 %       0 %
SEC_ASSIGN             0 %          0 %       0 %
IPMC_TIC               0 %          0 %       0 %
BPDUPRecover           0 %          0 %       0 %
GRA_ARP                0 %          0 %       0 %
RadiusCtrl             0 %          0 %       0 %
DLS_Agent              0 %          0 %       0 %
PingTask               0 %          0 %       0 %
STPTick                0 %          0 %       0 %
DRV_ARL                0 %          0 %       0 %
GM_APP_TFTP_TAS        0 %          0 %       0 %
Dhcp6lrPkt             0 %          0 %       0 %
Ping6Task              0 %          0 %       0 %
CFM_SYN_T              0 %          0 %       0 %
ACL_CNT                0 %          0 %       0 %
TFTP_S                 0 %          0 %       0 %
ARP_Unresolved         0 %          0 %       0 %
safeguard              0 %          0 %       0 %
FFS_GC                 0 %          0 %       0 %
TOPOLOGY               0 %          0 %       0 %
NDP_Unresolved         0 %          0 %       0 %
STPSync                0 %          0 %       0 %
sred_cnt               0 %          0 %       0 %
IP6                    0 %          0 %       0 %
vlan counter ta        0 %          0 %       0 %
timerange              0 %          0 %       0 %
SNTP_TIMER             0 %          0 %       0 %
bcmXGS3AsyncTX         0 %          0 %       0 %
bcmTX                  0 %          0 %       0 %

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

21-23 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-3000-28SC:admin#no debug address_binding
Command: no debug address_binding

Success.

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

Chapter 22 DHCP Local Relay Command List

config dhcp_local_relay vlan <vlan_name 32> state [enable | disable]
config dhcp_local_relay vlan vlanid <vlan_id 1-4094> state [enable | disable]
enable dhcp_local_relay
disable dhcp_local_relay
show dhcp_local_relay

22-1 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> - Enter the VLAN name. This name can be up to 32 characters long.
state - Enables or disables DHCP local relay for specified vlan. **enable** - Specify to enable the DHCP local relay function. **disable** - Specify 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-3000-28SC:admin#config dhcp_local_relay vlan default state enable
Command: config dhcp_local_relay vlan default state enable

Success.

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

22-2 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 1-4094> state [enable | disable]

Parameters

<vlan_id 1-4094> - Enter the VLAN ID used here.
state - Enables or disables DHCP local relay for specified vlan. **enable** - Specify that the DHCP local relay function will be enabled. **disable** - Specify 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-3000-28SC:admin#config dhcp_local_relay vlan vlanid 1 state enable
Command: config dhcp_local_relay vlan vlanid 1 state enable

Success.

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

22-3 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-3000-28SC:admin#enable dhcp_local_relay
Command: enable dhcp_local_relay

Success.

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

22-4 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-3000-28SC:admin#disable dhcp_local_relay
Command: disable dhcp_local_relay

Success.

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

22-5 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-3000-28SC:admin#show dhcp_local_relay
Command: show dhcp_local_relay

DHCP/BOOTP Local Relay Status         : Disabled
DHCP/BOOTP Local Relay VID List       :

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

Chapter 23 DHCP Relay Command List

config dhcp_relay {hops <int 1-16> | time <sec 0-65535>}(1)
config dhcp_relay add ipif <ipif_name 12> <ipaddr>
config dhcp_relay option_82 {state [enable | disable] | check [enable | disable] | policy [replace | drop | keep] | remote_id [default | user_define <desc 32> | vendor2 | vendor3] | circuit_id [default | user_define <desc 32> | vendor1 | vendor2 | vendor3 | vendor4 | vendor5 | vendor6]}(1)
enable dhcp_relay
disable dhcp_relay
config dhcp_relay unicast [enable | disable]
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 <desc_long 255>] [relay <ipaddr> | drop]
config dhcp_relay option_61 default [relay <ipaddr> | drop]
config dhcp_relay option_61 delete [mac_address <macaddr> | string <desc_long 255> | all]
show dhcp_relay option_61
config dhcp_relay add vlanid <vlan_id_list> <ipaddr>
config dhcp_relay ports [<portlist> | all] state [enable | disable]
show dhcp_relay ports {<portlist>}
config dhcp_relay port_option_82 {<portlist>} [circuit_id | remote_id] [vendor3 <sentence 32>]
show dhcp_relay port_option_82 {<portlist>}
config dhcp_relay server_cvid <ipaddr> [<vlan_id1-4094> | null]
show dhcp_relay server_cvid {<ipaddr>}
config dhcp_relay delete ipif <ipif_name 12> <ipaddr>
config dhcp_relay delete vlanid <vlan_id_list> <ipaddr>

23-1 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>}(1)

Parameters

hops - Specify 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 - 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-3000-28SC:admin#config dhcp_relay hops 4 time 2
Command: config dhcp_relay hops 4 time 2

Success.

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

23-2 config dhcp_relay add ipif

Description

This command is used to add an IP destination address of the DHCP server for relay of DHCP/BOOTP packets.

Format

config dhcp_relay add ipif <ipif_name 12> <ipaddr>

Parameters

<ipif_name 12> - Enter the IP interface name used here. This name can be up to 12 characters long.
<ipaddr> - 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-3000-28SC:admin#config dhcp_relay add ipif System 10.43.21.12
Command: config dhcp_relay add ipif System 10.43.21.12

Success.

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

23-3 config dhcp_relay option_82

Description

This command is used to configure the processing of DHCP 82 option for the DHCP relay function. When DHCP 82 option is enabled, the DHCP packet received from the client will be inserted with option 82 fields before being relayed to the server. The DHCP 82 option contains 2 sub-options: circuit ID and remote ID sub-option.

Format

config dhcp_relay option_82 {state [enable | disable] | check [enable | disable] | policy [replace | drop | keep] | remote_id [default | user_define <desc 32> | vendor2 | vendor3] | circuit_id [default | user_define <desc 32> | vendor1 | vendor2 | vendor3 | vendor4 | vendor5 | vendor6]}(1)

Parameters

state - When the state is enabled, the DHCP packet will be inserted with the option 82 field before being relayed to server. The DHCP packet will be processed based on the 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** - Specify that the option 82 processing will be enabled.
- **disable** - Specify that the option 82 processing will be disabled.

check - 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** - Specify that checking will be enabled.
- **disable** - Specify that checking will be disabled.

policy - Specify the policy used. This option takes effect only when the check status is disabled. The default setting is set to 'replace'.
- **replace** - Specify 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** - Specify to discard if the packet has the option 82 field. If the packet, that comes from the client side, contains an 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** - Specify to retain the existing option 82 field in the packet. If the packet, that comes from the client side, contains an 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 - Specify 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.
- **vendor2** - If configured to vendor2, the remote ID uses the following format:

a. b. c.

2	n	System name
1 byte	1 byte	N bytes

a. Sub-option type, 2 indicates this is the remote ID.
b. Length: length of value
c. Value: Character string. System name of the switch. (No remote ID sub-option type, directly fill the value.)

vendor3 - If configured to vendor3, the remote ID uses the following format:

a.	b.	c.
2	n	User-defined
1 byte	1 byte	Maximum 32 bytes

a. Sub-option type (2 means remote ID).
b. Length: Total length of user-defined string. By default, the length is 0 with no field value.
c. Value: User-defined string that can be configured using the config dhcp_relay port_option_82 command. The maximum length of the user-defined string is 32 bytes. (No remote ID sub-option type, directly fill the value.)

circuit_id - Specify the DHCP relay option 82 circuit ID.

default - If configured to default, the circuit ID use the original format:

a.	b.	c.	d.	e.	f.	g.
1	0x6	0	4	VLAN	Module ID	Port ID
1 byte	1 byte	1 byte	1 byte	2 bytes	1 byte	1 byte

a. Sub-option type (1 means circuit ID)
b. Length, it should be 6.
c. Circuit ID's sub-option, it should be 0.
d. Sub-option's length, it should be 4
e. VLAN ID (S-VID)
f. Module ID, for standalone switch, it is 0; for stacking switch, it is the box ID that assigned by stacking.
g. Port ID: port number of each box.

user_define - Use user-defined string as the circuit ID.

a.	b.	c.	d.	e.
1	n+2	1	n	User-defined
1 byte	1 byte	1 byte	1 byte	Max. 32 bytes

<desc 32> - Enter the user-defined ID. Space is allowed in the string.

vendor1 - If configured to vendor1, the circuit ID uses the following format to communicate with Alcatel-Lucent's server:

a.	b.	c.	d.	e.	f.	g.	h.	i.	j.
1	0x10	0	6	VLAN	Slot ID	Port ID	1	6	MAC
1 byte	1 byte	1 byte	1 byte	2 bytes	2 bytes	2 bytes	1 byte	1 byte	6 bytes

a. Sub-option type (1 means circuit ID)
b. Length
c. Circuit ID's sub-option's first tag, it should be 0.
d. First tag's length, it should be 6
e. VLAN ID
f. Slot ID, for standalone switch, it is 1; for stacking switch, it is the box ID that assigned by stacking.
g. Port ID: port number of each box
h. Circuit ID's sub-option's second tag, it should be 1.
i. Second tag's length, it should be 6.
j. MAC address: System's MAC address

vendor2 - If configured to vendor2, the circuit ID uses the following format:

a.	b.	c.
1	n	Port number
1 byte	1 byte	N bytes

a. Sub-option type, 1 indicates this is the Circuit ID.
b. Length: length of value
c. Value: Character string. The incoming port number of DHCP client packet, start with character "p". Ex: p02 means port 2. (No Circuit ID sub-option type, directly fill the value.) For stacking port(1~768), The format of port 129(port 1 of box3) is p129.

vendor3 - If configured to vendor3, the circuit ID uses the following format:

a.	b.	c.
1	n	User-defined
1 byte	1 byte	Maximum 32 bytes

a. Sub-option type 1 (1 means circuit ID).
b. Length: Total length of user-defined string. By default, the length is 0 with no field value.
c. Value: User-defined string that can be configured using the config dhcp_relay port_option_82 command. The maximum length of the user-defined string is 32 bytes.

vendor4 - If configured to vendor4, the circuit ID uses the following format:

a.	b.	c.	d.	e.	f.	g.	h.	i.
1	n	System name	-	Module ID	/	Port ID	-	CVID
1 byte	1 byte	0-128 bytes	1 byte	1 byte	1 byte	1-2 bytes	1 byte	1-4 bytes

a. Sub-option type (1 means circuit ID)
b. Length: Total lengths of all follow fields.
c. System name.
d. Separator character
e. Module ID
f. Separator character.
g. Port ID: port number
h. Separator character
i. CVID(Client VLAN ID)

vendor5 - If configured to vendor5, the circuit ID uses the following format:

a.	b.	c.	d.	e.	f.	g.	h.
1	n	System name	Space (0x20)	e (0x65)	t (0x74)	h (0x68)	Space (0x20)
1 byte	1 byte	0-128 bytes	1 byte	1 byte	1 byte	1 byte	1 byte

i.	j.	k.	l.	m.	n.	o.
Chassis ID	/ (0x2F)	Slot ID	/ (0x2F)	Port number	: (0x3A)	VLAN ID
1-2 bytes	1 byte	1-2 bytes	1-2 bytes	1 byte	1 byte	1-4 bytes

a. Sub-option type (1 means circuit ID).
b. Length.
c. System name of the Switch. NOTE: If the System name exceeds 128 bytes, it will only use the first 128 bytes.
d. Space
e. Character ‘e’.
f. Character ‘t’.
g. Character ‘h’.
h. Space.
i. Chassis ID. The number of the chassis. For stand-alone devices, the chassis ID will always be 0. For stacked devices, the chassis ID will be the unit ID.
j. Slash (/).
k. Slot ID. The number of the slot used in the chassis. For non-chassis devices, the slot ID is the module ID of the device starting from 0.
l. Slash (/).
m. Port number. The number of the client’s port.
n. Colon (:).
o. VLAN ID. The ID number of the client’s VLAN.

vendor6 - If configured to vendor6, the cicuit ID uses the following:

F01	F02	F03	F04	F05	F06	F07	F08
1	Length	E (0x45)	t (0x74)	h (0x68)	e (0x65)	r (0x72)	n (0x6E)
1 byte	1 byte	1 byte	1 byte	1 byte	1 byte	1 byte	1 byte

F09	F10	F11	F12	F13	F14	F15	F16
e (0x45)	t (0x74)	Chassis ID	/ (0x2F)	0 (0x30)	/ (0x2F)	Port number	: (0x3A)
1 byte	1 byte	1-2 bytes	1 byte	1 byte	1 byte	1-2 bytes	1 byte

F17	F18	F19	F20	F21	F22	F23	F24
cvlan	. (0x2E)	0 (0x30)	Space (0x20)	System Name	/ (0x2F)	0 (0x30)	/ (0x2F)
1-4 bytes	1 byte	1 byte	1 byte	1-128 bytes	1 byte	1 byte	1 byte

F25	F26	F27	F28	F29	F30	F31
0 (0x30)	/ (0x2F)	Chassis ID	/ (0x2F)	0 (0x30)	/ (0x2F)	Port number
1 byte	1 byte	1-2 bytes	1 byte	1 byte	1 byte	1-2 bytes

F01: Sub-option type (1 means circuit ID).
F02: Length.
F03: Character ‘E’.
F04: Character ‘t’.
F05: Character ‘h’.
F06: Character ‘e’.
F07: Character ‘r’.
F08: Character ‘n’.
F09: Character ‘e’.
F10: Character ‘t’.
F11: Chassis ID. The number of the chassis. For stand-alone devices, the chassis ID will always be 1. For stacked devices, the chassis ID will be the unit ID.
F12: Slash (/).
F13: ASCII format string ‘0’.
F14: Slash (/).
F15: Port number. The incoming port number DHCP client packets. ASCII format string.
F16: Colon (:)
F17: ‘cvlan’ is the client’s VLAN ID. The value ranges from 1 to 4094. ASCII format string.
F18: Dot (.).
F19: ASCII format string ‘0’.
F20: Space.
F21: System name of the Switch. **NOTE:** If the System name exceeds 128 bytes, it will only use the first 128 bytes.
F22: Slash (/).
F23: ASCII format string ‘0’.
F24: Slash (/).
F25: ASCII format string ‘0’.
F26: Slash (/).
F27: Chassis ID. This value is the same as F11.
F28: Slash (/).
F29: ASCII format string ‘0’.
F30: Slash (/).
F31: Port number. The incoming port number of DHCP client packets. ASCII format string.

Restrictions

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

Example

To add a DHCP/BOOTP server 10.43.21.12 to VLAN 1 to 10:

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

To display the DHCP relay status:

```
DGS-3000-28SC:admin#show dhcp_relay
Command: show dhcp_relay

DHCP/BOOTP Relay Status : Disabled
DHCP/BOOTP Relay Unicast Status : Enabled
DHCP/BOOTP Hops Count Limit : 4
DHCP/BOOTP Relay Time Threshold : 0
DHCP Vendor Class Identifier Option 60 State: Disabled
DHCP Client Identifier Option 61 State: Disabled
DHCP Relay Agent Information Option 82 State : Disabled
DHCP Relay Agent Information Option 82 Check : Disabled
DHCP Relay Agent Information Option 82 Policy : Replace
DHCP Relay Agent Information Option 82 Remote ID : 00-01-02-03-04-00
DHCP Relay Agent Information Option 82 Circuit ID : Default

Interface    Server 1        Server 2        Server 3        Server 4
------------ --------------- --------------- --------------- ---------------

Server           VLAN ID List
---------------  ------------------------------------------------------------
10.43.21.12      1-10

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

23-4 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-3000-28SC:admin#enable dhcp_relay
Command: enable dhcp_relay

Success.

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

23-5 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-3000-28SC:admin#disable dhcp_relay
Command: disable dhcp_relay

Success.

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

23-6 config dhcp_relay unicast

Description

This command is used to configure the processing state for DHCP unicast packets from client machines.

Format

config dhcp_relay unicast [enable | disable]

Parameters

enable - DHCP unicast packet will be processed by DHCP relay and local relay function. This is the default value.
disable - DHCP relay/ local relay function will not process DHCP unicast packet.

Restrictions

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

Example

To disable the DHCP relay and local relay agent to process the DHCP unicast packet:

```
DGS-3000-28SC:admin#enable config dhcp_relay unicast disable
Command:     config dhcp_relay unicast disable
Success

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

23-7 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) Specify 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-3000-28SC:admin#show dhcp_relay ipif System
Command: show dhcp_relay ipif System

DHCP/BOOTP Relay Status : Disabled
DHCP/BOOTP Relay Unicast Status : Enabled
DHCP/BOOTP Hops Count Limit : 4
DHCP/BOOTP Relay Time Threshold : 0
DHCP Vendor Class Identifier Option 60 State: Disabled
DHCP Client Identifier Option 61 State: Disabled
DHCP Relay Agent Information Option 82 State : Disabled
DHCP Relay Agent Information Option 82 Check : Disabled
DHCP Relay Agent Information Option 82 Policy : Replace
DHCP Relay Agent Information Option 82 Remote ID : 00-01-02-03-04-00
DHCP Relay Agent Information Option 82 Circuit ID : Default

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


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

23-8 config dhcp_relay option_60 state

Description

This command is used to decide whether DHCP relay will process the DHCP option 60 or not.

When option_60 is enabled, if the packet does not have option 60, then the relay servers cannot be determined based on option 60. The relay servers will be determined based on either option 61 or per IPIF configured servers.

If the relay servers are determined based on option 60 or option 61, then 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

enable - Specify that the option 60 rule will be enabled.
disable - Specify 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-3000-28SC:admin#config dhcp_relay option_60 state enable
Command: config dhcp_relay option_60 state enable

Success

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

23-9 config dhcp_relay option_60 add string

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

<multiword 255> - Enter the string value here. This value can be up to 255 characters long.
relay - Specify 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-3000-28SC: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-3000-28SC:admin#
```

23-10 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 - Specify the IP address used for the DHCP relay forward function. **<ipaddr>** - Enter the IP address used for this configuration here.
mode - Specify the DHCP relay option 60 mode. **relay** - Specify to relay the packet based on the relay rules. **drop** - Specify 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-3000-28SC:admin#config dhcp_relay option_60 default mode drop
Command: config dhcp_relay option_60 default mode drop

Success.

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

23-11 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 - Specify to delete 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) Specify to delete 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 - Specify to delete 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 - Specify to delete all the entry. Default relay servers are excluded.
default - Specify to delete the default relay IP address that is specified by the user. **<ipaddr>** - (Optional) Enter the IP address used for this configuration here.

Restrictions

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

Example

To delete the DHCP relay option 60 string called ‘abc’:

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

23-12 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) Specify to display 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.
ipadddress - (Optional) Specify to display the IP address specified by the user. **<ipaddr>** - Enter the IP address here.
default - (Optional) Specify to display the defaut 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-3000-28SC: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-3000-28SC:admin#
```

23-13 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

enable - Specify to enable the function DHCP relay use option 61 ruler to relay DHCP packet.
disable - Specify to disable 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-3000-28SC:admin#config dhcp_relay option_61 state enable
Command: config dhcp_relay option_61 state enable

Success

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

23-14 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 <desc_long 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. **<desc_long 255>** - Enter the client's description here. This value can be up to 255 characters long.
relay - Specify to relay the packet to a IP address. **<ipaddr>** - Enter the IP address used for this configuration here.
drop - Specify 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-3000-28SC: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-3000-28SC:admin#
```

23-15 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 - Specify 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 - Specify 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-3000-28SC:admin#config dhcp_relay option_61 default drop
Command: config dhcp_relay option_61 default drop

Success

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

23-16 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 < desc_long 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. **<desc_long 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-3000-28SC: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-3000-28SC:admin#
```

23-17 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-3000-28SC: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-3000-28SC:admin#
```

23-18 config dhcp_relay add vlanid

Description

This command is used to add an IP address as a destination to forward (relay) DHCP/BOOTP packets. If there is an IP interface in the VLAN and it has configured a DHCP server at the interface level, then the configuration at the interface level has higher priority. In this case, the DHCP server configured on the VLAN will not be used to forward the DHCP packets.

Format

config dhcp_relay add vlanid <vlan_id_list> <ipaddr>

Parameters

<vlan_id_list> - Enter the VLAN ID list used for this configuration here.
<ipaddr> - Enter the DHCP/BOOTP server IP address used here.

Restrictions

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

Example

To add a DHCP/BOOTP server 10.43.21.12 to VLAN 1 to 10:

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

To display the DHCP relay status:

```
DGS-3000-28SC:admin#show dhcp_relay
Command: show dhcp_relay

DHCP/BOOTP Relay Status : Disabled
DHCP/BOOTP Relay Unicast Status : Enabled
DHCP/BOOTP Hops Count Limit : 4
DHCP/BOOTP Relay Time Threshold : 0
DHCP Vendor Class Identifier Option 60 State: Disabled
DHCP Client Identifier Option 61 State: Disabled
DHCP Relay Agent Information Option 82 State : Disabled
DHCP Relay Agent Information Option 82 Check : Disabled
DHCP Relay Agent Information Option 82 Policy : Replace
DHCP Relay Agent Information Option 82 Remote ID : 00-01-02-03-04-00
DHCP Relay Agent Information Option 82 Circuit ID : Default

Interface    Server 1        Server 2        Server 3        Server 4
------------ --------------- --------------- --------------- ---------------

Server           VLAN ID List
---------------  ------------------------------------------------------------
10.43.21.12      1-10

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

23-19 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> - Enter a list of ports to be configured.
all - Specify all ports to be configured.
state - Specify 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-3000-28SC:admin#config dhcp_relay ports 1-3 state enable
Command: config dhcp_relay ports 1-3 state enable

Success.

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

23-20 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) Enter a list of ports to be displayed.

Restrictions

None.

Example

To display the DHCP relay state of port 1-10:

```
DGS-3000-28SC:admin#show dhcp_relay ports 1-10
Command: show dhcp_relay ports 1-10

Port  DHCP Relay State
----  ----------------
1     Enabled
2     Enabled
3     Enabled
4     Enabled
5     Enabled
6     Enabled
7     Enabled
8     Enabled
9     Enabled
10    Enabled

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

23-21 config dhcp_relay port_option_82

Description

This command is used to configure DHCP relay agent option 82 information of each port.

Format

config dhcp_relay port_option_82 {<portlist>} [circuit_id | remote_id] [vendor3 <sentence 32>]

Parameters

<portlist> - (Optional) Enter the specific ports' option 82 information. A non-specified portlist means all ports are available.
circuit_id - Specify the content in the Circuit ID sub-option.
remote_id - Specify the content in the Remote ID sub-option.
vendor3 - Specify the specific ports' vendor3 user defined string. **<sentence 32>** - Enter the string with 32 characters.

Restrictions

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

Example

To configure vendor3 circuit_id of port 1 to 12345678:

```
DGS-3000-28SC:admin# config dhcp_relay port_option_82 1  circuit_id  vendor3
12345678
Command: config dhcp_relay port_option_82 1  circuit_id  vendor3 12345678

Success

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

23-22 show dhcp_relay port_option_82

Description

This command is used to display the current DHCP relay option 82 information of each port.

Format

show dhcp_relay port_option_82 {<portlist>}

Parameters

<portlist> - (Optional) Enter the list of ports that will be used for this display. If this parameter is not specified, then all ports will be displayed.

Restrictions

None.

Example

To display DHCP relay option 82 information of ports 1:1 to 1:4:

```
DGS-3000-28SC:admin#show dhcp_relay port_option_82 1:1-1:4
Command: show dhcp_relay port_option_82 1:1-1:4

DHCP Relay Agent Information Option 82 Per port info:
Port  Type     Option 82 Remote ID Value        Option 82 Circuit ID Value
----- -------- -------------------------------- ----------------------------
1:1   vendor3                                   12345678
1:2   vendor3
1:3   vendor3
1:4   vendor3

Total Entries : 4

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

23-23 config dhcp_relay server_cvid

Description

This command is used to configure DHCP relay agent destination IP address inner VLAN ID. If the configure inner VID unequal to null, the DHCP relay will insert the inner VLAN ID when it sends ARP packet to the DHCP server.

Format

config dhcp_relay server_cvid <ipaddr> [<vlan_id 1-4094> | null]

Parameters

<ipaddr> - Enter the DHCP or BOOTP server IP address.
<vlan_id 1-4094> - Enter the DHCP or BOOTP inner VLAN ID.
null - Do not enter the inner VLAN ID. This is the default.

Restrictions

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

Example

To configure the inner VID as 10 to the DHCP server with the IP of 10.0.0.1:

```
DGS-3000-28SC:admin# config dhcp_relay server_cvid 10.0.0.1 10
Command: config dhcp_relay server_cvid 10.0.0.1 10

Success.

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

23-24 show dhcp_relay server_cvid

Description

This command is used to display DHCP relay agent destination IP address inner VLAN ID.

Format

show dhcp_relay server_cvid {<ipaddr>}

Parameters

<ipaddr> - (Optional) Enter the DHCP or BOOTP server IP address.

Restrictions

None.

Example

To display the DHCP server with the IP of 10.0.0.1:

```
DGS-3000-28SC:admin#show dhcp_relay server_cvid 10.0.0.1
Command: show dhcp_relay server_cvid 10.0.0.1

Server          CVID
------------    ---------------
10.0.0.1        10

Total Entries : 1

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

23-25 config dhcp_relay delete

Description

This command is used to delete one of the IP destination addresses in the Switch’s relay table.

Format

config dhcp_relay delete ipif <ipif_name 12> <ipaddr>

Parameters

<ipif_name 12> - Enter the IP interface name used here. This name can be up to 12 characters long.
<ipaddr> - 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-3000-28SC:admin#config dhcp_relay delete ipif System 10.43.21.12
Command: config dhcp_relay delete ipif System 10.43.21.12

Success.

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

23-26 config dhcp_relay delete vlanid

Description

This command is used to delete an IP address as a destination to forward (relay) DHCP/BOOTP packets.

Format

config dhcp_relay delete vlanid <vlan_id_list> <ipaddr>

Parameters

<vlan_id_list> - Enter the VLAN ID list used for this configuration here.
<ipaddr> - Enter the DHCP/BOOTP server IP address used here.

Restrictions

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

Example

To delete a DHCP/BOOTP server 10.43.21.12 from VLAN 2 and VLAN 3:

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

Chapter 24 DHCP Server Screening Command List

create filter dhcpv6_server permit sip <ipv6addr> ports [<portlist> | all]
create filter icmpv6_ra_all_node permit sip <ipv6addr> ports [<portlist> | all]
config filter dhcp_server [add permit server_ip <ipaddr> {client_mac <macaddr>} ports [<portlist> | all] | delete permit server_ip <ipaddr> {client_mac <macaddr>} ports [<portlist> | all] | ports [<portlist> | all] {vlanid <vid_list>} state [enable | disable] | illegal_server_log_suppress_duration [1min | 5min | 30min]]
config filter dhcp_server log [enable | disable]
config filter dhcp_server trap [enable | disable]
config filter dhcpv6_server log [enable | disable]
config filter dhcpv6_server ports [<portlist> | all] state [enable | disable]
config filter dhcpv6_server trap [enable | disable]
config filter icmpv6_ra_all_node log [enable | disable]
config filter icmpv6_ra_all_node ports [<portlist> | all] state [enable | disable]
config filter icmpv6_ra_all_node trap [enable | disable]
delete filter dhcpv6_server permit sip <ipv6addr>
delete filter icmpv6_ra_all_node permit sip <ipv6addr>
show filter dhcp_server {ports <portlist>}
show filter dhcpv6_server
show filter icmpv6_ra_all_node

24-1 create filter dhcpv6_server permit sip

Description

This command is used to create a permit entry for DHCPv6 server filtering. The specific DHCPv6 server packets, with the source IPv6 address, will be forwarded on the specified port(s).

Format

create filter dhcpv6_server permit sip <ipv6addr> ports [<portlist> | all]

Parameters

<ipv6addr> - Enter the source address of the entry which will be created into the Filter DHCPv6 server forward list.
ports - Specify the list of ports used for this configuration. **<portlist>** - Enter the list of ports, used for this configuration, here. **all** - Specify that all ports will be used for this configuration.

Restrictions

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

Example

To create a Filter DHCPv6 server permit entry on port 5:

```
DGS-3000-28SC:admin#create filter dhcpv6_server permit sip 2200::5 ports 5
Command: create filter dhcpv6_server permit sip 2200::5 ports 5

Success.

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

24-2 create filter icmpv6_ra_all_node permit sip

Description

This command is used to create a permit entry. The specific ICMPv6 RA All-nodes packets with source IPv6 address can be forwarded on the specified port(s).

Format

create filter icmpv6_ra_all_node permit sip <ipv6addr> ports [<portlist> | all]

Parameters

<ipv6addr> - Enter the source address of entry which will be created into the Filter ICMPv6 RA All-nodes forward list.
ports - Specify a list of ports which apply to icmpv6_ra_all_node permit entry. **<portlist>** - Enter a range of ports that the permit entry will apply to. **all** - Specify all the existing ports that apply to the permit entry.

Restrictions

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

Example

To create a filter ICMPv6 RA All-nodes permit entry on port 5:

```
DGS-3000-28SC:admin#create filter icmpv6_ra_all_node permit sip 2200::5 ports 5
Command: create filter icmpv6_ra_all_node permit sip 2200::5 ports 5

Success.

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

24-3 config filter dhcp_server

Description

This command is used to configure filters on a DHCP server.

You can use DHCP Filtering as a security measure against unauthorized DHCP servers. A known attack can occur when an unauthorized DHCP server responds to a client that is requesting an IP

address. The unauthorized server can configure the gateway for the client to be equal to the IP address of the server. At that point, the client sends all of its IP traffic destined to other networks to the unauthorized machine, giving the attacker the possibility of filtering traffic for passwords or employing a 'man-in-the-middle' attack.

DHCP filtering works by allowing the administrator to configure each port as a trusted or untrusted port. The port that has the authorized DHCP server should be configured as a trusted port. Any DHCP responses received on a trusted port will be forwarded. All other ports should be configured as untrusted. Any DHCP (or BOOTP) responses received on the ingress side will be discarded.

Thi command has three purposes:

1. Specify to filter all DHCP server packets on the specific port.
2. Specify to allow some DHCP server packets with pre-defined server IP addresses.
3. Deny all DHCPOFFER requests by using the default DHCP Server filtering method to specify explicit "permit" rules for the (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 the other provides the public IP address.

Enabling DHCP server port state filtering will create one access profile and create one access rule per port (UDP port = 67). Filter commands in this file will share the same access profile.

Addition of a permit DHCP entry will create one access profile and create one access rule. Filtering commands in this file will share the same access profile.

Format

config filter dhcp_server [add permit server_ip <ipaddr> {client_mac <macaddr>} ports [<portlist> | all] | delete permit server_ip <ipaddr> {client_mac <macaddr>} ports [<portlist> | all] | ports [<portlist> | all] {vlanid <vid_list>} state [enable | disable] | illegal_server_log_suppress_duration [1min | 5min | 30min]]

Parameters

add permit - Specify 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** - Specify that all the port will be used for this configuration.

delete permit - Specify 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** - Specify that all the port will be used for this configuration.
  - **vlan_id** – Specify the VLAN ID to delete.
    - **<vid_list>** - Enter the VLAN ID used for this configuration here.
  - **state** - Specify to enable or disable the filter DHCP server state.
    - **enable** - Specify that the filter DHCP server state will be enabled.
    - **disable** - Specify that the filter DHCP server state will be disabled.

illegal_server_log_suppress_duration - Specify the same illegal DHCP server IP address detected will be logged only once within the duration. The default value is 5 minutes.
- **1min** - Specify that illegal server log suppress duration value will be set to 1 minute.
- **5min** - Specify that illegal server log suppress duration value will be set to 5 minutes.
- **30min** - Specify that illegal server log suppress duration value will be set to 30 minutes.

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-3000-28SC:admin# config filter dhcp_server add permit server_ip 10.1.1.1
client_mac 00-00-00-00-00-01 port 1:1-1:24
Command: config filter dhcp_server add permit server_ip 10.1.1.1 client_mac 00-
00-00-00-00-01 port 1:1-1:24

Success.

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

```
DGS-3000-28SC:admin# config filter dhcp_server ports 1:1-1:10 state enable
Command: config filter dhcp_server ports 1:1-1:10 state enable

Success.

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

24-4 config filter dhcp_server log

Description

This command is used to enable or disable the log function.

Format

config filter dhcp_server log [enable | disable]

Parameters

enable - Specify to enable the log function.
disable - Specify to disable the log function.

Restrictions

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

Example

To disable the log function:

```
DGS-3000-28SC:admin# config filter dhcp_server log disable
Command: config filter dhcp_server log disable

Success.

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

24-5 config filter dhcp_server trap

Description

This command is used to enable and disable the trap command

Format

config filter dhcp_server trap [enable | disable]

Parameters

enable - Specify to enable the DHCP server trap filter.
disable - Specify to disable the DHCP server trap filter.

Restrictions

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

Example

To disable trap for a DHCP server filter event:

```
DGS-3000-28SC:admin# config filter dhcp_server trap disable
Command: config filter dhcp_server trap disable

Success.

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

24-6 config filter dhcpv6_server log

Description

This command is used to enable or disable the Filter DHCPv6 server log state.

Format

config filter dhcpv6_server log [enable | disable]

Parameters

enable - Specify that the log for the Filter DHCPv6 server will be enabled. The log for Filter

DHCPv6 server will be generated.
disable - Specify that the log for the Filter DHCPv6 server will be disabled.

Restrictions

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

Example

To enable the Filter DHCPv6 Server log state:

```
DGS-3000-28SC:admin#config filter dhcpv6_server log enable
Command: config filter dhcpv6_server log enable

Success.

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

24-7 config filter dhcpv6_server ports

Description

This command is used to configure the state of filter DHCPv6 server packets on the switch. The filter DHCPv6 server function is used to filter the DHCPv6 server packets on the specific port(s) and receive the trust packets from the specific source. This feature can be protected network usable when a malicious host sends the DHCPv6 server packets.

Format

config filter dhcpv6_server ports [<portlist> | all] state [enable | disable]

Parameters

<portlist> - Enter a range of ports to configure the Filter DHCPv6 server state.
all - Specify all the existing ports on the switch for configuring the Filter DHCPv6 server state.
state - Specify whether the port's filter DHCPv6 server function is enabled or disabled. **enable** - Specify that the filter option is enabled. **disable** - Specify that the filter option is disabled.

Restrictions

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

Example

To configure enabling all port states:

```
DGS-3000-28SC:admin#config filter dhcpv6_server ports all state enable
Command: config filter dhcpv6_server ports all state enable

Success.

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

24-8 config filter dhcpv6_server trap

Description

This command is used to enable or disable the filter DHCPv6 server trap state.

Format

config filter dhcpv6_server trap [enable | disable]

Parameters

enable - Specify that the trap for the filter DHCPv6 server will be enabled. The trap for filter DHCPv6 server will be sent out.
disable - Specify that the trap for the filter DHCPv6 server will be disabled.

Restrictions

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

Example

To enable the filter DHCPv6 server trap state:

```
DGS-3000-28SC:admin#config filter dhcpv6_server trap enable
Command: config filter dhcpv6_server trap enable

Success.

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

24-9 config filter icmpv6_ra_all_node log

Description

This command is used to enable or disable the filter ICMPv6 RA All-nodes log state.

Format

config filter icmpv6_ra_all_node log [enable | disable]

Parameters

enable - Specify that the log for the filter ICMPv6 RA will be enabled. The log for filter ICMPv6 RA all-nodes will be generated.
disable - Specify that the log for the filter ICMPv6 RA will be disabled.

Restrictions

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

Example

To enable the filter ICMPv6 RA all-nodes log state:

```
DGS-3000-28SC:admin#config filter icmpv6_ra_all_node log enable
Command: config filter icmpv6_ra_all_node log enable

Success.

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

24-10 config filter icmpv6_ra_all_node ports

Description

This command is used to configure the state of the filter ICMPv6 RA all-nodes packets on the switch. The filter ICMPv6 RA all-nodes function is used to filter the ICMPv6 RA all-nodes packets on the specific port(s) and receive the trust packets from the specific source. This feature can be protected network usable when a malicious host sends ICMPv6 RA all-nodes packets.

NOTE: It only needs to filter the packet of which the destination address is the all-nodes multicast address (FF02::1).

Format

config filter icmpv6_ra_all_node ports [<portlist> | all] state [enable | disable]

Parameters

<portlist> - Enter a range of ports for configuring the Filter icmpv6_ra_all_node state.
all - Specify all the existing ports on the switch for configuring the Filter icmpv6_ra_all_node state.
state - Specify whether the port's filter ICMPv6 RA all-nodes packets function is enabled or disabled. **enable** - Specify that the filter ICMPv6 RA all-nodes packets function is be enabled. **disable** - Specify that the filter ICMPv6 RA all-nodes packets function is be disabled.

Restrictions

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

Example

To configure the filter ICMPv6 RA all-nodes state to enabled for ports 1:

```
DGS-3000-28SC:admin#config filter icmpv6_ra_all_node ports 1 state enable
Command: config filter icmpv6_ra_all_node ports 1 state enable

Success.

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

24-11 config filter icmpv6_ra_all_node trap

Description

This command is used to enable or disable the filter ICMPv6 RA all-nodes trap state. If the ICMPv6 RA all-nodes server trap state is disabled, no trap will be sent out.

Format

config filter icmpv6_ra_all_node trap [enable | disable]

Parameters

enable - Specify that the trap for the filter ICMPv6 RA all-nodes will be enabled. The trap for filter ICMPv6 RA all-nodes will be sent out.
disable - Specify that the trap for the filter ICMPv6 RA all-nodes will be disabled.

Restrictions

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

Example

To enable the filter ICMPv6 RA all-nodes trap state:

```
DGS-3000-28SC:admin#config filter icmpv6_ra_all_node trap enable
Command: config filter icmpv6_ra_all_node trap enable

Success.

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

24-12 delete filter dhcpv6_server permit sip

Description

This command is used to delete a filter DHCPv6 server permit entry.

Format

delete filter dhcpv6_server permit sip <ipv6addr>

Parameters

<ipv6addr> - Enter the source IPv6 address of the entry here.

Restrictions

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

Example

To delete permit entry from the filter DHCPv6 server forward list:

```
DGS-3000-28SC:admin#delete filter dhcpv6_server permit sip 2200::4
Command: delete filter dhcpv6_server permit sip 2200::4

Success.

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

24-13 delete filter icmpv6_ra_all_node permit sip

Description

This command is used to delete a filter ICMPv6 RA all-nodes permit entry.

Format

delete filter icmpv6_ra_all_node permit sip <ipv6addr>

Parameters

<ipv6addr> - Enter the source IPv6 address of the entry which will be deleted in the filter ICMPv6 RA all-nodes forward list.

Restrictions

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

Example

To delete permit entry from the filter ICMPv6 RA all-nodes forward list:

```
DGS-3000-28SC:admin#delete filter icmpv6_ra_all_node permit sip 2200::4
Command: delete filter icmpv6_ra_all_node permit sip 2200::4

Success.

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

24-14 show filter dhcp_server

Description

This command is used to display the DHCP server filter list created on the Switch.

Format

show filter dhcp_server {ports <portlist>}

Parameters

ports - (Optional) Specify to show DHCP Server Screening ports configuration with VLAN information. **<portlist>** - Enter the port to show the DHCP server filter.

Restrictions

None.

Example

To display the DHCP server/client filter list created on the Switch:

```
DGS-3000-28SC:admin# show filter dhcp_server
Command: show filter dhcp_server

Enabled ports: 1-3
Trap State: Enabled
Log State: Enabled
Illegal Server Log Suppress Duration : 5 Minutes

Permit DHCP Server/Client Table:
Server IP Address   Client MAC address   Port
-----------------  ------------------  ------
10.255.255.254      00-00-00-00-00-01    1-26

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

24-15 show filter dhcpv6_server

Description

This command is used to display the filter DHCPv6 server information.

Format

show filter dhcpv6_server

Parameters

None.

Restrictions

None.

Example

To display filter DHCPv6 server information:

```
DGS-3000-28SC:admin#show filter dhcpv6_server
Command: show filter dhcpv6_server

Enabled ports:1-8
Trap State: Disabled
Log  State: Enabled

Permit Source Address Table:
Source IP Address                       Port
--------------------------------------  ---------------

Total Entries:0

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

24-16 show filter icmpv6_ra_all_node

Description

This command is used to display the filter ICMPv6 RA all-nodes information.

Format

show filter icmpv6_ra_all_node

Parameters

None.

Restrictions

None.

Example

To display filter ICMPv6 RA all-nodes information:

```
DGS-3000-28SC:admin#show filter icmpv6_ra_all_node
Command: show filter icmpv6_ra_all_node

Enabled ports:1
Trap State: Disabled
Log  State: Enabled

Permit Source Address Table:
Source IP Address                       Port
--------------------------------------  ---------------
 3FFE::1                                 1

Total Entries:1

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

Chapter 25 DHCPv6 Relay Command List

enable dhcpv6_relay
enable dhcpv6_local_relay
disable dhcpv6_relay
disable dhcpv6_local_relay
config dhcpv6_relay [add | delete] ipif <ipif_name 12> <ipv6addr>
config dhcpv6_relay hop_count <value 1-32>
config dhcpv6_relay ipif [<ipif_name 12> | all] state [enable | disable]
config dhcpv6_local_relay vlan [<vlan_name 32> |vlanid <vlan_id>] state [enable | disable]
config dhcpv6_relay option_18 {state [enable | disable] | check [enable | disable] | interface_id [default | cid | vendor1]}(1)
config dhcpv6_relay option_37 {state [enable | disable] | check [enable | disable] | remote_id [default | cid_with_user_define <desc 128> | user_define <desc 128> | vendor1]}(1)
show dhcpv6_relay {ipif <ipif_name 12>}
show dhcpv6_local_relay

25-1 enable dhcpv6_relay

Description

This command is used to enable the DHCPv6 relay function on the Switch.

Format

enable dhcpv6_relay

Parameters

None.

Restrictions

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

Example

To configure the DHCPv6 relay global state to enable:

```
DGS-3000-28SC:admin# enable dhcpv6_relay
Command: enable dhcpv6_relay

Success.

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

25-2 disable dhcpv6_relay

Description

This command is used to disable the DHCPv6 relay function on the Switch.

Format

disable dhcpv6_relay

Parameters

None.

Restrictions

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

Example

To configure the DHCPv6 relay global state to disable:

```
DGS-3000-28SC:admin# disable dhcpv6_relay
Command: disable dhcpv6_relay

Success.

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

25-3 enable dhcpv6_local_relay

Description

This command is used to enable the DHCPv6 local relay function of the Switch.

Format

enable dhcpv6_local_relay

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the DHCPv6 local relay global state to enable:

```
DGS-3000-28SC:admin# enable dhcpv6_local_relay
Command: enable dhcpv6_local_relay

Success.

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

25-4 disable dhcpv6_local_relay

Description

This command is used to disable the DHCPv6 local relay function of the switch

Format

disable dhcpv6_local_relay

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the DHCPv6 local relay global state to disable:

```
DGS-3000-28SC:admin# disable dhcpv6_local_relay
Command: disable dhcpv6_local_relay

Success.

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

25-5 config dhcpv6_relay

Description

This command is used to add/delete an IPv6 address which is a destination to forward (relay) DHCPv6 packets.

Format

config dhcpv6_relay [add | delete] ipif <ipif_name 12> <ipv6addr>

Parameters

add - Add an IPv6 destination to the DHCPv6 relay table.
delete - Delete an IPv6 destination from the DHCPv6 relay table.
ipif - The name of the IP interface in which DHCPv6 relay is to be enabled.

<ipif_name 12> - Enter the IP interface name here. This name can be up to 12 characters long.
<ipv6addr> - Enter the DHCPv6 server IP address.

Restrictions

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

Example

To add a DHCPv6 server to the relay table:

```
DGS-3000-28SC:admin# config dhcpv6_relay add ipif System
2001:DB8:1234:0:218:FEFF:FEFB:CC0E
Command: config dhcpv6_relay add ipif System 2001:DB8:1234:0:218:FEFF:FEFB:CC0E

Success.

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

25-6 config dhcpv6_relay hop_count

Description

This command is used to configure the DHCPv6 relay hop_count of the switch.

Format

config dhcpv6_relay hop_count <value 1-32>

Parameters

<value 1-32> - Enter the number of relay agents that have relayed this message. The default value is 4.

Restrictions

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

Example

To configure the maximum hops of a DHCPv6 relay packet could be transferred to 4:

```
DGS-3000-28SC:admin# config dhcpv6_relay hop_count 4
Command: config dhcpv6_relay hop_count 4

Success.

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

25-7 config dhcpv6_relay ipif

Description

This command is used to configure the DHCPv6 relay state of one specific interface or all interfaces.

Format

config dhcpv6_relay ipif [<ipif_name 12> | all] state [enable | disable]

Parameters

<ipif_name 12> - Enter the IP interface name used here. This name can be up to 12 characters long.
all - Specify that all the configured IP interfaces wil be used.
state - Specify if the DHCPv6 relay state will be enabled or disabled. **enable** - Choose this parameter to enable the DHCPv6 relay state of the interface. **disable** - Choose this parameter to disable the DHCPv6 relay state of the interface.

Restrictions

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

Example

To configure the DHCPv6 relay state of the System interface to enable:

```
DGS-3000-28SC:admin#  config dhcpv6_relay ipif System state enable
Command: config dhcpv6_relay ipif System state enable

Success.

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

25-8 config dhcpv6_local_relay vlan

Description

This command is used to enable or disable the DHCPv6 local relay function for a specified VLAN.

Format

config dhcpv6_local_relay vlan [<vlan_name 32> | vlanid <vlan_id>] state [enable | disable]

Parameters

<vlan_name 32> - Enter the VLAN name that will be used for this configuration
vlanid - Specify the VLAN ID that will be used for this configuration. It supports up to 48 VLANs. **<vlan_id>** - Enter the VLAN ID that will be used for this configuration. It supports up to 48 VLANs.
state - Specify the DHCPv6 local relay function's state for the specified VLAN. **enable** - Specify to enable the DHCPv6 local relay function's state for the specified VLAN.

disable - Specify to disable the DHCPv6 local relay function's state for the specified VLAN.

Restrictions

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

Example

To enable the DHCPv6 local relay function for the default VLAN:

```
DGS-3000-28SC:admin# config dhcpv6_local_relay vlan default state enable
Command: config dhcpv6_local_relay vlan default state enable

Success.

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

25-9 config dhcpv6_relay option_18

Description

This command is used to configure the DHCPv6 relay agent information for processing option 18 within the switch.

Format

config dhcpv6_relay option_18 {state [enable | disable] | check [enable | disable] | interface_id [default | cid | vendor1]}(1)

Parameters

state - Specify the DHCPv6 relay Option 18's state. **enable** - Specify that the DHCPv6 relay Option 18's state is enabled. When the state is enabled, the DHCP packet will be inserted with the Option 18 field before being relayed to server. **disable** - Specify that the DHCPv6 relay Option 18's state is disabled. When the state is disabled, the DHCP packet will be relayed directly to server without further checks and inserted with the Option 18.
check - Specify whether or not to check for the Option 18 field in incoming packets. If the incoming packets contains an Option 18 field, then it will be dropped. **enable** - Specify to enable the check function. **disable** - Specify to disable the check function.
interface_id - Specify the format of the Interface ID. **default** - Specify to used the default formation for the Interface ID. **cid** - Specify to use the CID format for the Interface ID. **vendor1** - Specify to use the Vendor 1 format for the Interface ID.

Restrictions

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

Example

To configure the DHCPv6 relay option 18:

```
DGS-3000-28SC:admin#config dhcpv6_relay option_18 state enable
Command: config dhcpv6_relay option_18 state enable

Success.


DGS-3000-28SC:admin#config dhcpv6_relay option_18 check enable
Command: config dhcpv6_relay option_18 check enable

Success.


DGS-3000-28SC:admin#config dhcpv6_relay option_18 interface_id default
Command: config dhcpv6_relay option_18 interface_id default

Success.


DGS-3000-28SC:admin#config dhcpv6_relay option_18 interface_id cid
Command: config dhcpv6_relay option_18 interface_id cid

Success.


DGS-3000-28SC:admin#config dhcpv6_relay option_18 interface_id vendor1
Command: config dhcpv6_relay option_18 interface_id vendor1

Success.


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

25-10 config dhcpv6_relay option_37

Description

This command is used to configure the processing of option 37 for the DHCPv6 relay function

Format

config dhcpv6_relay option_37 {state [enable | disable] | check [enable | disable] | remote_id [default | cid_with_user_define <desc 128> | user_define <desc 128> | vendor1]}(1)

Parameters

state - When the state is enabled, the DHCP packet will be inserted with the option 37 field before being relayed to server. When the state is disabled, the DHCP packet will be relayed directly to server without further checks and inserted with the option 37.

enable - Specify that the DHCPv6 relay Option 37's state is enabled. When the state is enabled, the DHCP packet will be inserted with the Option 37 field before being relayed to server. **disble** - Specify that the DHCPv6 relay Option 37's state is disabled. When the state is disabled, the DHCP packet will be relayed directly to server without further checks and inserted with the Option 37.
check - When the check state is enabled, packets coming from client side should not have the option 37 field. If client originating packets have the option 37 field set they will be dropped. **enable** - Specify to enable the check function. **disable** - Specify to disable the check function.
remote_id Specify the content in the Remote ID. **default** - The remote ID will be VLAN ID + Module + Port +System MAC address of the device. **cid_with_user_define** - The remote ID will be VLAN ID + Module + Port + user defined string. **<desc 128>** - Enter the user defined cid. The page title description can be up to 128 characters long. **user_define** - The remote ID will be user defined string. **<desc 128>** - Enter the user defined spec up to 128 characters long. **vendor1** - The remote ID will be System MAC address of the device

Restrictions

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

Example

To configure the DHCPv6 relay option 37:

```
DGS-3000-28SC:admin#config dhcpv6_relay option_37 state enable
Command: config dhcpv6_relay option_37 state enable

Success.


DGS-3000-28SC:admin#config dhcpv6_relay option_37 check enable
Command: config dhcpv6_relay option_37 check enable

Success.


DGS-3000-28SC:admin#config dhcpv6_relay option_37 remote_id default
Command: config dhcpv6_relay option_37 remote_id default

Success.


DGS-3000-28SC:admin#config dhcpv6_relay option_37 remote_id cid_with_user_define
D-link DGS3200 Series
Command: config dhcpv6_relay option_37 remote_id cid_with_user_define D-link
DGS3200 Series

Success.


DGS-3000-28SC:admin#config dhcpv6_relay option_37 remote_id user_define D-link
DGS3200 Series
Command: config dhcpv6_relay option_37 remote_id user_define D-link DGS3200
Series

Success.

DGS-3000-28SC:admin#config dhcpv6_relay option_37 remote_id vendor1
Command: config dhcpv6_relay option_37 remote_id vendor1

Success.

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

25-11 show dhcpv6_relay

Description

This command is used to display the current DHCPv6 relay configuration of all interfaces, or if an IP interface name is specified, the DHCPv6 relay configuration for that IP interface.

Format

show dhcpv6_relay {ipif <ipif_name 12>}

Parameters

ipif - (Optional) The name of the IP interface for which to display the current DHCPv6 relay configuration. **<ipif_name 12>** - Enter the IP interface name used here. This name can be up to 12 characters long.
If no IP interface is specified, all configured DHCPv6 relay interfaces are displayed.

Restrictions

None.

Example

To display local DHCPv6 relay configuration:

```
DGS-3000-28SC:admin#show dhcpv6_relay
Command: show dhcpv6_relay

DHCPv6 Relay Global State : Disabled
DHCPv6 Hops Count Limit   : 4
DHCPv6 Relay Information Option 18 State : Disabled
DHCPv6 Relay Information Option 18 Check : Disabled
DHCPv6 Relay Information Option 18 Interface ID Type : Default
DHCPv6 Relay Information Option 37 State : Disabled
DHCPv6 Relay Information Option 37 Check : Disabled
DHCPv6 Relay Information Option 37 Remote ID Type : Default
DHCPv6 Relay Information Option 37 Remote ID :
-----------------------------------------------------------------
IP Interface              : System
DHCPv6 Relay Status       : Enabled
Server Address            :

 Total Entries   : 1


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

25-12 show dhcpv6_local_relay

Description

This command is used to display the current DHCPv6 local relay configuration.

Format

show dhcpv6_local_relay

Parameters

None.

Restrictions

None.

Example

To display local DHCPv6 relay configuration:

```
DGS-3000-28SC:admin#oper#show dhcpv6_local_relay
Command: show dhcpv6_local_relay

DHCPv6 Local Relay Status         : Disabled
DHCPv6 Local Relay VID List       : 1,3-4

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

Chapter 26 Digital Diagnostic Monitoring (DDM) Command List

config ddm [trap | log] [enable | disable]
config ddm ports [<portlist> | all] [[temperature_threshold {high_alarm <degrees> | low_alarm <degrees> | high_warning<degrees> | low_warning <degrees>}(1) | voltage_threshold {high_alarm <voltage> | low_alarm<voltage> | high_warning<voltage> | low_warning<voltage>}(1) | bias_current_threshold {high_alarm <milliampere> | low_alarm <milliampere> | high_warning <milliampere> | low_warning<milliampere>}(1) | tx_power_threshold {high_alarm <mw_or_dbm> | low_alarm <mw_or_dbm> | high_warning <mw_or_dbm> | low_warning <mw_or_dbm>}(1) | rx_power_threshold {high_alarm <mw_or_dbm> | low_alarm <mw_or_dbm> | high_warning <mw_or_dbm> | low_warning <mw_or_dbm>}(1)] | {state [enable | disable] | shutdown [alarm | warning | none]}]
show ddm
show ddm ports {<portlist>} [status | configuration]
config ddm power_unit [mw | dbm]

26-1 config ddm

Description

This command is used to 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 - Specify whether to send traps, when the operating parameter exceeds the corresponding threshold. The DDM trap is disabled by default.
log - Specify whether to send a log, when the operating parameter exceeds the corresponding threshold. The DDM log is enabled by default.
enable - Specify to enable the log or trap sending option.
disable - Specify 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-3000-28SC:admin#config ddm log enable
Command: config ddm log enable

Success.

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

To configure DDM trap state to enable:

```
DGS-3000-28SC:admin#config ddm trap enable
Command: config ddm trap enable

Success.

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

26-2 config ddm ports

Description

This command is used to configure the DDM settings of the specified ports.

Format

config ddm ports [<portlist> | all] [[temperature_threshold {high_alarm <degrees> | low_alarm <degrees> | high_warning<degrees> | low_warning <degrees>}(1) | voltage_threshold {high_alarm <voltage> | low_alarm<voltage> | high_warning<voltage> | low_warning<voltage>}(1) | bias_current_threshold {high_alarm <milliampere> | low_alarm <milliampere> | high_warning <milliampere> | low_warning<milliampere>}(1) | tx_power_threshold {high_alarm <mw_or_dbm> | low_alarm <mw_or_dbm> | high_warning <mw_or_dbm> | low_warning <mw_or_dbm>}(1) | rx_power_threshold {high_alarm <mw_or_dbm> | low_alarm <mw_or_dbm> | high_warning <mw_or_dbm> | low_warning <mw_or_dbm>}(1)] | {state [enable | disable] | shutdown [alarm | warning | none]}]

Parameters

<portlist> - Enter the range of ports to be configured here.
all - Specify that all the optic ports' operating parameters will be configured.
temperature_threshold - Specify the threshold of the optic module's temperature in centigrade. At least one parameter shall be specified for this threshold. **high_alarm -** Specify the high threshold value for the temperature alarm.When the operating parameter rises above this value, the action associated with the alarm is taken. **<degrees>** - Enter the high threshold alarm value used here. **low_alarm** - Specify the low threshold value for the temperature alarm.When the operating parameter falls below this value, the action associated with the alarm is taken. **<degrees>** - Enter the low threshold alarm value used here. **high_warning** - Specify the high threshold for the warning. When the operating parameter rises above this value, the action associated with the warning is taken. **<degrees>** - Enter the high threshold warning value here. **low_warning** - Specify the low threshold for the warning. When the operating parameter falls below this value, the action associated with the warning is taken. **<degrees>** - Enter the low threshold warning value here.
voltage_threshold - Specify the threshold of optic module's voltage. **high_alarm -** Specify the high threshold value for the alarm.When the operating parameter

rises above this value, the action associated with the alarm is taken.
<voltage> - Enter the high threshold alarm value used here.
low_alarm - Specify the low threshold value for the alarm.When the operating parameter falls below this value, the action associated with the alarm is taken.
<voltage> - Enter the low threshold alarm value used here.
high_warning - Specify the high threshold for the warning. When the operating parameter rises above this value, the action associated with the warning is taken.
<voltage> - Enter the high threshold warning value here.
low_warning - Specify the low threshold for the warning. When the operating parameter falls below this value, the action associated with the warning is taken.
<voltage> - Enter the low threshold warning value here.

bias_current_threshold - Specify the threshold of the optic module's bias current.
high_alarm - Specify the high threshold value for the alarm. When the operating parameter rises above this value, the action associated with the alarm is taken.
<milliampere> - Enter the high threshold alarm value used here.
low_alarm - Specify the low threshold value for the alarm. When the operating parameter falls below this value, the action associated with the alarm is taken.
<milliampere> - Enter the low threshold alarm value used here.
high_warning - Specify the high threshold for the warning. When the operating parameter rises above this value, the action associated with the warning is taken.
<milliampere> - Enter the high threshold warning value here.
low_warning - Specify the low threshold for the warning. When the operating parameter falls below this value, the action associated with the warning is taken.
<milliampere> - Enter the low threshold warning value here.

tx_power_threshold - Specify the threshold of the optic module's output power.
high_alarm - Specify the high threshold for the alarm. When the operating parameter rises above this value, the action associated with the alarm is taken.
<mw_or_dbm> - Enter the high threshold alarm value used here.
low_alarm - Specify the low threshold for the alarm. When the operating parameter falls below this value, the action associated with the alarm is taken.
<mw_or_dbm> - Enter the low threshold alarm value used here.
high_warning - Specify the high threshold for the warning. When the operating parameter rises above this value, the action associated with the warning is taken.
<mw_or_dbm> - Enter the high threshold warning value here.
low_warning - Specify the low threshold for the warning. When the operating parameter falls below this value, the action associated with the warning is taken.
<mw_or_dbm> - Enter the low threshold warning value here.

rx_power_threshold - Specify the threshold of optic module's received power.
high_alarm - Specify the high threshold for the alarm. When the operating parameter rises above this value, the action associated with the alarm is taken.
<mw_or_dbm> - Enter the high threshold alarm value used here.
low_alarm - Specify the low threshold for the alarm. When the operating parameter falls below this value, the action associated with the alarm is taken.
<mw_or_dbm> - Enter the low threshold alarm value used here.
high_warning - Specify the high threshold for the warning. When the operating parameter rises above this value, the action associated with the warning is taken.
<mw_or_dbm> - Enter the high threshold warning value here.
low_warning - Specify the low threshold for the warning. When the operating parameter falls below this value, the action associated with the warning is taken.
<mw_or_dbm> - Enter the low threshold warning value here.

state - (Optional) Specify the DDM state to enable or disable. If the state is disabled, no DDM action will take effect.
enable - Specify to enable the DDM state.
disable - Specify to disable the DDM state.

shutdown - (Optional) Specify whether or not to shutdown the port when the operating parameter exceeds the corresponding alarm threshold or warning threshold. The default value is none.
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-3000-28SC:admin#config ddm ports 25 temperature_threshold high_alarm 84
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

Success.

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

To configure the port 25's voltage threshold:

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

To configure the port 25's bias current threshold:

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

To configure the port 25's transmit power threshold:

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

To configure the port 25's receive power threshold:

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

To configure the port 25's actions associate with the alarm:

```
DGS-3000-28SC:admin#config ddm ports 25 state enable shutdown alarm
Command: config ddm ports 25 state enable shutdown alarm

Success.

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

26-3 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-3000-28SC:admin#show ddm
Command: show ddm

DDM Log           :Enabled
DDM Trap          :Disabled
DDM Tx/Rx Power Unit    : mw

DGS-3000-28SC:admin
```

26-4 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 - Specify that the operating parameter will be displayed.
configuration - Specify that the configuration values will be displayed.

Restrictions

None.

Example

To display ports 25-26's operating parameters:

```
DGS-3000-28SC:admin#show ddm ports 25-26 status
Command: show ddm ports 25-26 status

 Port    Temperature   Voltage    Bias Current   TX Power     RX Power
        (in Celsius)     (V)         (mA)         (mW)         (mW)
------- ------------- ---------- -------------- ---------- ------------
  25         -             -            -            -            -
  26         -             -            -            -            -

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

26-5 config ddm power_unit

Description

This command is used to configure the unit of DDM TX and RX power.

Format

config ddm power_unit [mw | dbm]

Parameters

mw - Specify the DDM TX and RX power unit as mW.

dbm - Specify the DDM TX and RX power unit as dBm.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the DDM TX and RX power unit as dBm:

```
DGS-3000-28SC:admin#config ddm power_unit dbm
Command: config ddm power_unit dbm

Success.

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

Chapter 27 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>}
config duld recover_timer [<value 0> | <sec 60-1000000>]
show duld

27-1 config duld ports

Description

This command is used to configure unidirectional link detection on ports. Unidirectional link detection provides discovery mechanism based on 802.3ah to discovery its neighbor. If the OAM discovery can complete in configured discovery time, it concludes the link is bidirectional. Otherwise, it starts detecting task to detect the link status.

Format

config duld ports [<portlist> | all] {state [enable | disable] | mode [shutdown | normal] | discovery_time <sec 5-65535>}(1)

Parameters

<portlist> - Enter a range of ports.
all - Specify to select all ports.
state - Specify these ports unidirectional link detection status. **enable** - Enables unidirectional link detection status. **disable** - Disables unidirectional link detection status.
mode - Specify 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 - Specify 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-3000-28SC:admin#config duld ports 1 state enable
Command: config duld ports 1 state enable

Success.

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

27-2 show duld ports

Description

This command is used to show unidirectional link detection information.

Format

show duld ports {<portlist>}

Parameters

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

Restrictions

None.

Example

To show ports 1-4 unidirectional link detection information:

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

27-3 config duld recover_timer

Description

This command is used to configure unidirectional link detection auto-recovery time. Zero is a special value which means to disable the auto-recovery mechanism.

Format

config duld recover_timer [<value 0> | <sec 60-1000000>]

Parameters

<value 0> - Enter the specific auto-recover time.
<sec 60-1000000> - Enter the default time of 60 seconds or within the range of 60 to 1000000 seconds.

Restrictions

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

Example

To configure unidirectional link detection auto-recover time to 60 seconds:

```
DGS-3000-28SC:admin# config duld recover_timer 60
Command: config duld recover_timer 60

Success.

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

27-4 show duld

Description

This command is used to show unidirectional link detection global information.

Format

show duld

Parameters

None.

Restrictions

None.

Example

To show unidirectional link detection global information:

```
DGS-3000-28SC:admin# show duld
Command: show duld

DULD Global Settings
------------------------
Recover Time     : 60 sec

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

Chapter 28 Domain Name System (DNS) Relay Command List

config dnsr [[primary | secondary] nameserver <ipaddr> | [add | delete] static <domain_name 32> <ipaddr>]
enable dnsr {[cache | static]}
disable dnsr {[cache | static]}
show dnsr {static}

28-1 config dnsr

Description

This command is used to configure the DNS relay name server of the Switch.

Format

config dnsr [[primary | secondary] nameserver <ipaddr> | [add | delete] static <domain_name 32> <ipaddr>]

Parameters

primary - Specify that the name server is a primary name server.
secondary - Specify the secondary name server.
nameserver - Specify the IP address of the nameserver. **<ipaddr>** - Enter the name server's IP address here.
add - Specify to add the name server IP address.
delete - Specify to delete the name server IP address.
static - Specify the static domain name. **<domain_name 32>** - Enter the doman name with a minimum of 32 characters. **<ipaddr>** - Enter the name server IP address here.

Restrictions

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

Example

To configure 10.43.21.12 as a DNS relay primary name server:

```
DGS-3000-28SC:admin# config dnsr primary nameserver 10.43.21.12
Command: config dnsr primary nameserver 10.43.21.12

Success.

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

To add a static domain name entry (host name: dns1, IP address: 10.43.21.12) to DNS relay resolution table:

```
DGS-3000-28SC:admin# config dnsr add static dns1 10.43.21.12
Command: config dnsr add static dns1 10.43.21.12

Success.

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

To delete a static domain name entry (host name: dns1, IP address: 10.43.21.12) from DNS relay resolution table:

```
DGS-3000-28SC:admin# config dnsr delete static dns1 10.43.21.12
Command: config dnsr delete static dns1 10.43.21.12

Success.

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

28-2 enable dnsr

Description

This command is used to enable DNS Relay.

Format

enable dnsr {[cache | static]}

Parameters

cache - (Optional) Specify the DNS relay lookup cache..
static - (Optional) Specify to disable a static domain name entry from the switch's DNS relay resolution table.

Restrictions

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

Example

To enable DNS Relay:

```
DGS-3000-28SC:admin# enable dnsr
Command: enable dnsr

Success.

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

28-3 disable dnsr

Description

This command is used to disable DNS Relay.

Format

disable dnsr {[cache | static]}

Parameters

cache - (Optional) Specify the DNS relay lookup cache..
static - (Optional) Specify to disable a static domain name entry from the switch's DNS relay resolution table.

Restrictions

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

Example

To disable DNS Relay:

```
DGS-3000-28SC:admin# disable dnsr
Command: disable dnsr

Success.

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

28-4 show dnsr

Description

This command is used to display the DNS Relay.

Format

show dnsr {static}

Parameters

static - Specify to display a static domain name entry from the switch's DNS relay resolution table.

Restrictions

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

Example

To display DNS Relay:

```
DGS-3000-28SC:admin# show dnsr
Command: show dnsr

DNSR Status              : Disabled
Primary Name Server      : 0.0.0.0
Secondary Name Server    : 0.0.0.0
DNSR Cache Status        : Disabled
DNSR Static Table Status : Disabled

DNS Relay Static Table

Domain Name                            IP Address
-------------------------------------  ---------------

Total Entries: 0

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

Chapter 29 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

29-1 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) Specify 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-3000-28SC:admin#config name_server add 10.10.10.10 primary
Command: config name_server add 10.10.10.10 primary

Success.

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

29-2 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) Specify 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-3000-28SC:admin#config name_server delete 10.10.10.1
Command: config name_server delete 10.10.10.1

Success.

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

29-3 config name_server timeout

Description

This command is used to configure the timeout value of a DNS Resolver name server.

Format

config name_server timeout <sec 1-60>

Parameters

<sec 1-60> - Enter the maximum time waiting for a response from a specified name server.

Restrictions

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

Example

To configure DNS Resolver name server time out to 10 seconds:

```
DGS-3000-28SC:admin#config name_server timeout 10
Command: config name_server timeout 10

Success.

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

29-4 show name_server

Description

This command is used to display the current DNS Resolver name servers and name server time out on the Switch.

Format

show name_server

Parameters

None.

Restrictions

None.

Example

To display the current DNS Resolver name servers and name server time out:

```
DGS-3000-28SC:admin#show name_server
Command: show name_server

Name Server Timeout: 3 seconds

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-3000-28SC:admin#
```

29-5 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-3000-28SC:admin#create host_name www.example.com 10.10.10.10
Command: create host_name www.example.com 10.10.10.10

Success.

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

29-6 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 - Specify 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-3000-28SC:admin#delete host_name www.example.com
Command: delete host_name www.example.com

Success.

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

29-7 show host_name

Description

This command is used to display the current host name.

Format

show host_name {static | dynamic}

Parameters

static - (Optional) Specify to display the static host name entries.
dynamic - (Optional) Specify to display the dynamic host name entries.

Restrictions

None.

Example

To display the static and dynamic host name entries:

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

29-8 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-3000-28SC:admin#enable dns_resolver
Command: enable dns_resolver

Success.

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

29-9 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-3000-28SC:admin#disable dns_resolver
Command: disable dns_resolver

Success.

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

Chapter 30 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}(1) | all] {action [drop] | state [enable | disable]}(1)
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]

30-1 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}(1) | all] {action [drop] | state [enable | disable]}(1)

Parameters

land_attack - Specify to check whether the source address is equal to destination address of a received IP packet.
blat_attack - Specify to check whether the source port is equal to destination port of a received TCP packet.
tcp_null_scan - Specify to check whether a received TCP packet contains a sequence number of 0 and no flags
tcp_xmasscan - Specify to check whether a received TCP packet contains URG, Push and FIN flags.
tcp_synfin -) Specify to check whether a received TCP packet contains FIN and SYN flags.
tcp_syn_srcport_less_1024 - Specify to check whether the TCP packets source ports are less than 1024 packets.
ping_death_attack - Specify to detect whether received packets are fragmented ICMP packets.
tcp_tiny_frag_attack - Specify to check whether the packets are TCP tiny fragment packets.
all - Specify all DoS attack type.
action - When enabling DoS prevention, the following actions can be taken. **drop** - Drops DoS attack packets.
state - Specify the DoS attack prevention state. **enable** - Specify to enable DoS attack prevention. **disable** - Specify to disable DoS attack prevention.

Restrictions

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

Example

To configure land attack and blat attack prevention, the action is drop:

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

30-2 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-3000-28SC: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              -
```

30-3 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 - Specify to enable DoS prevetion trap state.
disable - Specify to disable DoS prevention trap state.

Restrictions

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

Example

To disable DoS prevention trap:

```
DGS-3000-28SC:admin#config dos_prevention trap disable
Command: config dos_prevention trap disable

Success.

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

30-4 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 - Specify to enable DoS prevetion log state.
disable - Specify to disable DoS prevention log state.

Restrictions

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

Example

To enable DoS prevention log:

```
DGS-3000-28SC:admin#config dos_prevention log enable
Command: config dos_prevention log enable

Success.

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

Chapter 31 Energy Efficient Ethernet (EEE) Command List

config eee ports [<portlist> | all] state [enable | disable]
show eee ports {<portlist>}

31-1 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 - Specify to configure all ports.
state - Specify 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-3000-28SC:admin#config eee ports 2-5 state enable
Command: config eee ports 2-5 state enable

Success.

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

31-2 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) Enter a list of ports to be displayed.

Restrictions

None.

Example

To display the EEE state:

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

Chapter 32 Ethernet Ring Protection Switching (ERPS) Command List

enable erps
disable erps
create erps raps_vlan <vlanid 1-4094>
delete erps raps_vlan <vlanid 1-4094>
config erps raps_vlan <vlanid 1-4094> [state [enable | disable] | ring_mel <value 0-7> | ring_port [west [<port> | virtual_channel] | east [<port> | virtual_channel]] | rpl_port [west | east | none] | rpl_owner [enable | disable] | protected_vlan [add | delete] vlanid <vidlist> | sub_ring raps_vlan <vlanid 1-4094> tc_propagation state [enable | disable] | [add | delete] sub_ring raps_vlan <vlanid 1-4094> | revertive [enable | disable] | timer {holdoff_time <millisecond 0 - 10000> | guard_time <millisecond 10 - 2000 > | wtr_time <min 1 - 12>}]
config erps log [enable | disable]
show erps {raps_vlan <vlanid 1-4094> {sub_ring}}
config erps trap [enable | disable]

32-1 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 sepcified as virtual channel.

NOTE: The default state is disabled.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-3000-28SC:admin#enable erps
Command: enable erps

Success.

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

32-2 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-3000-28SC:admin#disable erps
Command: disable erps

Success.

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

32-3 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 1-4094>

Parameters

<vlanid 1-4094> - Enter the VLAN which will be the R-APS VLAN.

Restrictions

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

Example

To create an R-APS VLAN:

```
DGS-3000-28SC:admin#create erps raps_vlan 4094
Command: create erps raps_vlan 4094

Success.

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

32-4 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 1-4094>

Parameters

<vlanid 1-4094> - Enter the VLAN which will be the R-APS VLAN**.**

Restrictions

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

Example

To delete an R-APS VLAN:

```
DGS-3000-28SC:admin#delete erps raps_vlan 4094
Command: delete erps raps_vlan 4094

Success.

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

32-5 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 can be modified when ERPS is enabled.

RPL port - Specify 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 - Specify the node as the RPL owner.

Note that the RPL port and RPL owner can 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.

When both the global state and the specified ring ERPS state are enabled, the specified ring will be activated. STP and LBD should be disabled on the ring ports before the specified ring is activated.

The ring cannot be enabled before the R-APS VLAN is created, and ring ports, RPL port, 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 1-4094> [state [enable | disable] | ring_mel <value 0-7> | ring_port [west [<port> | virtual_channel] | east [<port> | virtual_channel]] | rpl_port [west | east | none] | rpl_owner [enable | disable] | protected_vlan [add | delete] vlanid <vidlist> | sub_ring raps_vlan <vlanid 1-4094> tc_propagation state [enable | disable] | [add | delete] sub_ring raps_vlan <vlanid 1-4094> | revertive [enable | disable] | timer {holdoff_time <millisecond 0 - 10000> | guard_time <millisecond 10 - 2000 > | wtr_time <min 1 - 12>}]

Parameters

<vlanid 1-4094> - Enter the VLAN ID used here.
state - Specify 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 - Specify 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 - Specify the ring port used. **west** - Specify that the port or the virtual channel will be associated with the west ring port. **<port>** - Enter the port number here. **virtual_channel** - Specify that the virtual channel will be associated with the west ring port. **east** - Specify that the port or the virtual channel will be associated with the east ring port. **<port>** - Enter the port number here. **virtual_channel** - Specify that the virtual channel will be associated with the east ring port.
rpl_port - Specify the RPL port used. **west** - Specify the west ring port as the RPL port. **east** - Specify 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 - Specify to enable or disable the RPL owner node. **enable** - Specify the device as an RPL owner node. **disable** - This node is not an RPL owner. By default, the RPS owner is disabled.
protected_vlan - Specify to add or delete the protected VLAN group. **add** - Add VLANs to the protected VLAN group. **delete** - Delete VLANs from the protected VLAN group. **vlanid** - Specify the VLAN ID to be removed or added. **<vidlist>** - Enter the VLAN ID list here.
sub_ring - Specify that the sub-ring is being configured. **raps_vlan** - Specify the R-APS VLAN.

<vlanid 1-4094> - Enter the VLAN ID used here. **tc_propogation** - Specify to configure the state of the topology change propagation for the sub-ring. **state** - Specify the propagation state of the topology change for the sub-ring. **enable** - Enable the propagation state of the topology change for the sub-ring. **disable** - Disable the propagation state of the topology change for the sub-ring.
add - Specify to connect a sub-ring to another ring.
delete - Specify to disconnect a sub-ring from the connected ring. **sub_ring** - Specify the sub-ring configuration information. **raps_vlan** - Specify the R-APS VLAN. **<vlanid 1-4094>** - Enter the R-APS VLAN ID used here
revertive - Specify the state of the R-APS revertive option. **enable** - Specify that the R-APS revertive option will be enabled. **disable** - Specify that the R-APS revertive option will be disabled.
timer - Specify the R-APS timer used. **holdoff_time** - (Optional) Specify 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 millseconds. **guard_time** - (Optional) Specify 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 millseconds. **wtr_time** - (Optional) Specify the WTR time of the R-APS function. **<min 1-12>** - Enter the WTR time range value here. The range is from 1 to 12 minutes. The default WTR time is 5 minutes.

Restrictions

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

Example

To configure the MEL of the ERPS ring for a specific R-APS VLAN:

```
DGS-3000-28SC:admin#config erps raps_vlan 4094 ring_mel 2
Command: config erps raps_vlan 4094 ring_mel 2

Success.

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

To set the R-APS east ring port parameter to 7:

```
DGS-3000-28SC:admin#config erps raps_vlan 4094 ring_port east 7
Command: config erps raps_vlan 4094 ring_port east 7

Success.

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

To configure the RPL port for a specific R-APS VLAN:

```
DGS-3000-28SC:admin#config erps raps_vlan 4094 rpl_port west
Command: config erps raps_vlan 4094 rpl_port west

Success.

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

To configure the protected VLAN for a specific R-APS VLAN:

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

To configure the ERPS timers for a specific R-APS VLAN:

```
DGS-3000-28SC: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_t
ime 10

Success.

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

To configure the ring state of the ERPS:

```
DGS-3000-28SC:admin#config erps raps_vlan 4094 state enable
Command: config erps raps_vlan 4094 state enable

Success.

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

To configure a sub-ring connected to another ring:

```
DGS-3000-28SC:admin# config erps raps_vlan 4094 add sub_ring raps_vlan 4093
Command: config erps raps_vlan 4094 add sub_ring raps_vlan 4093

Success.

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

To configure the state of topology change propagation:

```
DGS-3000-28SC:admin# config erps raps_vlan 4094 sub_ring raps_vlan 4093
tc_propagation state enable
Command: config erps raps_vlan 4094 sub_ring raps_vlan 4093 tc_propagation
state enable

Success.

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

32-6 config erps log

Description

This command is used to configure the log state of the ERPS events.

Format

config erps log [enable | disable]

Parameters

enable - Specify to enable an ERPS event in the log state.
disable - Specify to disable an ERPS event in the log state.

Restrictions

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

NOTE: The default value is disabled.

Example

To enable the ERPS log state:

```
DGS-3000-28SC:admin# config erps log enable
Command: config erps log enable

Success.

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

32-7 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.

This command displays both admin value and operational value of ring port. The admin value is the latest user configuration. The operational value is actual running configuration. Sometimes, modifying a ring needs more than one command. Before user configure complete, the current configuration may invalid. In this case, to avoid temporary loop, user configuration will not apply to state machine immediately. The ERPS will run protocol by previous configuration which is valid. If the admin value is different from the operational value, it means that the new configuration is not applied.

Both RPL port and RPL owner have admin value and operational value, the reason is same as ring port.

If ERPS is disabled on a ring, the admin value of this ring, is applied to the operational value immediately.

If ERPS is enabled on a ring, the admin value of this ring, is applied to the operational value only when all of the following conditions are satisfied:

1. The Ring port is a tagged member port of the R-APS VLAN.

2. The RPL port is specified if the RPL owner is enabled.

3. The RPL port is not a virtual channel.

4. The Ring port is the master port if it belongs to a link aggregation group.

Save function will record the operational value if the operational value is different form the admin value.

Format

show erps {raps_vlan <vlanid 1-4094> {sub_ring}}

Parameters

raps_vlan - (Optional) Specify the R-APS VLAN. **<vlanid 1-4094>** - Enter the VLAN ID between 1-4094. **sub_ring** - (Optional) Display the sub-ring configuration information.

Restrictions

None.

Example

To display ERPS information:

```
DGS-3000-28SC:admin#show erps
Command: show erps

ERPS Information
Global Status         : Enabled
Log Status            : Disabled
Trap Status           : Disabled
------------------------
R-APS VLAN            : 4092
Ring Status           : Enabled
Admin West Port       : 5
Operational West Port : 5 (Blocking)
Admin East Port       : 7
Operational East Port : 7 (Forwarding)
Admin RPL Port        : None
Operational RPL Port  : West Port
Admin RPL Owner       : Enabled
Operational RPL Owner : Enabled
Protected VLANs       : 100-300, 4093, 4094
Ring MEL              : 2
Revertive             : Enabled
Holdoff Time          : 0 milliseconds
Guard Time            : 500 milliseconds
WTR Time              : 5 minutes
Revertive mode        : Disabled
Current Ring State    : Idle
------------------------
R-APS VLAN            : 4093
Ring Status           : Enabled
Admin West Port       : 5
Operational West Port : Virtual Channel
Admin East Port       : 10
Operational East Port : 10 (Forwarding)
Admin RPL Port        : None
Operational RPL Port  : None
Admin RPL Owner       : Enabled
Operational RPL Owner : Disabled
Protected VLANs       : 200-220
Ring MEL              : 2
Revertive             : Enabled
Holdoff Time          : 0 milliseconds
Guard Time            : 500 milliseconds
WTR Time              : 5 minutes
Revertive mode        : Disabled
Current Ring State    : Idle
------------------------
R-APS VLAN            : 4094
Ring Status           : Enabled
Admin West Port       : Virtual Channel
Operational West Port : Virtual Channel
Admin East Port       : 12
Operational East Port : 12 (Forwarding)
```

```
Admin RPL Port        : None
Operational RPL Port  : None
Admin RPL Owner       : Disabled
Operational RPL Owner : Disabled
Protected VLANs       : 250-300
Ring MEL              : 2
Revertive             : Enabled
Holdoff Time          :  0 milliseconds
Guard Time            : 500 milliseconds
WTR Time              :  5 minutes
Revertive mode        : Disabled
Current Ring State    : Idle
------------------------
Total Ring: 3

DGS-3000-28SC:N#show erps raps_vlan 4092 sub_ring
Command: show erps raps_vlan 4092 sub_ring
R-APS VLAN: 4092
Sub-Ring R-APS VLAN     TC Propagation State
------------------      --------------------
4093                       Enabled
4094                       Enabled
-------------------------------------------
Total Sub-Ring Connected: 2

DGS-30000-28SC:admin#
```

32-8 config erps trap

Description

This command is used to configure the trap state of ERPS events.

Format

config erps trap [enable | disable]

Parameters

enable - Specify to enable the ERPS trap state. The default value is disabled.
disable - Specify to disable the ERPS trap state

Restrictions

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

Example

To enable the ERPS trap state:

```
DGS-3000-28SC:admin# config erps trap enable
Command: config erps trap enable

Success.

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

Chapter 33 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 fdb vlan_learning [<vlan_name32> | vlanid <vidlist>] state [enable | disable]
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 | vlan_learning {[<vlan_name32> | vlanid <vidlist>]}]}
show multicast vlan_filtering_mode {[vlanid < vidlist> | vlan <vlan_name 32>]}

33-1 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> - Enter a VLAN name associated with a MAC address. The maximum length of the VLAN name is 32 bytes.
<macaddr> - Enter 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 - Specify 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-3000-28SC: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-3000-28SC:admin#
```

To filter a unicast MAC:

```
DGS-3000-28SC:admin#create fdb default 00-00-00-00-01-02 drop
Command: create fdb default 00-00-00-00-01-02 drop

Success.

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

33-2 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> - Enter a VLAN ID associated with a MAC address.
<macaddr> - Enter 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 - Specify 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-3000-28SC: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-3000-28SC:admin#
```

To filter a unicast MAC:

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

33-3 create multicast_fdb

Description

This command is used to create a static entry in the multicast MAC address forwarding table (database).

Format

create multicast_fdb <vlan_name 32> <macaddr>

Parameters

<vlan_name 32> - Enter the VLAN name on which the MAC address resides. The maximum name length is 32.
<macaddr> - Enter the multicasts MAC address to be added to the static forwarding table.

Restrictions

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

Example

To create a multicast MAC forwarding entry to the default VLAN:

```
DGS-3000-28SC:admin#create multicast_fdb default 01-00-00-00-00-01
Command: create multicast_fdb default 01-00-00-00-00-01

Success.

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

33-4 config multicast_fdb

Description

This command is used to configure the Switch's multicast MAC address forwarding database.

Format

config multicast_fdb <vlan_name 32> <macaddr> [add | delete] <portlist>

Parameters

<vlan_name 32> - Enter the VLAN name on which the MAC address resides. The maximum name length is 32.
<macaddr> - Enter the MAC address that will be added or deleted to the forwarding table.
add - Specify to add ports to the multicast forwarding table.
delete - Specify to remove ports from the multicast forwarding table.
<portlist> - Enter a range of ports to be configured.

Restrictions

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

Example

To add a multicast MAC forwarding entry to the default VLAN on port 1 to 5:

```
DGS-3000-28SC:admin#config multicast_fdb default 01-00-00-00-00-01 add 1-5
Command: config multicast_fdb default 01-00-00-00-00-01 add 1-5

Success.

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

33-5 config fdb aging_time

Description

This command is used to configure the MAC address table aging time. The aging time affects the learning process of the Switch. Dynamic forwarding table entries, which are made up of the source MAC addresses and their associated port numbers, are deleted from the table if they are not accessed within the aging time. 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.

Format

config fdb aging_time <sec 10-1000000>

Parameters

<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-3000-28SC:admin#config fdb aging_time 600
Command: config fdb aging_time 600

Success.

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

33-6 config fdb vlan_learning

Description

This command is used to enable or disable FDB learning state base on VLAN.

By default, MAC address learning will always be enabled on all VLANs on the switch when a user creates VLAN. MAC address learning. It will be recovered to the default value when a user deletes the VLAN. MAC address learning can only be configured on an existing VLAN.Disabling MAC address learning on a VLAN will cause all port members in this VLAN to stop the MAC address learning. Disabling MAC address learning on the Voice or Surveillance VLAN, these function will be working abnormally based on the MAC address learning. Disabling MAC address learning on a VLAN will cause Asymmetric VLAN work abnormal on a related VLAN. Disabling the MAC address learning on a Private VLAN will cause related Private VLAN work abnormal. RSPAN VLAN has the higher precedence, MAC address learning always is disabled on the RSPAN VLAN, and if you delete the RSPAN VLAN, the configured MAC address learning state will be active. The MAC address learning for secure module have the higher precedence, If you disable MAC address learning on a VLAN that includes a secure port, MAC address learning is not disabled on the VLAN. If you disable all of the secure member ports on the VLAN, the configured MAC address learning state is active.

(Note: The secure module: Port-Security, 802.1x, MAC-based Access Control, WAC, IP-MAC-Port binding).

Format

config fdb vlan_learning [<vlan_name32> | vlanid <vidlist>] state [enable | disable]

Parameters

<vlan_name32> - Enter the VLAN name. It should be 32 characters long.
vlanid - Specify a list of VLAN's based on their VLAN ID. **<vidlist>** - Enter a VLAN ID here.
state - Specify the database state. **enable** - Specify to enable VLAN learning. **disable** - Specify to disable VLAN learning.

Restrictions

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

Example

To disable FDB learning on the VLAN 1:

```
DGS-3000-28SC:admin# config fdb vlan_learning vlanid 1 state disable
Command: config fdb vlan_learning vlanid 1 state disable

Success.

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

33-7 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 - Specify a list of VLANs to be configured. **<vidlist>** - Enter the VLAN ID list here.
vlan - Specify the name of the VLAN. The maximum name length is 32. **<vlan_name 32>** - Enter the VLAN name can be up to 32 characters long.
all - Specify 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-3000-28SC: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-3000-28SC:admin#
```

33-8 delete fdb

Description

This command is used to delete a static entry from the forwarding database.

Format

delete fdb <vlan_name 32> <macaddr>

Parameters

<vlan_name 32> - Enter VLAN name on which the MAC address resides. The maximum name length is 32.
<macaddr> - Enter the multicast MAC address to be deleted from the static forwarding table.

Restrictions

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

Example

To delete a static FDB entry:

```
DGS-3000-28SC:admin#delete fdb default 00-00-00-00-01-02
Command: delete fdb default 00-00-00-00-01-02

Success.

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

33-9 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>** - Enter the VLAN name on which the MAC address resides. The maximum name length is 32.
port - Clears the FDB entry by specifying the port number. **<port>** - Enter 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-3000-28SC:admin#clear fdb all
Command: clear fdb all

Success.

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

33-10 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) Specify 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-3000-28SC:admin#show multicast_fdb
Command: show multicast_fdb


 VLAN Name      : default
 MAC Address    : 01-00-00-00-00-01
 Egress Ports   : 1-5
 Mode           : Static


Total Entries: 1


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

33-11 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 | vlan_learning {[<vlan_name32> | vlanid <vidlist>]}]}

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.
vlan_learning - (Optional) Specify to display the FDB learning state. If no parameter is specified, the system will display the unicast address table. **<vlan_name32>** - (Optional) Enter the VLAN name here. **vlanid** - (Optional) Specify the VLAN ID here. **<vidlist>** - Enter the VLAN list here.
If no parameter is specified, system will display the unicast address table.

Restrictions

None.

Example

To display the FDB table:

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

To display the security FDB table:

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

33-12 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) Specify a list of VLANs to be configured. **<vidlist>** - Enter the VLAN ID list here.
vlan - (Optional) Specify 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-3000-28SC: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-3000-28SC:admin#
```

Chapter 34 Filter NetBIOS 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

34-1 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> - Enter the portlist to configure the filter netbios.
all - Specify to add all the ports to the configuration.
state - Specify the state to block the NetBIOS packets. **enable** - Specify to enable to block the NetBIOS packet. **disable** - Specify to disable to block the NetBIOS packet

Restrictions

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

Example

To configure filter NetBIOS state:

```
DGS-3000-28SC:admin# config filter netbios 1-10 state enable
Command: config filter netbios 1-10 state enable

Success.

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

34-2 show filter netbios

Description

This command is used to display the filter NetBIOS state on the switch.

Format

show filter netbios

Parameters

None.

Restrictions

None.

Example

To display the filter NetBIOS state:

```
DGS-3000-28SC:admin# show filter netbios
Command: show filter netbios

Enabled ports: 1-3

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

34-3 config filter extensive_netbios

Description

This command is used to configure the Switch to filter NetBIOS packets over 802.3 flame on the specific ports.

Format

config filter extensive_netbios <portlist | all> state [enable | disable]

Parameters

<portlist> - Enter the portlist to configure the filter extensive netbios.
all - Specify to add all the ports to the configuration.
state - Specify the state to filter to block the NetBIOS packet over 802.3 frame. **enable** - Specify to enable to block the NetBIOS packet over 802.3. **disable** - Specify to disable to block the NetBIOS packet over 802.3.

Restrictions

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

Example

To configure filter extensive NetBIOS state:

```
DGS-3000-28SC:admin# config filter extensive_netbios 1-10 state enable
Command: config filter extensive_netbios 1-10 state enable

Success.

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

34-4 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 filter extensive NetBIOS state:

```
DGS-3000-28SC:admin# show filter extensive_netbios
Command: show filter extensive_netbios

Enabled ports: 1-3

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

Chapter 35 Flash File System (FFS) Command List

show storage_media_info {[unit <unit_id> | all]}
change drive {unit <unit_id>} <drive_id>
md {{unit<unit_id>} <drive_id>} <pathname>
rd {{unit <unit_id>} <drive_id>} <pathname>
cd {<pathname>}
dir {{unit<unit_id>} <drive_id>} {<pathname>}
rename {{unit <unit_id>} <drive_id>} <pathname> <filename>
del {{unit <unit_id>} <drive_id>} <pathname> {recursive}
erase {{unit <unit_id>} <drive_id>} <pathname>
move {{unit <unit_id>} <drive_id>} <pathname> {{unit <unit_id>} <drive_id>} <pathname>
copy {{unit <unit_id>} <drive_id>} <pathname> {{unit <unit_id>} <drive_id>} <pathname>

35-1 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 {[unit <unit_id> | all]}

Parameters

unit - (Optional) Specify a unit ID if in the stacking system. **<unit_id>** - Enter the unit ID value. This value must be between 1 and 6. **all** - Specify all storage media units.
If no parameter is specified, the master unit is applied.

Restrictions

None.

Example

To display the storage media's information:

```
DGS-3000-28SC:admin#show storage_media_info
Command: show storage_media_info

Drive  Media Type      Size  Label        FS Type
-----  ----------  --------  -----------  -------
c:/    Flash          28 MB               FFS

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

35-2 change drive

Description

This command is used to change the current drive.

Format

change drive {unit <unit_id>} <drive_id>

Parameters

unit - (Optional) Specify a unit ID if in the stacking system. If not specified, it refers to the master unit. **<unit_id>** - Enter the unit ID value. This value must be between 1 and 6.
<drive_id> - Specify the drive ID. The format of drive_id is C:.

Restrictions

None.

Example

To display the storage media's information:

```
DGS-3000-28SC:admin# change drive unit 3 c:
Command: change drive unit 3 c:

Success.

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

35-3 md

Description

This command is used to create a directory.

Format

md {{unit <unit_id>} <drive_id>} <pathname>

Parameters

unit - (Optional) Specify a unit ID if in the stacking system. If not specified, it refers to the master unit. **<unit_id>** - Enter the unit ID value. This value must be between 1 and 6.
<drive_id> - (Optional) Enter the drive ID used here. Examples are C:
<pathname> - Specify 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. 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-3000-28SC:admin#md c:/abc
Command: md c:/abc

Success.

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

35-4 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 {{unit <unit_id>} <drive_id>} <pathname>

Parameters

unit - (Optional) Specify a unit ID if in the stacking system. If not specified, it refers to the master unit. **<unit_id>** - Enter the unit ID value. This value must be between 1 and 6.
<drive_id> - (Optional) Enter the drive ID used here. Examples are C:
<pathname> - Specify 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-3000-28SC:admin#rd c:/abc
Command: rd c:/abc

Success.

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

35-5 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) Enter 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-3000-28SC:admin#cd
Command: cd

Current work directory: "/c:".

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

35-6 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 {{unit <unit_id>} <drive_id>} {<pathname>}

Parameters

unit - (Optional) Specify a unit ID if in the stacking system. If not specified, it refers to the master unit. **<unit_id>** - Enter the unit ID value. This value must be between 1 and 6.
<drive_id> - (Optional) Enter the drive ID used, for example, C:.
<pathname> - (Optional) Enter 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-3000-28SC:admin#dir
Command: dir

Directory of /c:

Idx Info    Attr Size     Update Time         Name
--- ------- ---- -------- ------------------- ----------------
  1 CFG(*)  -rw- 39192    2000/02/25 00:41:03 config.cfg
  2 RUN(b)  -rw- 9163584  2000/02/03 02:19:40 5.00.020
  3 RUN(*)  -rw- 9027396  2000/02/24 07:02:27 sw_test
  4         d---          2000/01/01 23:07:34 system

29937 KB total (11579 KB free)
(*) -with boot-up info          (b) -with backup info

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

35-7 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 Specify the file (in path form) to be renamed and the filename Specify 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 {{unit <unit_id>} <drive_id>} <pathname> <filename>

Parameters

unit - (Optional) Specify a unit ID if in the stacking system. If not specified, it refers to the master unit. **<unit_id>** - Enter the unit ID value. This value must be between 1 and 6.
<drive_id> - (Optional) Enter the drive ID used here. Examples are C:
<pathname> - Specify the file (in path form) to be renamed.
<filename> - Specify the new name of the file.

Restrictions

Only Administrators and Operators can issue this command.

Example

To rename a file:

```
DGS-3000-28SC:admin#rename run.had run1.had
Command: rename run.had run1.had

Success.

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

35-8 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 boot-up.

Format

del {{unit <unit_id>} <drive_id>} <pathname> {recursive}

Parameters

unit - (Optional) Specify a unit ID if in the stacking system. If not specified, it refers to the master unit. **<unit_id>** - Enter the unit ID value. This value must be between 1 and 6.
<drive_id> - (Optional) Enter the drive ID used, for example, C:.
<pathname> - Enter 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) Specify 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-3000-28SC: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 runtime.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-3000-28SC:admin#del 12 recursive
Command: del 12 recursive

Success.

DGS-3000-28SC: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 runtime.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-3000-28SC:admin#
```

35-9 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 {{unit <unit_id>} <drive_id>} <pathname>

Parameters

unit - (Optional) Specify a unit ID if in the stacking system. If not specified, it refers to the master unit. **<unit_id>** - Enter the unit ID value. This value must be between 1 and 6.
<drive_id> - (Optional) Enter the drive ID used here. Examples are C:
<pathname> - Specify 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-3000-28SC: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 runtime.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-3000-28SC:admin#erase config2.cfg
Command: erase config2.cfg

Success.

DGS-3000-28SC: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 runtime.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-3000-28SC:admin#
```

35-10 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 {{unit <unit_id>} <drive_id>} <pathname> {{unit <unit_id>} <drive_id>} <pathname>

Parameters

unit - (Optional) Specify a unit ID if in the stacking system. If not specified, it refers to the master unit. **<unit_id>** - Enter the unit ID value. This value must be between 1 and 6.
<drive_id> - (Optional) Enter the drive ID used here. Examples are C:
<pathname> - Specify the file to be moved. The path name can be specified either as a full path name or partial name. Specified either as a full path name or partial name. For partial path name, it indicates the file is in the current directory.
unit - (Optional) Specify a unit ID if in the stacking system. If not specified, it refers to the master unit. **<unit_id>** - Enter the unit ID value. This value must be between 1 and 6.
<drive_id> - (Optional) Enter the drive ID used here. Examples are C:
<pathname> - Specify 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-3000-28SC:admin#move c:/log.txt c:/log1.txt
Command: move c:/log.txt c:/log1.txt

Success.

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

35-11 copy

Description

This command is used to copy a file to another file in the file system.

Format

copy {{unit <unit_id>} <drive_id>} <pathname> {{unit <unit_id>} <drive_id>} <pathname>

Parameters

unit - (Optional) Specify the unit to copy. **<unit_id>** - Enter the unit ID here.
<drive_id> - (Optional) Enter the drive ID, for example, C:.
<pathname> - Enter 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.
unit - (Optional) Specify the pathname unit ID here. **<unit_id>** - Enter the pathname unit ID here.
<drive_id> - (Optional) Enter the drive ID, for example, C:.
<pathname> - Enter 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-3000-28SC:admin#copy c:/log.txt c:/log1.txt
Command: copy c:/log.txt c:/log1.txt

Success.

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

Chapter 36 FTP Client Command List

download firmware_fromFTP [[<ipaddr> | <ipv6addr>] {tcp_port <tcp_port_number 1-65535>} src_file <path_filename 64> | ftp:<string 128 >] {[unit <unit_id> | all]} {dest_file <path_filename 64> {boot_up}}
upload firmware_toFTP [[<ipaddr> | <ipv6addr>] {tcp_port <tcp_port_number 1-65535>} dest_file <path_filename 64> | ftp: <string 128>] {unit <unit_id>} {src_file <pathname 64>}
download cfg_fromFTP [[<ipaddr> | <ipv6addr>] {tcp_port < tcp_port_number 1-65535>} src_file <path_filename 64> | ftp:<string 128 >] {[unit <unit_id> | all]} {dest_file <path_filename 64>}
upload cfg_toFTP [[<ipaddr> | <ipv6addr>] {tcp_port <tcp_port_number 1-65535>} dest_file <path_filename 64> | ftp: <string 128>] {unit <unit_id>} {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>}}}}}
upload log_toFTP [[<ipaddr> | <ipv6addr>] {tcp_port <tcp_port_number 1-65535>} dest_file <path_filename 64> | ftp: <string 128>]
upload attack_log_toFTP [[<ipaddr> | <ipv6addr>] {tcp_port <tcp_port_number 1-65535>} dest_file <path_filename 64> | ftp: <string 128>] {unit <unit_id>}

36-1 download firmware_fromFTP

Description

This command is used to download a firmware image file from the FTP server.

Format

download firmware_fromFTP [[<ipaddr> | <ipv6addr>] {tcp_port <tcp_port_number 1-65535>} src_file <path_filename 64> | ftp:<string 128 >] {[unit <unit_id> | all]} {dest_file <path_filename 64> {boot_up}}

Parameters

<ipaddr> - Enter the IPv4 address of the FTP server here.
<ipv6addr> - Enter the IPv6 address of the FTP server here.
tcp_port - (Optional) Specify the TCP port number used for the FTP connection. **<tcp_port_number 1-65535>** - Enter the TCP port number here. This value must be between 1 and 65535.
src_file - Specify the source file's name and path. **<path_filename 64>** - Enter the source file's name and path here. This can be up to 64 characters long.
ftp - Specify the FTP connection details. **<string 128>** - Enter the FTP connection details here. For example, john:123456@172.18.211.41:21/image/cfg.txt.
unit - (Optional) Specify the unit ID. **<unit_id>** - Enter the unit ID here.
all - (Optional) Specify all the unit ID's.
dest_file - (Optional) Specify the destination file name and path. **<path_filename 64>** - Enter the destination file name and path here. This can be up to 64 characters long. **boot_up** - (Optional) Specify that the firmware will be used as the boot-up firmware after the download was completed successfully.

Restrictions

Only Administrators can issue this command.

Examples

This example shows how to download a firmware file from an FTP server.

```
DGS-3000-28SC:admin# download firmware_fromFTP 10.54.71.1 tcp_port 21 px.had
Command: download firmware_fromFTP 10.54.71.1 tcp_port 21 px.had

Connecting to server.................. Done.
User(Anonymous): john
Pass:******
Download firmware..................... Done.  Do not power off!
Please wait, programming flash......... Done.

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

This example shows how to download a firmware form an FTP server using a string.

```
DGS-3000-28SC:admin# download firmware_fromFTP ftp:
john:123456@10.54.71.1:21/image/px.had
Command: download firmware_fromFTP ftp: john:123456@10.54.71.1:21/image/px.had

Connecting to server.................. Done.
Download firmware..................... Done.  Do not power off!
Please wait, programming flash......... Done.

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

36-2 upload firmware_toFTP

Description

This command is used to upload a firmware from the Switch to an FTP server.

Format

upload firmware_toFTP [[<ipaddr> | <ipv6addr>] {tcp_port <tcp_port_number 1-65535>} dest_file <path_filename 64> | ftp: <string 128>] {unit <unit_id>} {src_file <pathname 64>}

Parameters

<ipaddr> - Enter the IPv4 address of the FTP server here.
<ipv6addr> - Enter the IPv6 address of the FTP server here.
tcp_port - (Optional) Specify the TCP port number used for the FTP connection. **<tcp_port_number 1-65535>** - Enter the TCP port number here. This value must be between 1 and 65535.
dest_file - Specify the destination file name and path. **<path_filename 64>** - Enter the destination file name and path here. This can be up to 64 characters long.
ftp: - Specify the FTP connection details.

<string 128> - Enter the FTP connection details here.
unit - (Optional) Specify which unit on the stacking system. If it is not specified, it refers to the master unit. **<unit_id>** - Enter the unit ID value. This value must be between 1 and 6.
src_file - (Optional) Specify the source file's name and path. **<pathname 64>** - Enter the source file's name and path here. This can be up to 64 characters long.

Restrictions

Only Administrators and Operators can issue this command.

Example

This example shows how to upload a firmware file from the Switch to an FTP server.

```
DGS-3000-28SC:admin# upload firmware_toFTP ftp:
john:123456@10.54.71.1:21/image/image.had runtime.had
Command: upload firmware_toFTP ftp: john:123456@10.54.71.1:21/image/image.had
runtime.had

 Connecting to server.................. Done.
 Upload firmware....................... Done.

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

36-3 download cfg_fromFTP

Description

This command is used to download a configuration file from an FTP server.

Format

download cfg_fromFTP [[<ipaddr> | <ipv6addr>] {tcp_port < tcp_port_number 1-65535>} src_file <path_filename 64> | ftp:<string 128 >] {[unit <unit_id> | all]} {dest_file <path_filename 64>}

Parameters

<ipaddr> - Enter the IPv4 address of the FTP server here.
<ipv6addr> - Enter the IPv6 address of the FTP server here.
tcp_port - (Optional) Specify the TCP port number used for the FTP connection. **<tcp_port_number 1-65535>** - Enter the TCP port number here. This value must be between 1 and 65535.
src_file - Specify the source file's name and path. **<path_filename 64>** - Enter the source file's name and path here. This can be up to 64 characters long.
ftp: - Specify the FTP connection details. **<string 128>** - Enter the FTP connection details here. For example, john:123456@172.18.211.41:21/image/cfg.txt.
unit - (Optional) Specify the unit used. **<unit_id>** - Enter the unit ID value here.
all - (Optional) Specify all the unit ID's.

dest_file - (Optional) Specify the destination file name and path. **<path_filename 64>** - Enter the destination file name and path here. This can be up to 64 characters long.

Restrictions

Only Administrators can issue this command.

Examples

This example shows how to download the configuration file from an FTP server.

```
DGS-3000-28SC:admin# download cfg_fromFTP 10.54.71.1 cfg01.txt 1
Command: download cfg_fromFTP 10.54.71.1 cfg01.txt 1

Connecting to server.................. Done.
User(Anonymous): john
Pass:******
Download configuration................. Done.

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

This example shows how to download the configuration file from an FTP server using a string.

```
DGS-3000-28SC:admin# download cfg_fromFTP ftp:
john:123456@10.90.90.15:21/cfg.txt 2
Command: download cfg_fromFTP ftp: john:123456@10.90.90.15:21/cfg.txt 2

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

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

36-4 upload cfg_toFTP

Description

This command is used to upload a configuration file from the Switch to an FTP server.

Format

upload cfg_toFTP [[<ipaddr> | <ipv6addr>] {tcp_port <tcp_port_number 1-65535>} dest_file <path_filename 64> | ftp: <string 128>] {unit <unit_id>} {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>}}}}}

Parameters

<ipaddr> - Enter the IPv4 address of the FTP server here.
<ipv6addr> - Enter the IPv6 address of the FTP server here.
tcp_port - (Optional) Specify the TCP port number used for the FTP connection.

<tcp_port_number 1-65535> - Enter the TCP port number here. This value must be between 1 and 65535.
dest_file - Specify the destination file name and path. **<path_filename 64>** - Enter the destination file name and path here. This can be up to 64 characters long.
ftp: - Specify the FTP connection details. **<string 128>** - Enter the FTP connection details here. For example, john:123456@172.18.211.41:21/image/cfg.txt.
unit - (Optional) Specify which unit on the stacking system. If it is not specified, it refers to the master unit. **<unit_id>** - Enter the unit ID value. This value must be between 1 and 6.
src_file – (Optional) Specify the source file's name and path. **<path_filename 64>** - Enter the source file's name and path here. This can be up to 64 characters long.
include – (Optional) Specify to include a filter string. **exclude** - (Optional) Specify to exclude a filter string. **begin** - (Optional) Specify to use a filter string that begins with the string specified. **<filter_string 80>** - Enter a filter string enclosed by the quotation mark symbol. Thus, the filter string itself cannot contain the quotation mark character. The filter string is case sensitive. **<filter_string 80>** - (Optional) Enter a filter string enclosed by the quotation mark symbol. **<filter_string 80>** - (Optional) Enter a filter string enclosed by the quotation mark symbol.
include – (Optional) Specify to include a filter string. **exclude** - (Optional) Specify to exclude a filter string. **begin** - (Optional) Specify to use a filter string that begins with the string specified. **<filter_string 80>** - Enter a filter string enclosed by the quotation mark symbol. Thus, the filter string itself cannot contain the quotation mark character. The filter string is case sensitive. **<filter_string 80>** - (Optional) Enter a filter string enclosed by the quotation mark symbol. **<filter_string 80>** - (Optional) Enter a filter string enclosed by the quotation mark symbol.
include – (Optional) Specify to include a filter string. **exclude** - (Optional) Specify to exclude a filter string. **begin** - (Optional) Specify to use a filter string that begins with the string specified. **<filter_string 80>** - Enter a filter string enclosed by the quotation mark symbol. Thus, the filter string itself cannot contain the quotation mark character. The filter string is case sensitive. **<filter_string 80>** - (Optional) Enter a filter string enclosed by the quotation mark symbol. **<filter_string 80>** - (Optional) Enter a filter string enclosed by the quotation mark symbol.

Restrictions

Only Administrators and Operators can issue this command.

Examples

This example shows how to upload the configuration file to an FTP server in the interactive mode.

```
DGS-3000-28SC:admin# upload cfg_toFTP 10.90.90.15 cfg.txt
Command: upload cfg_toFTP 10.90.90.15 cfg.txt

Connecting to server.................. Done.
User(Anonymous): john
Password:******
Upload configuration.................. Done.

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

This example shows how to upload the configuration file to an FTP server using a string.

```
DGS-3000-28SC:admin# download cfg_fromFTP ftp: john:123456@10.90.90.15:21/cfg/
cfg.txt config_id 2
Command: download cfg_fromFTP ftp: john:123456@10.90.90.15:21/cfg/cfg.txt
config_id 2

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

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

This example shows how to upload the configuration file to an FTP server using a string and the filter expression.

```
DGS-3000-28SC:admin# download cfg_fromFTP ftp:
john:123456@10.90.90.15:21/cfg/cfg.txt config_id 2 include “VLAN” “ipif”
exclude “fdb”
Command: download cfg_fromFTP ftp: john:123456@10.90.90.15:21/cfg/cfg.txt
config_id 2 include “VLAN” “ipif” exclude “fdb”

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

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

36-5 upload log_toFTP

Description

This command is used to upload a log file from the Switch to an FTP server.

Format

upload log_toFTP [[<ipaddr> | <ipv6addr>] {tcp_port <tcp_port_number 1-65535>} dest_file <path_filename 64> | ftp: <string 128>]

Parameters

<ipaddr> - Enter the IPv4 address of the FTP server here.
<ipv6addr> - Enter the IPv6 address of the FTP server here.
tcp_port - (Optional) Specify the TCP port number used for the FTP connection. **<tcp_port_number 1-65535>** - Enter the TCP port number here. This value must be between 1 and 65535.
dest_file - Specify the destination file name and path. **<path_filename 64>** - Enter the destination file name and path here. This can be up to 64 characters long.
ftp - Specifiy the FTP connection details. **<string 128>** - Enter the FTP connection details here. For example, john:123456@172.18.211.41:21/image/cfg.txt.

Restrictions

Only Administrators and Operators can issue this command.

Examples

This example shows how to upload the log file to an FTP server.

```
DGS-3000-28SC:admin# upload log_toFTP 10.90.90.15 d:/log.txt
Command: upload log_toFTP 10.90.90.15 d:/log.txt

Connecting to server.................. Done.
User(Anonymous): john
Pass:******
Upload log............................ Done.

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

This example shows how to upload the log file to an FTP server using a string.

```
DGS-3000-28SC:admin# upload log_toFTP ftp:
john:123456@10.90.90.15:21/log/log.txt
Command: upload log_toFTP ftp: john:123456@10.90.90.15:21/log/log.txt

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

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

36-6 upload attack_log_toFTP

Description

This command is used to upload the attack log from the Switch to an FTP server.

Format

upload attack_log_toFTP [[<ipaddr> | <ipv6addr>] {tcp_port <tcp_port_number 1-65535>} dest_file <path_filename 64> | ftp: <string 128>] {unit <unit_id>}

Parameters

<ipaddr> - Enter the IPv4 address of the FTP server here.
<ipv6addr> - Enter the IPv6 address of the FTP server here.
tcp_port - (Optional) Specify the TCP port number used for the FTP connection. **<tcp_port_number 1-65535>** - Enter the TCP port number here. This value must be between 1 and 65535.
dest_file - Specify the destination file name and path. **<path_filename 64>** - Enter the destination file name and path here. This can be up to 64 characters long.
ftp - Specify the FTP connection details. **<string 128>** - Enter the FTP connection details here. For example, john:123456@172.18.211.41:21/image/cfg.txt.
unit - (Optional) Specify which unit on the stacking system. If it is not specified, it refers to the master unit. **<unit_id>** - Enter the unit ID value. This value must be between 1 and 6.

Restrictions

Only Administrators and Operators can issue this command.

Examples

This example shows how to upload the attack log to an FTP server.

```
DGS-3000-28SC:admin# upload attack_log_toFTP 10.90.90.15 log.txt
Command: upload attack_log_toFTP 10.90.90.15 log.txt

Connecting to server.................. Done.
User(Anonymous): john
Pass:******
Upload Log............................ Done.

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

This example shows how to upload the attack log to an FTP server using a string.

```
DGS-3000-28SC:admin# upload attack_log_toFTP ftp:
john:123456@10.90.90.15:21/log.txt
Command: upload attack_log_toFTP ftp: john:123456@10.90.90.15:21/log.txt

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

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

Chapter 37 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>}

37-1 config gratuitous_arp send ipif_status_up

Description

This 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 - Specify to enable the sending of gratuitous ARP packets when the IP interface's status is up. This is the default value.
disable - Specify to disable 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-3000-28SC:admin#config gratuitous_arp send ipif_status_up enable
Command: config gratuitous_arp send ipif_status_up enable

Success.

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

37-2 config gratuitous_arp send dup_ip_detected

Description

This 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 - Specify to enable the sending of gratuitous ARP request packet when duplicate IP is detected. This is the default value.
disable - Specify to disable 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-3000-28SC:admin#config gratuitous_arp send dup_ip_detected enable
Command: config gratuitous_arp send dup_ip_detected enable

Success.

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

37-3 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. This 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 - Specify to enable the learning of ARP entry based on the received gratuitous ARP packet. This is the default value.
disable - Specify to disable 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-3000-28SC:admin#config gratuitous_arp learning enable
Command: config gratuitous_arp learning enable

Success.

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

37-4 config gratuitous_arp send periodically

Description

This 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_name 12> - Enter the IP interface name here. This name can be up to 12 characters long.
interval - Specify 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-3000-28SC:admin#config gratuitous_arp send periodically ipif System
interval 5
Command: config gratuitous_arp send periodically ipif System interval 5

Success.

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

37-5 enable gratuitous_arp

Description

This 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) Specify 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 - Specify to enable the trap function.
log - Specify 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-3000-28SC:admin#enable gratuitous_arp ipif System trap log
Command: enable gratuitous_arp ipif System trap log

Success.

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

37-6 disable gratuitous_arp

Description

This 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) Specify 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 - Specify to disable the trap function.
log - Specify 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-3000-28SC:admin#disable gratuitous_arp ipif System trap log
Command: disable gratuitous_arp ipif System trap log

Success.

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

37-7 show gratuitous_arp

Description

This command is used to display gratuitous ARP configuration.

Format

show gratuitous_arp {ipif <ipif_name 12>}

Parameters

ipif - (Optional) Specify 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-3000-28SC: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-3000-28SC:admin#
```

Chapter 38 Internet Group Management Protocol (IGMP) Command List

config igmp access_authentication ports [all | <portlist>] state [enable | disable]
show igmp access_authentication ports [all | <portlist>]

38-1 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 - Specify all ports to be configured.
<portlist> - Enter a range of ports to be configured.
state - Specify the state of the RADIUS authentication function on the specified ports. **enable** - Enable the RADIUS authentication function on the specified ports. **disable** - Disable the RADIUS authentication function on the specified ports.

Restrictions

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

Example

To enable IGMP Access Control for all ports:

```
DGS-3000-28SC:admin# config igmp access_authentication ports all state enable
Command: config igmp access_authentication ports all state enable

Success.

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

38-2 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 - Specify all ports to be displayed.
<portlist> - Enter a range of ports to be displayed.

Restrictions

None.

Example

To display the IGMP Access Control status for ports 1-4:

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

To display the IGMP Access Control status for all ports:

```
DGS-3000-28SC: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
```

Chapter 39 IGMP Proxy Command List

enable igmp_proxy
disable igmp_proxy
config igmp_proxy downstream_if [add | delete] vlan [<vlan_name 32> | vlanid <vidlist>]
config igmp_proxy upstream_if {vlan [<vlan_name 32> | vlanid <vlanid1-4094>] | router_ports [add | delete] <portlist> | source_ip <ipaddr> | unsolicited_report_interval <sec 0-25>}(1)
show igmp_proxy {group}

39-1 enable igmp_proxy

Description

This command is used to enable the IGMP proxy on the switch.

Format

enable igmp_proxy

Parameters

None.

Restrictions

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

Example

To enable the IGMP proxy:

```
DGS-3000-28SC:admin#enable igmp_proxy
Command: enable igmp_proxy

Success.

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

39-2 disable igmp_proxy

Description

This command is used to disable the IGMP proxy on the switch.

Format

disable igmp_proxy

Parameters

None.

Restrictions

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

Example

To disable the IGMP proxy:

```
DGS-3000-28SC:admin#disable igmp_proxy
Command: disable igmp_proxy

Success.

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

39-3 config igmp_proxy downstream_if

Description

This command is used to configure the IGMP proxy downstream interfaces. The IGMP proxy plays the server role on the downstream interfaces. The downstream interface must be an IGMP-snooping enabled VLAN.

Format

config igmp_proxy downstream_if [add | delete] vlan [<vlan_name 32> | vlanid <vidlist>]

Parameters

add - Specify to add a downstream interface.
delete - Specify to delete a downstream interface .
vlan – Specify the VLAN by name or ID. **<vlan_name 32>** - Specify a name of VLAN which will be added to or deleted from the IGMP proxy downstream interface. The maximum length is 32 characters. **vlanid** - Specify a list of VLAN IDs to be added to or deleted from the IGMP proxy downstream interface. **<vidlist>** - Specify a list of VLAN IDs which will be added to or deleted from the IGMP proxy downstream interface.

Restrictions

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

Example

To configure the IGMP proxy's downstream interface:

```
DGS-3000-28SC:admin# config igmp_proxy downstream_if add vlan vlanid 2-7
Command: config igmp_proxy downstream_if add vlan vlanid 2-7

Success.

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

39-4 config igmp_proxy upstream_if

Description

This command is used to configure the setting for the IGMP proxy's upstream interface. The IGMP proxy plays the host role on the upstream interface. It will send IGMP report packets to the router port.

The source IP address determines the source IP address to be encoded in the IGMP protocol packet.

If the router port is empty, the upstream will send the IGMP protocol packet to all member ports on the upstream interface.

Format

config igmp_proxy upstream_if {vlan [<vlan_name 32> | vlanid <vlanid 1-4094>] | router_ports [add | delete] <portlist> | source_ip <ipaddr> | unsolicited_report_interval <sec 0-25>}(1)

Parameters

vlan - Specify the VLAN for the upstream interface. **<vlan_name 32>** - Specify a VLAN name between 1 and 32 characters. **vlanid** - Specify the VLAN ID for the upstream interface. **<1-4094>** - Specify the VLAN ID between 1 and 4094.
router_ports - Specify a list of ports that are connected to multicast-enabled routers. **add** - Specify to add the router ports. **delete** - Specify to delete the router ports. **<portlist>** - Specify a range of ports to be configured.
source_ip - Specify the source IP address of the upstream protocol packet. If it is not specified, zero IP address will be used as the protocol source IP address. **<ipaddr>** - Specify the IP address.
unsolicited_report_interval - Specify the time between repetitions of the host's initial report of membership in a group. The default is 10 seconds. If set to 0, only one report packet is sent. **<sec 0-25>** - Specify the time between 0 and 25 seconds.

Restrictions

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

Example

To configure the router port of IGMP proxy's upstream interface:

```
DGS-3000-28SC:admin#config igmp_proxy upstream_if vlan default router_ports add
1:3
Command: config igmp_proxy upstream_if vlan default router_ports add 1:3

Success.

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

39-5 show igmp_proxy

Description

This command is used to display the IGMP proxy's configuration or group information on the switch.

Format

show igmp_proxy {group}

Parameters

group - Specify to display the group information. If a group is not specified, the IGMP proxy configuration will be displayed.

Restrictions

None.

Example

To show IGMP proxy information:

```
DGS-3000-28SC:admin# show igmp_proxy
Command: show igmp_proxy

IGMP Proxy Global State                : Disabled

Upstream Interface
 VLAN ID                               : 1
 Dynamic Router Ports                  :
 Static Router Ports                   :
 Unsolicited Report Interval           : 10
 Source IP Address                     : 0.0.0.0

Downstream Interface
 VLAN List                             :

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

Chapter 40 IGMP Snooping Command List

The Internet Group Management Protocol (IGMP) is a L3 protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. IGMP snooping is the process of listening to IGMP network traffic. IGMP snooping, as implied by the name, is a feature that allows a layer 2 switch to "listen in" on the IGMP conversation between hosts and routers by processing the layer 3 IGMP packets sent in a multicast network.

When IGMP snooping is enabled in a switch it analyzes all IGMP packets between hosts connected to the Switch and multicast routers in the network. When a switch hears an IGMP report from a host for a given multicast group, the Switch adds the host's port number to the multicast list for that group. And, when the Switch hears an IGMP Leave, it removes the host's port from the table entry.

config igmp_snooping [vlan_name <vlan_name 32> | vlanid <vlanid_list> | all] {state [enable | disable] | topology_changes_notification [ignore | process] | fast_leave [enable | disable] | report_suppression [enable | disable] | suppression_time <sec 0-300> | 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 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_name32 <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 1-960>
config igmp_snooping forward_lookup_mode [ip | mac]
clear igmp_snooping data_driven_group [all | [vlan_name <vlan_name32> | 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 igmp_snooping forward_lookup_mode
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>]
clear igmp_snooping statistics counter

40-1 config igmp_snooping

Description

This command is used to configure IGMP snooping on the Switch.

Format

config igmp_snooping [vlan_name <vlan_name 32> | vlanid <vlanid_list> | all] {state [enable | disable] | topology_changes_notification [ignore | process] | fast_leave [enable | disable] | report_suppression [enable | disable] | suppression_time <sec 0-300> | proxy_reporting {state [enable | disable] | source_ip <ipaddr>}(1)}(1)

Parameters

vlan_name - Specify 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 - Specify the VLAN ID for which IGMP snooping is to be configured. **<vlanid_list>** - Enter the VLAN ID here.
all - Specify to configure all configured VLAN's.
state - (Optional) Enable or disable IGMP snooping for the chosen VLAN. **enable** - Enter enable to enable IGMP snooping for the chosen VLAN. **disable** - Enter disable to disable IGMP snooping for the chosen VLAN.
topology_changes_notification - Specify that IGMP snooping should be aware of link-layer topology changes caused by Spanning Tree operation or not. **ignore** - Specify that IGMP snooping will ignore link-layer topology changes caused by Spanning Tree operation. General queries won't be sent on the same domain of link-layer topology changes. **process** - Specify that IGMP snooping will process link-layer topology changes caused by Spanning Tree operation. General queries will be sent on the same domain of link-layer topology changes.
fast_leave - Enable or disable the IGMP snooping fast leave function. **enable** - Enter enable to enable the IGMP snooping fast leave function. If enabled, the membership is immediately removed when the system receives the IGMP leave message. **disable** - Enter disable to disable the IGMP snooping fast leave function.
report_suppression - Specify the switch which uses IGMP report suppression to forward only one IGMP report per multicast router query to multicast devices. **enable** - Enable report suppression. **disable** - Disable report suppression.
suppression_time - Specify the interval of suppressiong duplicates reports. If this time is set to zero, report suppression function can't take effect. **<sec 0-300>** - Enter a suppression time between 0 to 300.
proxy reporting - Specify IGMP proxy reporting. If enabled, multiple IGMP reports will be integrated into one report only before sending to the router port. **state** - Enable or disable the proxy reporting. **enable** - Enable the proxy reporting. **disable** - Disable the proxy reporting. **source_ip** - Specify 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-3000-28SC:admin#config igmp_snooping vlan_name default state enable
Command: config igmp_snooping vlan_name default state enable

Success.

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

40-2 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 - Specify a range of ports to be configured. **<portlist>** - Enter the range of ports to be configured here.
vlanid - Specify 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 - Specify 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-3000-28SC:admin#config igmp_snooping rate_limit ports 1 100
Command: config igmp_snooping rate_limit ports 1 100

Success.

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

40-3 config igmp_snooping querier

Description

This command is used to configure the time in seconds between general query transmissions, the maximum time in seconds to wait for reports from members, and the permitted packet loss that guarantees IGMP snooping.

Format

config igmp_snooping querier [vlan_name <vlan_name 32> | vlanid <vlanid_list> | all] {query_interval <sec 1-65535> | max_response_time <sec 1-25> | robustness_variable <value 1-7> | last_member_query_interval <sec 1-25> | state [enable | disable] | version <value 1-3>}(1)

Parameters

vlan_name - Specify 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 - Specify the VLAN ID for which IGMP snooping querier is to be configured.
<vlanid_list> - Enter the VLAN ID list here.

all - Specify all VLANs for which IGMP snooping querier is to be configured.

query_interval - Specify 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 between between 1 and 65535 seconds.

max_reponse_time - Specify 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 - 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 - Specify the maximum amount of time between group-specific query messages, including those sent in response to leave-group messages. You might lower

this interval to reduce the amount of time it takes a router to detect the loss of the last member of a group. On receiving a leave message, the router will assume there are no local members on the interface if there are no reports received after the response time (which is last member query interval * robustness variable) **<sec 1-25>** - Enter the last member query interval value here. This value must be between 1 and 25 seconds.
state - If the state is enabled, it allows the Switch to be selected as an IGMP Querier (sends IGMP query packets). It the state is disabled, then the Switch cannot play the role as a querier. Note that if the Layer 3 router connected to the Switch 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** - Specify to enable this state. **disable** - Specify to disable this state.
version - Specify the version of IGMP packet that will be sent by this device. **<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-3000-28SC: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-3000-28SC:admin#
```

40-4 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> - Enter the name of the VLAN on which the router port resides.
vlanid - Specify the ID of the VLAN on which the router port resides. **<vlanid_list>** - Enter the VLAN ID here.
add - Specify to add the router ports.
delete - Specify to delete the router ports.
<portlist> - Enter a range of ports to be configured.

Restrictions

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

Example

To set up static router ports:

```
DGS-3000-28SC:admin#config router_ports default add 1-10
Command: config router_ports default add 1-10

Success.

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

40-5 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> - Enter the name of the VLAN on which the router port resides.
vlanid - Specify the ID of the VLAN on which the router port resides. **<vlanid_list>** - Enter the VLAN ID list here.
add - Specify to add the forbidden router ports.
delete - Specify to delete the forbidden router ports.
<portlist> - Enter a range of ports to be configured.

Restrictions

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

Example

To set up port range 1-10 to forbidden router ports of default VLAN:

```
DGS-3000-28SC:admin#config router_ports_forbidden default add 11-12
Command: config router_ports_forbidden default add 11-12

Success.

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

40-6 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-3000-28SC:admin#enable igmp_snooping
Command: enable igmp_snooping

Success.

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

40-7 disable igmp_snooping

Description

This command is used to disable IGMP snooping on the Switch.

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-3000-28SC:admin#disable igmp_snooping
Command: disable igmp_snooping

Success.

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

40-8 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 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 - Specify 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 - Specify the ID of the VLAN on which the static group resides. **<vlanid_list>** - Enter the VLAN ID here.
<ipaddr> - Enter the multicast group IP address.

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-3000-28SC: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-3000-28SC:admin#
```

40-9 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 - Specify 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 - Specify the ID of the VLAN on which the static group resides. **<vlanid_list>** - Enter the VLAN ID list here.
<ipaddr> - Enter the multicast group IP address.

Restrictions

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

Example

To delete an IGMP snooping static group for VLAN 1, group 239.1.1.1:

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

40-10 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 - Specify 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 - Specify the ID of the VLAN on which the static group resides. **<vlanid_list>** - Enter the VLAN ID here.
<ipaddr> - Enter the multicast group IP address (for Layer 3 switch).
add - Specify to add the member ports.
delete - Specify to delete the member ports.
<portlist> - Enter 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-3000-28SC: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-3000-28SC:admin#
```

40-11 show igmp_snooping static_group

Description

This command is used to display the IGMP snooping multicast group static members.

Format

show igmp_snooping static_group {[vlan <vlan_name 32> | vlanid <vlanid_list>] <ipaddr>}

Parameters

vlan - (Optional) Specify 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) Specify the ID of the VLAN on which the static group resides. **<vlanid_list>** - Enter the VLAN ID here.

<ipaddr> - (Optional) Enter the multicast group IP address.

Restrictions

None.

Example

To display all the IGMP snooping static groups:

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

40-12 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_name32 <vlan_name> | vlanid <vlanid_list>] {state [enable | disable] | aged_out [enable | disable] | expiry_time <sec 1-65535>}(1)

Parameters

all - Specify all VLANs to be configured.
vlan_name - Specify the VLAN name to be configured. **<vlan_name32>** - Enter the VLAN name here.
vlanid - Specify the VLAN ID to be configured. **<vlanid_list>** - Enter the VLAN ID here.

state - Specify to enable or disable the data driven learning of an IGMP snooping group. **enable** - Specify to enable the data driven learning option. By default, the state is enabled. **disable** - Specify to disable the data driven learning option.
aged_out - Specify to enable or disable the aging out of the entry. **enable** - Specify to enable the aging out of the entry. **disable** - Specify to disable the aging out of the entry. By default, the state is disabled state.
expiry_time - Specify the data driven group lifetime in seconds. This parameter is valid only when aged_out is enabled. **<sec 1-65535>** - Enter the expiry time here. This value must be between 1 and 65535 seconds.

Restrictions

Only 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-3000-28SC: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-3000-28SC:admin#
```

40-13 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 1-960>

Parameters

<value 1-960> - Enter number of groups that can be learned by data driven. This value must be between 1 and 960. The default setting is 128.

Restrictions

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

Example

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

```
DGS-3000-28SC:admin#config igmp_snooping data_driven_learning max_learned_entry
50
Command: config igmp_snooping data_driven_learning max_learned_entry 50

Success.

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

40-14 config igmp_snooping forward_lookup_mode

Description

This command is used to configure IGMP snooping forward lookup mode. If this mode is configured to ip, the multicast forwarding is based on IP address; if this mode is configured to mac, the multicast forwarding is based on MAC address.

Format

config igmp_snooping forward_lookup_mode [ip | mac]

Parameters

ip - Specify the multicast forwarding lookup to be based on IP address.
mac - Specify the multicast forwarding lookup to be based on MAC address.

Restrictions

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

Example

To configure the IGMP snooping forward lookup mode to be MAC-based:

```
DGS-3000-28SC:admin# config igmp_snooping forward_lookup_mode mac
Command: config igmp_snooping forward_lookup_mode mac

Success.

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

40-15 clear igmp_snooping data_driven_group

Description

This command is used to delete the IGMP snooping group(s) learned by data driven.

Format

clear igmp_snooping data_driven_group [all | [vlan_name <vlan_name32> | vlanid <vlanid_list>] [<ipaddr> | all]]

Parameters

all - Specify all VLANs to which IGMP snooping groups will be deleted.
vlan_name - Specify the VLAN name. **<vlan_name32>** - Enter the VLAN name here.
vlanid - Specify the VLAN ID. **<vlanid_list>** - Enter the VLAN ID here.
<ipaddr> - Enter 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-3000-28SC:admin#clear igmp_snooping data_driven_group all
Command: clear igmp_snooping data_driven_group all

Success.

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

40-16 show igmp_snooping

Description

This command is used to display the current IGMP snooping configuration on the Switch.

Format

show igmp_snooping {[vlan <vlan_name 32> | vlanid <vlanid_list>]}

Parameters

vlan - (Optional) Specify 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) Specify 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-3000-28SC:admin#show igmp_snooping
Command: show igmp_snooping

 IGMP Snooping Global State              : Disabled
 Data Driven Learning Max Entries        : 120

 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
 Topology Changes Notification  : Process
 Fast Leave                     : Disabled
 Rate Limit(pkt/sec)            : No Limitation
 Report Suppression             : Enabled
 Suppression Time               : 10
 Proxy Reporting                : Disabled
 Proxy Reporting Source IP      : 0.0.0.0
 Version                        : 3
 Data Driven Learning State     : Enabled
 Data Driven Learning Aged Out  : Disabled
 Data Driven Group Expiry Time  : 260

Total Entries: 1


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

40-17 show igmp_snooping rate_limit

Description

This command is used to display the IGMP snooping rate limit setting.

Format

show igmp_snooping rate_limit [ports <portlist> | vlanid <vlanid_list>]

Parameters

ports - Specify the port range. **<portlist>** - Enter the range of ports here.
vlanid - Specify 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-3000-28SC:admin#show igmp_snooping rate_limit ports 1-15
Command: show igmp_snooping rate_limit ports 1-15

 Port      Rate Limit(pkt/sec)
 --------  --------------------
 1         No Limit
 2         No Limit
 3         No Limit
 4         No Limit
 5         No Limit
 6         No Limit
 7         No Limit
 8         No Limit
 9         No Limit
 10        No Limit
 11        No Limit
 12        No Limit
 13        No Limit
 14        No Limit
 15        No Limit

Total Entries: 15

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

40-18 show igmp_snooping group

Description

This command is used to display the current IGMP snooping group configuration on the Switch.

Format

show igmp_snooping group {[vlan <vlan_name 32> | vlanid <vlanid_list> | ports <portlist>] {<ipaddr>}} {data_driven}

Parameters

vlan - (Optional) Specify 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) Specify 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) Specify a list of ports for which you want to view IGMP snooping group information. **<portlist>** - Enter the list of ports here.
<ipaddr> - (Optional) Enter 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-3000-28SC: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-3000-28SC:admin#
```

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

40-19 show igmp_snooping forwarding

Description

This command is used to display the Switch's current IGMP snooping forwarding table. It provides an easy way for users to check the list of ports that the multicast group that comes from a specific sources will be forwarded to. 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) Specify 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) Specify 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-3000-28SC: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-3000-28SC:admin#
```

40-20 show igmp_snooping forward_loopup_mode

Description

This command is used to show IGMP snooping forward lookup mode on the switch.

Format

show igmp_snooping forward_lookup_mode

Parameters

None.

Restrictions

None.

Example

To show IGMP snooping forward lookup mode:

```
DGS-3000-28SC:admin# show igmp_snooping forward_lookup_mode
Command: show igmp_snooping forward_lookup_mode

IGMP snooping forward lookup mode: MAC address

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

40-21 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 - Specify 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 - Specify the ID of the VLAN on which the router port resides. **<vlanid_list>** - Enter the VLAN ID list here.
all - Specify 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-3000-28SC: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-3000-28SC:admin#
```

40-22 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 - Specify a VLAN to be displayed. **<vlan_name>** - Enter the VLAN name here.
vlanid - Specify a list of VLANs to be displayed. **<vlanid_list>** - Enter the VLAN ID list here.
ports - Specify 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-3000-28SC: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-3000-28SC:admin#
```

To display the IGMP snooping statistics counter for a port:

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

40-23 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-3000-28SC:admin#clear igmp_snooping statistic counter
Command: clear igmp_snooping statistic counter

Success.

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

Chapter 41 IP Interface Command List

create ipif <ipif_name 12> {<network_address>} <vlan_name 32> {secondary | state [enable | disable] | proxy_arp [enable | disable] {local [enable | disable]}}
config ipif <ipif_name 12> [{ipaddress <network_address> | vlan <vlan_name 32> | state [enable | disable]} | proxy_arp [enable | disable] {local [enable | disable]} | bootp | dhcp | ipv6 [ipv6address {prefix_name <string 1-12>} <ipv6networkaddr> | state [enable | disable]] | ip_mtu <value 512-16383> | ipv4 state [enable | disable] | dhcpv6_client [enable | disable] {rapid_commit} | dhcp_option 12 [hostname <hostname 63> | clear_hostname | state [enable | disable]] | dhcpv6_client_pd [enable prefix_name <string 1-12> | disable] {rapid_commit}]
delete ipif [<ipif_name12> {ipv6address {prefix_name <string1-12>} <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>}

41-1 create ipif

Description

This command is used to create an IP interface.

Format

create ipif <ipif_name 12> {<network_address>} <vlan_name 32> {secondary | state [enable | disable] | proxy_arp [enable | disable] {local [enable | disable]}}

Parameters

<ipif_name 12> - Enter the IP interface name here. This name can be up to 12 characters long.
<network_address> - (Optional) Specify the IPv4 networkaddress (xxx.xxx.xxx/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.
secondary - (Optional) Specify the IPv4 secondary interface to be created.
state - (Optional) Specify the state of the IP interface. **enable** - Specify that the IP interface state will be enabled. **disable** - Specify that the IP interface state will be disabled.
proxy_arp - (Optional) Enable or disable of proxy ARP function. It is for IPv4 function. Default: Disabled. **enable** - Specify that the proxy ARP option will be enabled. **disable** - Specify that the proxy ARP option will be disabled. **local** - (Optional) This setting controls whether the system provides the proxy reply for the ARP packets destined for IP address located in the same interface as the received interface. When proxy ARP is enabled for an interface, the system will do the proxy reply for the ARP packets destined for IP address located in a different interface. For ARP packets destined for IP address located in the same interface, the system will check this setting to determine whether to reply. **enable** - Specify that the local option will be enabled. **disable** - Specify that the local option will be disabled.

Restrictions

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

Example

To create an IP interface:

```
DGS-3000-28SC:admin# create ipif Inter2 192.168.16.1/24 default state enable
secondary
Command: create ipif Inter2 192.168.16.1/24 default state enable secondary

Success.

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

41-2 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]} | proxy_arp [enable | disable] {local [enable | disable]} | bootp | dhcp | ipv6 [ipv6address {prefix_name <string 1-12>} <ipv6networkaddr> | state [enable | disable]] | ip_mtu <value 512-16383> | ipv4 state [enable | disable] | dhcpv6_client [enable | disable] {rapid_commit} | dhcp_option 12 [hostname <hostname 63> | clear_hostname | state [enable | disable]] | dhcpv6_client_pd [enable prefix_name <string 1-12> | disable] {rapid_commit}]

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) Specify 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) Specify the state of the interface. **enable** - Enables the state of the interface. **disable** - Disables the state of the interface.
proxy_arp – Specify the proxy_arp function. This is for IPv4. The default is disabled. **enable** - Specify that the proxy_arp is enabled. **disable** - Specify that the proxy arp is disabled. **local** - Specify the setting controls whether the system provides the proxy reply for the ARP packets destined for an IP address located in the same interface as the received interface. **enable** - Specify to enable the proxy ARP for an interface, the system will do the proxy reply for the ARP packets destined for an IP address located in a different interface. ARP packets destined for an IP address located in the same interface, the system will check this setting to determine whether to reply. **disable** - Specify to use the default disabled setting.

bootp - Uses BOOTP to obtain the IPv4 address.
dhcp - Uses DHCP to obtain the IPv4 address.
ipv6 - Specify that the IPv6 configuration will be done. **ipv6address** - Specify 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. **prefix_name** - Specify the prefix name to be used. **<string 1-12>** - Enter a prefix name with a string of 1 to 12 characters. **<ipv6networkaddr>** - Enter the IPv6 address used here. **state** - Specify that the IPv6 interface state will be set to enabled or disabled. **enable** - Specify that the IPv6 interface sate will be enabled. **disable** - Specify that the IPv6 interface sate will be disabled.
ip_mtu - Specify the ip mtu command. This forces it to drop any packets that exceed the ip mtu. **<value 512-16383>** - Enter a value between 512 to 16383.
ipv4 - Specify that the IPv4 configuration will be done. **state** - Specify that the IPv4 interface state will be set to enabled or disabled. **enable** - Specify that the IPv4 interface sate will be enabled. **disable** - Specify that the IPv4 interface sate will be disabled.
dhcpv6_client - Specify the DHCPv6 client state of the interface. **enable** - Enable the DHCPv6 client state of the interface. **disable** - Disable the DHCPv6 client state of the interface. **rapid_commit** - Specify to rapid commit DHCPv6.
dhcp_option12 - Specify the DHCP option 12. **hostname** - Specify 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.
dhcpv6_client_pd – Specify the DHCPv6 client PD state. **enable prefix_name** - Enable the DHCPv6 client PD state of the interface. Specify an alias name for the prefix requested from the delegation router. If disable the DHCPv6 client PD the name will be automatic clear. **<string 1-12>** - Enter an DHCPv6 client pd interface name used here. This name can be up to 12 characters long. **disable** - Disable the DHCPv6 client PD state of the interface. **rapid_commit** - Specify to commit the DHCPv6 client PD.

Restrictions

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

Example

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

```
DGS-3000-28SC:admin#config ipif System dhcpv6_client enable
Command: config ipif System dhcpv6_client enable

Success.

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

To enable the System interface DHCPv6 client PD state:

```
DGS-3000-28SC:admin#config ipif System dhcpv6_client_pd enable prefix alpha
Command: config ipif System dhcpv6_client_pd enable prefix alpha

Success.

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

To configure the IP2 interface for IPv6 address:

```
DGS-3000-28SC:admin#config ipif ip2 ipv6 ipv6address prefix_name alpha
2:2::2::1/64
Command: config ipif ip2 ipv6 ipv6address prefix_name alpha 2:2::2::1/64

Success.

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

To display :

```
DGS-3000-28SC:admin# show ipif
Command: show ipif

IP Interface                  : ip2
VLAN Name                      : vlan2
Interface Admin State       : Enabled
Link Status                    : LinkDown
IPv4 Address                   : 0.0.0.0/0 (Manual)  Primary
Proxy ARP                      : Disabled   (Local : Disabled)
IPv4 State                     : Enabled
DHCPv6 Client State          : Disabled
DHCPv6 Client PD State       : Disabled
IPv6 Link-Local Address      : FE80::200:1FF:FE02:301/128
IPv6 Global Unicast Address : alpha 2:2:2::1/64 (DHCPv6 PD)
                                    2001:0:2::1/64
IPv6 Global Unicast Address : dlink 3:3:3:3::1/64 (DHCPv6 PD)
IPv6 State                     : Enabled
IP MTU                         : 1500
DHCP Option12 State         : Disabled
DHCP Option12 Host Name     :
IP Interface                  : System
VLAN Name                      : default
Interface Admin State        : Enabled
Link Status                    : LinkUp
IPv4 Address                   : 20.0.0.20/8 (Manual)  Primary
Proxy ARP                      : Disabled   (Local : Disabled)
IPv4 State                     : Enabled
DHCPv6 Client State          : Disabled
DHCPv6 Client PD State       : Enabled
DHCPv6 Client PD Prefix Name: alpha
DHCPv6 Client PD Prefix      : 2001::/32
IPv6 Link-Local Address      : FE80::200:1FF:FE02:300/128
IPv6 State                     : Enabled
IP MTU                         : 1500

Success.

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

41-3 delete ipif

Description

This command is used to delete an IP interface.

Format

delete ipif [<ipif_name12> {ipv6address {prefix_name <string1-12>} <ipv6networkaddr>} | all]

Parameters

<ipif_name 12> - Enter the IP interface name used here. This name can be up to 12 characters long. **ipv6address** - (Optional) Specify 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. **prefix_name** - (Optional) Specify the IPv6 prefix name. **<string1-12>** - Enter the string here using characters between 1 to 12. **<ipv6networkaddr>** - Enter the IPv6 address used here.
all - Specify 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-3000-28SC:admin#delete ipif newone
Command: delete ipif newone

Success.

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

41-4 enable ipif

Description

This command is used to enable the IP interface.

Format

enable ipif [<ipif_name 12> | all]

Parameters

<ipif_name 12> - Enter the IP interface name used here. This name can be up to 12 characters long.
all - Specify 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-3000-28SC:admin#enable ipif newone
Command: enable ipif newone

Success.

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

41-5 disable ipif

Description

This command is used to disable an IP interface.

Format

disable ipif [<ipif_name 12> | all]

Parameters

<ipif_name 12> - Enter the IP interface name used here. This name can be up to 12 characters long.
all - Specify 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-3000-28SC:admin#disable ipif newone
Command: disable ipif newone

Success.

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

41-6 show ipif

Description

This command is used to display an IP interface.

Format

show ipif {<ipif_name 12>}

Parameters

<ipif_name 12> - (Optional) Enter the IP interface name used here. This name can be up to 12 characters long.

Restrictions

None.

Example

To display an IP interface:

```
DGS-3000-28SC:admin#show ipif
Command: show ipif

IP Interface                : System
VLAN Name                   : default
Interface Admin State       : Enabled
Link Status                 : LinkDown
IPv4 Address                : 172.18.62.23/8 (Manual)  Primary
Proxy ARP                   : Disabled   (Local : Disabled)
IPv4 State                  : Enabled
DHCPv6 Client State         : Disabled   (Rapid commit : Disabled)
DHCPv6 Client PD State      : Disabled   (Rapid commit : Disabled)
IPv6 Link-Local Address     : FE80::211:22FF:FE33:4455/128
IPv6 Global Unicast Address : 3000::7/64 (Manual)
IPv6 State                  : Enabled
IP MTU                      : 1500
DHCP Option12 State         : Disabled
DHCP Option12 Host Name     :

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

41-7 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 - Specify 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-3000-28SC:admin#enable ipif_ipv6_link_local_auto newone
Command: enable ipif_ipv6_link_local_auto newone

Success.

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

41-8 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 - Specify 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-3000-28SC:admin#disable ipif_ipv6_link_local_auto newone
Command: disable ipif_ipv6_link_local_auto newone

Success.

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

41-9 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

T o display the link local address automatic configuration state.

```
DGS-3000-28SC:admin#show ipif_ipv6_link_local_auto
Command: show ipif_ipv6_link_local_auto

 IPIF: System          Automatic Link Local Address: Disabled

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

41-10 show ipif_ipv6_link_local_auto

Description

This commands is used to configure the IP directed-broadcast state of the interface. An IP directed broadcast is an IP packet whose destination address is a valid broadcast address of some IP subnet, but which originates from a node that is not a part of that destination subnet. The Switch that is not directly connected to its destination subnet and forwards an IP directed broadcast in the same way that it would forward unicast IP packets to a host on that subnet. When a directed broadcast packet reaches a router that is directly connected to its destination subnet, and that packet is "exploded" as a broadcast on the destination subnet. It only works on layer 3 Switch

Format

config ipif <ipif_name 12> ip_directed_broadcast [enable | disable]

Parameters

<ipif_name 12> - (Optional) Enter the Ip interface name used here. This name can be up to 12 characters long.
ip_directed_broadcast - Specify the IP directed broadcast location. **enable** - Specify to enable the IP directed-broadcast state of the interface. **disable** - Specify to disable the IP directed broadcast state of the interface.

Restrictions

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

Example

To display the link local address automatic configuration state.

```
DGS-3000-28SC:admin# config ipif System ip_directed_broadcast enable
Command: config ipif System ip_directed_broadcast enable

Success.

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

Chapter 42 IP-MAC-Port Binding (IMPB) Command List

create address_binding ip_mac ipaddress <ipaddr> mac_address <macaddr> {ports [<portlist> | all]}
config address_binding ip_mac ports [<portlist> | all] {arp_inspection [strict | loose | disable] | ip_inspection [enable | disable] | nd_inspection [enable | disable] | protocol [ipv4 | ipv6 | all] | allow_zeroip [enable | disable] | forward_dhcppkt [enable | disable] | stop_learning_threshold <int 0-500>}
create address_binding ip_mac ipv6address <ipv6addr> mac_address <macaddr> {ports [<portlist> | all]}
config address_binding ip_mac ipv6address <ipv6addr> mac_address <macaddr> {ports [<portlist> | all]}
delete address_binding blocked [all | vlan_name <vlan_name> mac_address <macaddr>]
delete address_binding ip_mac [all | ipaddress <ipaddr> mac_address <macaddr> | ipv6address <ipv6addr> mac_address <macaddr>]
config address_binding ip_mac ipaddress <ipaddr> mac_address <macaddr> {ports [<portlist> | all]}
config address_binding ip_mac vlan <vlanid 1-4094> ip_inspection state [enable | disable]
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 limit_rate {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>} | all]}
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]
config address_binding dhcp snooping ports [<portlist> | all] limit [rate <value 1-2048> mode [drop | shutdown] | no_limit]
config address_binding dhcp snooping recovery_timer [<sec 60-1000000> | infinite]
enable address_binding roaming
disable address_binding roaming
upload address_binding snoop_entry_toFTP [<ipaddr> {tcp_port <tcp_port_number 1-65535>} filename <path_filename 64> | ftp: <string user:pasword@ipaddr:tcpport/path_filename>]
upload address_binding snoop_entry_toTFTP [<ipaddr> | <ipv6addr> | <domain_name 255>] filename <path_filename 64>

download address_binding snoop_entry_fromFTP [<ipaddr> {tcp_port <tcp_port_number 1-65535>} filename <path_filename 64> | ftp: <string user:password@ipaddr: tcp port /path_filename>]
download address_binding snoop_entry_fromTFTP [<ipaddr> | <ipv6addr> | <domain_name 255>] filename <path_filename 64>

42-1 create address_binding ip_mac ipaddress

Description

This command is used to create an IMPB entry.

Format

create address_binding ip_mac ipaddress <ipaddr> mac_address <macaddr> {ports [<portlist> | all]}

Parameters

<ipaddr> - Enter the IP address used for the IMPB entry.
mac_address - Specify the MAC address used for the IMPB entry. **<macaddr>** - Enter the MAC address used here.
ports - (Optional) Specify 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** - Specify 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-3000-28SC: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-3000-28SC:admin#
```

42-2 config address_binding ip_mac ports

Description

This command is used to configure the state of IMPB on the Switch for each port.

Format

config address_binding ip_mac ports [<portlist> | all] {arp_inspection [strict | loose | disable] | ip_inspection [enable | disable] | nd_inspection [enable | disable] | protocol [ipv4 | ipv6 | all] | allow_zeroip [enable | disable] | forward_dhcppkt [enable | disable] | stop_learning_threshold <int 0-500>}

Parameters

<portlist> - Enter the list of ports used for this configuration here.
all - Specify that all the ports will be used.
arp_inspection - (Optional) Specify 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. This is the default option. **loose** - In this mode, all packets are forwarded by default until an illegal ARP or broadcast IP packets are detected. **disable** - Disable ARP inspection function. The default value is disabled.
ip_inspection - (Optional) Specify that the IP inspection option will be configured. **enable** - Enable IP inspection function. The legal IP packets will be forward, while the illegal IP packets will be dropped. **disable** - Disable IP inspection function. The default value is disabled.
nd_inspection - Specify that the ND inspection option will be configured. **enable** - Specify that the ND inspection option will be enabled. The legal ND packets will be forwarded while the illegal packets will be dropped. **disable** - Specify that the ND inspection option will be disabled. This is the default option.
protocol - (Optional) Specify the version used. **ipv4** - Only IPv4 packets will be checked. **ipv6** - Specify that only IPv6 packets will be checked. **all** - Specify that all packets will be checked.
allow_zeroip - (Optional) Specify whether to allow ARP packets with a source IP address of 0.0.0.0. If the IP address 0.0.0.0 is not configured in the binding list and this setting is enabled, ARP packets with the source IP address of 0.0.0.0 will be allowed; If the IP address 0.0.0.0 is not configured in the binding list and this setting is disabled, ARP packets with the source IP address of 0.0.0.0 will not be allowed. This option does not affect the IMPB ACL Mode. **enable** - Specify that the allow zero IP option will be enabled. **disable** - Specify that the allow zero IP option will be disabled.
forward_dhcppkt - (Optional) By default, DHCP packets with a broadcast DA will be flooded. When set to disabled, the broadcast DHCP packet received by the specified port will not be forwarded. This setting is effective when DHCP Snooping is enabled, in this case DHCP packets trapped by the CPU must be forwarded by the software. This setting controls the forwarding behavior in this situation. **enable** - Specify that the forward DHCP packets option will be enabled. **disable** - Specify that the forward DHCP packets option will be disabled.
stop_learning_threshold - (Optional) When the number of blocked entries exceeds the threshold, the port will stop learning new addresses. Packets with a new address will be dropped. **<int 0-500>** - Enter the stop learning threshold value here. This value must be between 0 and 500.

Restrictions

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

Example

To enable IMPB on port 1:

```
DGS-3000-28SC:admin# config address_binding ip_mac ports 1:1 arp_inspection
strict
Command: config address_binding ip_mac ports 1:1 arp_inspection strict

Success.

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

42-3 create address_binding ip_mac ipv6address

Description

This command is used to create an IP-MAC-Port binding entry using IPv6.

Format

create address_binding ip_mac ipv6address <ipv6addr> mac_address <macaddr> {ports [<portlist> | all]}

Parameters

<ipv6addr> - Enter the IPv6 address.
mac_address - Specify the MAC address. **<macaddr>** - Enter the MAC address here.
ports - (Optional) Specify a range of ports or all ports. **<portlist>** - Enter a range of ports to be configured. **all** - Specify 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-3000-28SC: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-3000-28SC:admin#
```

42-4 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 - Specify the MAC address. **<macaddr>** - Enter the MAC address here.
ports - (Optional) Specify a range of ports to be configured.If the ports are not specified, it will apply to all ports. **<portlist>** - Enter a range of ports to be applied to. **all** - Specify 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-3000-28SC: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-3000-28SC:admin#
```

42-5 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 - Specify that all the entries the address database that the system has automatically blocked to be deleted.
vlan_name - Specify the name of the VLAN to which the blocked MAC address belongs. **<vlan_name>** - Enter the VLAN name. **mac_address** - Specify 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-3000-28SC: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-3000-28SC:admin#
```

42-6 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 - Specify that all the MAC address will be used.
ipaddress - Specify the learned IP address of the entry in the database. **<ipaddr>** - Enter the IP address used. **mac_address** - Specify the MAC address used for this configuration. **<macaddr>** - Enter the MAC address used.
ipv6address - Specify the learned IPv6 address of the entry in the database. **<ipv6addr>** - Enter the IPv6 address used. **mac_address** - Specify 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-3000-28SC: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-3000-28SC:admin#
```

42-7 config address_binding ip_mac ipaddress

Description

This command is used to update an IMPB entry.

Format

config address_binding ip_mac ipaddress <ipaddr> mac_address <macaddr> {ports [<portlist> | all]}

Parameters

<ipaddr> - Enter the IP address used here.
mac_address - Specify the MAC address of the entry being updated **<macaddr>** - Enter the MAC address used here.
ports - (Optional) Specify which ports are used for the IMPB entry being updated. If no port is specified, this is applied to all ports. **<portlist>** - Enter the list of port used here. **all** - Specify 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-3000-28SC: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-3000-28SC:admin#
```

42-8 config address_binding ip_mac vlan

Description

This command is used to set specified VLAN's IP Inspection state.

Format

config address_binding ip_mac vlan <vlanid1-4094> ip_inspection state [enable | disable]

Parameters

<vlanid1-4094> - Specify the VLAN ID to set the IP inspection state.
ip_inspection - Specify to enhance IP inspection in a VLAN domain. **state** - Specify the IP inspection state here. **enable** - Specify the VLAN to enable IP inspection. **disable** - Specify the VLAN to disable IP inspection.

Restrictions

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

Example

To enable IP inspection on VLAN 2000:

```
DGS-3000-28SC:admin# config address_binding ip_mac vlan 2000 ip_inspection
state enable
Command: config address_binding ip_mac vlan 2000 ip_inspection state enable

Success.

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

42-9 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) Specify the ports for which the information is displayed. **<portlist>** - (Optional) Enter the list of ports used here.
If no port is specified, information for all ports will be displayed.

Restrictions

None.

Example

To show the IMPB global configuration:

```
DGS-3000-28SC: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  : 3.98


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

To show the IMPB ports:

```
DGS-3000-28SC:admin#show address_binding ports
Command: show address_binding ports

ARP:ARP Inspection   IP:IP Inspection   ND:ND Inspection   Prot:Protocol

 Port  ARP      IP       ND       Prot Zero IP   DHCP Packet Stop Learning
                                                            Threshold/Mode
 ----- -------- -------- -------- ---- --------- ----------- --------------
 1:1   Disabled Disabled Disabled All  Not Allow Forward     500/Normal
 1:2   Disabled Disabled Disabled All  Not Allow Forward     500/Normal
 1:3   Disabled Disabled Disabled All  Not Allow Forward     500/Normal
 1:4   Disabled Disabled Disabled All  Not Allow Forward     500/Normal
 1:5   Disabled Disabled Disabled All  Not Allow Forward     500/Normal
 1:6   Disabled Disabled Disabled All  Not Allow Forward     500/Normal
 1:7   Disabled Disabled Disabled All  Not Allow Forward     500/Normal
 1:8   Disabled Disabled Disabled All  Not Allow Forward     500/Normal
 1:9   Disabled Disabled Disabled All  Not Allow Forward     500/Normal
 1:10  Disabled Disabled Disabled All  Not Allow Forward     500/Normal
 1:11  Disabled Disabled Disabled All  Not Allow Forward     500/Normal
 1:12  Disabled Disabled Disabled All  Not Allow Forward     500/Normal
 1:13  Disabled Disabled Disabled All  Not Allow Forward     500/Normal
 1:14  Disabled Disabled Disabled All  Not Allow Forward     500/Normal
 1:15  Disabled Disabled Disabled All  Not Allow Forward     500/Normal
 1:16  Disabled Disabled Disabled All  Not Allow Forward     500/Normal
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

42-10 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 - Specify that all the addresses in the database that the system has auto learned and blocked to be displayed.
vlan_name - Specify the name of the VLAN to which the blocked MAC address belongs. **<vlan_name>** - Enter the VLAN name used. **mac_address** - Specify 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-3000-28SC: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-3000-28SC:admin#
```

42-11 show address_binding ip_mac

Description

This command is used to display the IMPB entries.

Format

show address_binding ip_mac [all | [[ipaddress <ipaddr> | ipv6address <ipv6addr>] {mac_address <macaddr>} | mac_address <macaddr>]]

Parameters

all - Specify that all the IP addresses to be displayed.
ipaddress - Specify the learned IP address of the entry in the database. **<ipaddr>** - Enter the learned IP address. **ipv6address** - Specify the learned IPv6 address of the entry in the database. **<ipv6addr>** - Enter the learned IPv6 address. **mac_address** - (Optional) Specify the MAC address of the entry in the database. **<macaddr>** - Enter the MAC address here.

mac_address - Specify the MAC address in the database. **<macaddr>** - Enter the binding IP MAC address.

Restrictions

None.

Example

To show IMPB entries:

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

42-12 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. 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 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) Specify to enable the IPv6 entries.
all - (Optional) Specify 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-3000-28SC:admin#enable address_binding dhcp_snoop
Command: enable address_binding dhcp_snoop

Success.

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

42-13 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) Specify to disable the IPv6 entries.
all - (Optional) Specify 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-3000-28SC:admin#disable address_binding dhcp_snoop
Command: disable address_binding dhcp_snoop

Success.

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

42-14 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 - Specify that all the ports will be used.
ipv6 - (Optional) Specify to clear the IPv6 entries.
all - (Optional) Specify 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-3000-28SC:admin#clear address_binding dhcp_snoop binding_entry ports 1-3
Command: clear address_binding dhcp_snoop binding_entry ports 1-3

Success.
s
DGS-3000-28SC:admin#
```

42-15 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** - (Optional) Specify the ports used for this configuration. **<portlist>** - Enter a list of ports used here.
If no parameter is specified, show DHCP snooping displays the enable/disable state.

Restrictions

None.

Example

To show the DHCP snooping state:

```
DGS-3000-28SC:admin#show address_binding dhcp_snoop
Command: show address_binding dhcp_snoop

DHCP Snoop(IPv4) : Disabled
DHCP Snoop(IPv6) : Disabled

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

To display DHCP snooping maximun entry configuration:

```
DGS-3000-28SC: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
```

42-16 show address_binding dhcp_snoop limit_rate

Description

This command is used to display the DHCP snooping limit rate entries.

Format

show address_binding dhcp_snoop limit_rate {ports <portlist>}

Parameters

port – (Optional) Specify the port used for this configuration. **<port>** - Enter the port number used here.

Restrictions

None.

Example

To display the DHCP snooping limit rate entries:

```
DGS-3000-28SC:admin# show address_binding dhcp_snoop limit_rate
Command: show address_binding dhcp_snoop limit_rate

 Port      Rate Limit (pps)     Action
 ------    ----------------     ---------
 1:1       No Limit             -
 1:2       No Limit             -
 1:3       No Limit             -
 1:4       No Limit             -
 1:5       No Limit             -
 1:6       No Limit             -
 1:7       No Limit             -
 1:8       No Limit             -
 1:9       No Limit             -
 1:10      No Limit             -
 1:11      No Limit             -
 1:12      No Limit             -
 1:13      No Limit             -
 1:14      No Limit             -
 1:15      No Limit             -
 1:16      No Limit             -
 1:17      No Limit             -
 1:18      No Limit             -
 1:19      No Limit             -
 1:20      No Limit             -
 1:21      No Limit             -
 1:22      No Limit             -
 1:23      No Limit             -
 1:24      No Limit             -

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

42-17 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) Specify the port used for this configuration. **<port>** - Enter the port number used here.

Restrictions

None.

Example

To display the DHCP snooping binding entries:

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

42-18 config address_binding dhcp_snoop max_entry ports

Description

This command is used to specify the maximum number of entries that can be learned by a specified port.

Format

config address_binding dhcp_snoop max_entry ports [<portlist> | all] limit [<value 1-50> | no_limit] {ipv6}

Parameters

<portlist> - Enter the list of ports used here.
all - Specify that all the ports will be used.
limit - Specify 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** - Specify that the maximum number of learned entries is unlimited.
ipv6 - (Optional) Specify 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-3000-28SC: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-3000-28SC:admin#
```

42-19 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-3000-28SC:admin#enable address_binding nd_snoop
Command: enable address_binding nd_snoop

Success.

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

42-20 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-3000-28SC:admin#disable address_binding nd_snoop
Command: disable address_binding nd_snoop

Success.

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

42-21 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 - Specify that all the ports will be usd for this configuration.
max_entry - Specify 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** - Specify 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-3000-28SC: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-3000-28SC:admin#
```

42-22 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>} | all]}

Parameters

ports - (Optional) Specify the list of ports used for this display. **<portlist>** - Enter the list of ports used for this display here.
all - (Optional) Specify all address binding ports.

Restrictions

None.

Example

To show the ND snooping state:

```
DGS-3000-28SC:admin#show address_binding nd_snoop
Command: show address_binding nd_snoop

ND Snoop          : Enabled

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

To show the ND snooping maximum entry information for ports 1-5:

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

42-23 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) Specify 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-3000-28SC: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-3000-28SC:admin#
```

42-24 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 - Specify 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-3000-28SC:admin#clear address_binding nd_snoop binding_entry ports 1-3
Command: clear address_binding nd_snoop binding_entry ports 1-3

Success.

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

42-25 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-3000-28SC:admin#enable address_binding trap_log
Command: enable address_binding trap_log

Success.

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

42-26 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-3000-28SC:admin#disable address_binding trap_log
Command: disable address_binding trap_log

Success.

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

42-27 config address_binding recover_learning ports

Description

This command is used to recover IMPB checking.

Format

config address_binding recover_learning ports [<portlist> | all]

Parameters

<portlist> - Enter the list of port used here.
all - Specify 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-3000-28SC:admin#config address_binding recover_learning ports 6-7
Command: config address_binding recover_learning ports 6-7

Success.

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

42-28 config address_binding dhcp snooping ports

Description

This command is used to configure the DHCP snooping rate limit state.

Format

config address_binding dhcp snooping ports [<portlist> | all] limit [rate <value 1-2048> mode [drop | shutdown] | no_limit]

Parameters

<portlist> - Specify list of ports to be configured.
all - Specify to configure all ports.
limit - Specify the reate limit. **rate** - The number of DHCP messages that an interface can receive per second. **<value 1-2048>** - Enter the value between 1 and 2048. **mode** - Specify the DHCP protection mode. The default is *shutdown*. **drop** - Drop all the above rate limit DHCP packets when the port enters the under attack state. **shutdown** - Shut down the port when the port enters the under attack state. **no_limit** – Disable DHCP snooping rate limiting. This is the default.

Restrictions

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

Example

To configure limit 10pps DHCP packet on port 1:

```
DGS-3000-28SC:admin# config address_binding dhcp snooping ports 1:1 limit rate
10 mode drop
Command: config address_binding dhcp snooping ports 1:1 limit rate 10 mode drop

Success.

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

42-29 config address_binding dhcp snooping recovery_timer

Description

This command is used to configure the auto recovery timer value.

Format

config address_binding dhcp snooping recovery_timer [<sec 60-1000000> | infinite]

Parameters

<sec 60-1000000> - Enter a value between 60 and 1000000 for the time interval used by the auto-recovery mechanism.
infinite - Specify that the port cannot be auto-recovered.

Restrictions

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

Example

To configure the auto-recovery time as 1000 seconds:

```
DGS-3000-28SC:admin# config address_binding dhcp snooping recovery_timer 1000
Command: config address_binding dhcp snooping recovery_timer 1000

Success.

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

42-30 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-3000-28SC:admin#enable address_binding roaming
Command: enable address_binding roaming

Success.

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

42-31 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-3000-28SC:admin#disable address_binding roaming
Command: disable address_binding roaming

Success.

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

42-32 upload address_binding snoop_entry_toFTP

Description

This command is used to upload DHCPv4 Snooping binding entries by FTP.

Format

upload address_binding snoop_entry_toFTP [<ipaddr> {tcp_port <tcp_port_number 1-65535>} filename <path_filename64> | ftp: <string user:pasword@ipaddr:tcpport/path_filename>]

Parameters

<ipaddr> - Enter the IPv4 address of the FTP server here. **tcp_port** Specify the TCP port here. **<tcp_port_number 1-65535>** - Enter the TCP port number here. Use a number within the range 1 to 65535. **filename** - Specify the path of the file located on the FTP server. **<path_filename 64>** - Enter the file path, located on the TFTP server, here.
ftp: <string user:pasword@ipaddr:tcpport/path_filename>] - Specify the standard FTP command, containing a user name, password, server IP, TCP port, the directory of a file, and a file name; For example: Tony:123456@172.18.211.41:21/image/dhcpsnp.cfg.

Restrictions

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

Example

To upload the DHCP snooping binding table by FTP:

```
DGS-3000-28SC:admin# upload address_binding snoop_entry_fromFTP 10.0.0.1
tcp_port 21 filename impb.cfg
Command: upload address_binding snoop_entry_fromFTP 10.0.0.1 tcp_port 21
filename impb.cfg

Connecting to server.................. Done.
User(Anonymous): Tony
Pass:******
Upload DHCPv4 Snooping binding table................. Done.

Success.

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

To upload the DHCP snooping binding table by FTP using string:

```
DGS-3000-28SC:admin# upload address_binding snoop_entry_fromFTP
ftp:Tony:123456@10.54.71.1:21/cfg/dhccpsnp.cfg
Command: upload address_binding snoop_entry_fromFTP
ftp:Tony:123456@10.54.71.1:21/cfg/dhccpsnp.cfg

Connecting to server.................. Done.
Upload DHCPv4 Snooping binding table................. Done.

Success.

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

42-33 upload address_binding snoop_entry_toTFTP

Description

This command is used to upload DHCPv4 Snooping binding entries by TFTP.

Format

upload address_binding snoop_entry_toTFTP [<ipaddr> | <ipv6addr> | <domain_name 255>] filename <path_filename 64>

Parameters

<ipaddr> - Enter the IPv4 address of the TFTP server here.
<ipv6addr> - Enter the IPv6 address of the TFTP server here.
domain_name 255 - Specify the domain name to be up to 255 characers long.
filename - Specify the path of the file located on the TFTP server. **<path_filename 64>** - Enter the file path, located on the TFTP server, here.

Restrictions

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

Example

To upload the DHCP snooping binding table by TFTP:

```
DGS-3000-28SC:admin# upload address_binding snoop_entry_toTFTP 10.0.0.1
filename impb.cfg
Command: upload address_binding snoop_entry_toTFTP 10.0.0.1 filename impb.cfg

Success.

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

42-34 download address_binding snoop_entry_fromFTP

Description

This command is used to download DHCPv4 Snooping binding entries by FTP.

Format

download address_binding snoop_entry_fromFTP [<ipaddr> {tcp_port <tcp_port_number 1-65535>} filename <path_filename 64> | ftp: <string user:password@ipaddr:tcpport/path_filename>]

Parameters

<ipaddr> - Enter the IPv4 address of the FTP server here. **tcp_port** Specify the TCP port here. **<tcp_port_number 1-65535>** - Enter the TCP port number here. Use a number within the range 1 to 65535. **filename** - Specify the path of the file located on the FTP server. **<path_filename 64>** - Enter the file path, located on the TFTP server, here.
ftp: <string user:pasword@ipaddr:tcpport/path_filename>] - Specify the standard FTP command, containing a user name, password, server IP, TCP port, the directory of a file, and a file name; For example: Tony:123456@172.18.211.41:21/image/dhcpsnp.cfg.

Restrictions

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

Example

To download the DHCP snooping binding table by FTP:

```
DGS-3000-28SC:admin# download address_binding snoop_entry_fromFTP
10.0.0.1tcp_port 21filename impb.cfg
Command: download address_binding snoop_entry_fromFTP 10.0.0.1 tcp_port
21filename impb.cfg

Connecting to server.................. Done.
User(Anonymous): Tony
Pass:******
Download DHCPv4 Snooping binding table................. Done.

Success.

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

To download the DHCP snooping binding table by FTP using string:

```
DGS-3000-28SC:admin# download address_binding snoop_entry_fromFTP
ftp:Tony:123456@10.54.71.1:21/cfg/dhccpsnp.cfg
Command: download address_binding snoop_entry_fromFTP
ftp:Tony:123456@10.54.71.1:21/cfg/dhccpsnp.cfg

Connecting to server.................. Done.
Download DHCPv4 Snooping binding table................. Done.

Success.

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

42-35 download address_binding snoop_entry_fromTFTP

Description

This command is used to download DHCPv4 Snooping binding entries by TFTP.

Format

download address_binding snoop_entry_fromTFTP [<ipaddr> | <ipv6addr> | <domain_name 255>] filename <path_filename 64>

Parameters

<ipaddr> - Enter the IPv4 address of the TFTP server here.
<ipv6addr> - Enter the IPv6 address of the TFTP server here.
<domain_name 255> - Enter the domain name of the TFTP server here. This name can be up to 255 characters long.
filename - Specify the path of the file to the TFTP server. **<path_filename 64>** - Enter the file path, to the TFTP server, here.

Restrictions

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

Example

To download the DHCP snooping binding table:

```
DGS-3000-28SC:admin# download address_binding snoop_entry_fromTFTP 10.90.90.6
filename impb.cfg
Command: download address_binding snoop_entry_fromTFTP 10.90.90.6 filename
impb.cfg

Connecting to server.................. Done.
Download DHCP Snooping Entry.............. Done.

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

Chapter 43 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>
config ipv6 nd ra ipif <ipif_name 12> {state [enable | disable] | life_time <sec 0-9000> | reachable_time <millisecond 0-3600000> | retrans_time <millisecond 0-4294967295> | hop_limit <value 0-255> | managed_flag [enable | disable] | other_config_flag [enable | disable] | min_rtr_adv_interval <sec 3-1350> | max_rtr_adv_interval <sec 4-1800>}(1)
show ipv6 nd {ipif <ipif_name 12>}
config ipv6 nd ra prefix_option ipif <ipif_name 12> <ipv6networkaddr> {preferred_life_time <sec 0-4294967295> | valid_life_time <sec 0-4294967295> | on_link_flag [enable | disable] | autonomous_flag [enable | disable]}(1)

43-1 create ipv6 neighbor_cache ipif

Description

This command is used to add a static neighbor on an IPv6 interface.

Format

create ipv6 neighbor_cache ipif <ipif_name 12> <ipv6addr> <macaddr>

Parameters

<ipif_name 12> - Enter the IP interface name here. This name can be up to 12 characters long.
<ipv6addr> - Enter the IPv6 address of the neighbor.
<macaddr> - Enter the MAC address of the neighbor.

Restrictions

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

Example

Create a static neighbor cache entry:

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

43-2 delete ipv6 neighbor_cache ipif

Description

This command is used to delete a neighbor cache entry or static neighbor cache entries from the address cache or all address cache entries on this IP interface. Both static and dynamic entries can be deleted.

Format

delete ipv6 neighbor_cache ipif [<ipif_name 12> | all] [<ipv6addr> | static | dynamic | all]

Parameters

<ipif_name 12> - Enter the IP interface name here. This name can be up to 12 characters long.
all - Specify that all the interfaces will be used in this configuration.
<ipv6addr> - Enter 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-3000-28SC:admin#delete ipv6 neighbor_cache ipif System 3ffc::1
Command: delete ipv6 neighbor_cache ipif System 3FFC::1

Success.

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

43-3 show ipv6 neighbor_cache ipif

Description

This command is used to display the neighbor cache entry for the specified interface. You can display a specific entry, all entries, or all static entries.

Format

show ipv6 neighbor_cache ipif [<ipif_name 12> | all] [ipv6address <ipv6addr> | static | dynamic | all]

Parameters

<ipif_name 12> - Enter the IP interface name here. This name can be up to 12 characters long.
all - Specify that all the interface will be displayed.
ipv6address - Specify 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-3000-28SC: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-3000-28SC:admin#
```

43-4 config ipv6 nd ns ipif

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_name 12> - Enter the IPv6 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-3000-28SC:admin#config ipv6 nd ns ipif Zira retrans_time 1000000
Command: config ipv6 nd ns ipif Zira retrans_time 1000000

Success.

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

43-5 config ipv6 nd ra ipif

Description

This command is used to configure the RA parameters of a specified interface.

Format

config ipv6 nd ra ipif <ipif_name 12> {state [enable | disable] | life_time <sec 0-9000> | reachable_time <millisecond 0-3600000> | retrans_time <millisecond 0-4294967295> | hop_limit <value 0-255> | managed_flag [enable | disable] | other_config_flag [enable | disable] | min_rtr_adv_interval <sec 3-1350> | max_rtr_adv_interval <sec 4-1800>}(1)

Parameters

<ipif_name 12> - Specify the name of the interface.
state - Specify the router advertisement status. **enable** - Enable the router advertisement state. **disable** - Disable the router advertisement state.
life_time - Specify the lifetime of the router as the default router, in seconds. **<sec 0-9000>** - Specify the time between 0 and 9000 seconds.
reachable_time - Specify the amount of time that a node can consider a neighboring node reachable after receiving a reachability confirmation, in milliseconds. **<millisecond 0-3600000>** - Specify the time between 0 and 3600000 milliseconds.
retrans_time - Specify the amount of time that a node can consider a neighboring node reachable after receiving a reachability confirmation, in milliseconds. **<millisecond 0-4294967295>** - Specify the time between 0 and 4294967295 milliseconds.
hop_limit - Specify the default value of the hop limit field in the IPv6 header for packets sent by hosts that receive this RA message. **<value 0-255>** - Specify the value between 0 and 255.
managed_flag - Specify to enable or disable the function. **enable** - When set to enable, it indicates that hosts receiving this RA must use a stateful address configuration protocol to obtain an address, in addition to the addresses derived from the stateless address configuration. **disable** - Set to disable to stop hosts receiving the RA from using a stateful address configuration to obtain an address.
other_config_flag - Specify to enable or disable the function. **enable** - When set to enable, it indicates that hosts receiving this RA must use a stateful address configuration protocol to obtain on-address configuration information. **disable** - Set to disable to stop hosts receiving this RA from using a stateful address configuration protocol to obtain on-address configuration information.
min_rtr_adv_interval - Specify the minimum time allowed between sending unsolicited multicast Router Advertisements from the interface, in seconds. It must be no less than 3 seconds and no greater than .75 * MaxRtrAdvInterval. The default is 0.33 * MaxRtrAdvInterval. **<sec 3-1350>** - Specify the time between 3 and 1350 seconds.

max_rtr_adv_interval - Specify the maximum time allowed between sending unsolicited multicast Router Advertisements from the interface, in seconds. It must be no less than 4 seconds and no greater than 1800 seconds. The default is 600 seconds. **<sec 4-1800>** - Specify the time between 4 and 1800 seconds.

Restrictions

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

Example

To configure the RA state as enabled and the life_time of the “System” interface to be 1000 seconds:

```
DGS-3000-28SC:admin# config ipv6 nd ra ipif System state enable life_time 1000
Command: config ipv6 nd ra ipif System state enable life_time 1000

Success.

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

43-6 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-3000-28SC:admin#show ipv6 nd ipif System
Command: show ipv6 nd ipif System


Interface Name            : System
Hop Limit                 : 64
NS Retransmit Time        : 0 (ms)
Router Advertisement      : Disabled
RA Max Router AdvInterval : 600 (sec)
RA Min Router AdvInterval : 198 (sec)
RA Router Life Time       : 1800 (sec)
RA Reachable Time         : 1200000 (ms)
RA Retransmit Time        : 0 (ms)
RA Managed Flag           : Disabled
RA Other Configuration Flag      : Disabled

DGS-3000-28SC:admin
```

43-7 config ipv6 nd ra prefix_option ipif

Description

This command is used to configure the prefix option for the router advertisement function.

Format

config ipv6 nd ra prefix_option ipif <ipif_name 12> <ipv6networkaddr> {preferred_life_time <sec 0-4294967295> | valid_life_time <sec 0-4294967295> | on_link_flag [enable | disable] | autonomous_flag [enable | disable]}(1)

Parameters

<ipif_name 12> - Specify the name of the interface. The maximum length is 12 characters.
<ipv6networkaddr> - Specify the IPv6 network address.
preferred_life_time - Specify the number in milliseconds that an address, based on the specified prefix using the stateless address configuration, remains in preferred state. **<sec 0-4294967295>** - Specify the time between 0 and 4294967295 milliseconds. For an infinite valid lifetime the value can be set to 4294967295.
valid_life_time - Specify the number of seconds that an address, based on the specified prefix, using the stateless address configuration, remains valid. **<sec 0-4294967295>** - Specify the time between 0 and 4294967295 milliseconds. For an infinite valid lifetime the value can be set to 4294967295.
on_link_flag - Specify to enable or disable the function. **enable** - Setting this field to enable will denote, within the IPv6 packet, that the IPv6 prefix configured here is assigned to this link-local network. Once traffic has been successfully sent to these nodes with this specific IPv6 prefix, the nodes will be considered reachable on the link-local network. **disable** - When set to disable, the addresses implied by the specified prefix are not available on the link where the RA message is received.
autonomous_flag - Specify to enable or disable the function. **enable** - Setting this field to enable will denote that this prefix may be used to autoconfigure IPv6 addresses on the link-local network. **disable** - When set to disable, the specified prefix will not be used to create an autonomous address configuration.

Restrictions

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

Example

To configure the value of the preferred_life_time of prefix option to be 1000 seconds for the prefix 3ffe:501:ffff:100::/64, which is the prefix of the ip1 interface:

```
DGS-3000-28SC:admin#config ipv6 nd ra prefix_option ipif ip1
3ffe:501:ffff:100::/64 preferred_life_time 1000
Command: config ipv6 nd ra prefix_option ipif ip1 3ffe:501:ffff:100::/64
preferred_life_time 1000


Success.


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

Chapter 44 IPv6 Route Command List

create ipv6route [default | <ipv6networkaddr>] [<ipif_name 12> <ipv6addr> | <ipv6addr>] {<metric 1-65535>} {[primary | backup]}
delete ipv6route [[default | <ipv6networkaddr>] [<ipif_name 12> <ipv6addr> | <ipv6addr>] | all]
show ipv6route {[<ipv6networkaddr> | <ipv6addr>]} {[static | hardware]}

44-1 create ipv6route

Description

This command is used to create an IPv6 static route. The primary route has higher priority than backup. When primary route is inactive, the backup route will be used. One static route will be primary route by default if there is no primary route to this destination yet

Format

create ipv6route [default | <ipv6networkaddr>] [<ipif_name 12> <ipv6addr> | <ipv6addr>] {<metric 1-65535>} {[primary | backup]}

Parameters

default - Specify an IPv6 default route.
<ipv6networkaddr> - Enter the IPv6 address and prefix of the destination of the route.
<ipif_name 12> - Enter the ipif_name to specify the IP interface for this route from an exisiting interface. Enter the IPv6 route name using a maximum of 12 characters. **<ipv6addr>** - Enter the next hop address of the route.
<ipv6addr> - Specify the next ipv6 address hop of the route.
<metric 1-65535> - (Optional) Allows the entry of a routing protocol metric entry representing the number of routers between the Switch and the IPv6 address above. The default setting is 1
primary - (Optional) Specify the route as the primary route to the destination.
backup - (Optional) Specify the route as the backup route to the destination

Restrictions

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

Example

To create an IPv6 static route with outgoing interface System:

```
DGS-3000-28SC:admin# create ipv6route 5000::/64 System FE80::1
Command: create ipv6route 5000::/64 System FE80::1

Success.

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

44-2 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 | <ipv6networkaddr>] [<ipif_name 12> <ipv6addr> | <ipv6addr>] | all]

Parameters

default - Specify the default route.
<ipv6networkaddr> - Enter the destination network route.
<ipif_name 12> - Enter the IP interface name used here. This name can be up to 12 characters long. **<ipv6addr>** - Enter the next hop address for the route.
<ipv6addr> - Enter the next hop address for the route.
all - Specify to delete all created static routes.

Restrictions

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

Example

To delete an IPv6 static route:

```
DGS-3000-28SC:admin#delete ipv6route default System 3FFC::1
Command: delete ipv6route default System 3FFC::1

Success.

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

44-3 show ipv6route

Description

This command is used to display IPv6 routes.

Format

show ipv6route {[<ipv6networkaddr> | <ipv6addr>]} {[static | hardware]}

Parameters

<ipv6networkaddr> - (Optional) Enter the destination network address of the route to be displayed.
<ipv6addr> - (Optional) Enter the destination IPv6 address of the route to be displayed. The

longest prefix matched route will be displayed
static - (Optional) Specify to display only static routes. One static route may be active or inactive.
hardware - (Optional) Specify to display only the route entries which have been wrote into hardware table.

Restrictions

None.

Example

To show all the IPv6 routes:

```
DGS-3000-28SC:admin#show ipv6route
Command: show ipv6route

IPv6 Prefix: 2002::/16                        Protocol: Static  Metric: 1
Next Hop   : ::                               IPIF    : tn2

IPv6 Prefix: 2002:404:104:1::/64              Protocol: Local   Metric: 1
Next Hop   : ::                               IPIF    : tn2

Total Entries: 2

DGS-3000-28SC:admin#show ipv6route static
Command: show ipv6route static

IPv6 Prefix: 3000:62:1::/64                   Protocol: Static  Metric: 1
Next Hop   : ::                               IPIF    : tn1
Backup     : Primary                          Status  : Active

Total Entries: 1

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

Chapter 45 Jumbo Frame Command List

enable jumbo_frame
disable jumbo_frame
show jumbo_frame
config jumbo_frame ports [<portlist> | all] state [enable | disable]

45-1 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-3000-28SC:admin#enable jumbo_frame
Command: enable jumbo_frame

The maximum size of jumbo frame is 13312 bytes.
Success.

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

45-2 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-3000-28SC:admin#disable jumbo_frame
Command: disable jumbo_frame

Success.

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

45-3 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-3000-28SC:admin#show jumbo_frame
Command: show jumbo_frame

Jumbo Frame State  : Disabled
Maximum Frame Size : 1536 Bytes

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

45-4 config jumbo_frame ports

Description

This command is used to configure the jumbo frame state on specified ports.

Format

config jumbo_frame ports [<portlist> | all] state [enable | disable]

Parameters

<portlist> - (Optional) Enter a range of ports to be configured with the jumbo frame state.
all - Specify to use this parameter to configure all ports of the switch to be configured with the jumbo frame state.
state - Specify the jumbo frame state to be applied to a range of ports specified. **enable** - Enable the jumbo frame state on the specified ports. **disable** - Disable the jumbo frame state on the specified ports.

Restrictions

Only Administrators, Operators, and Power users can issue this command.

Example

To enable jumbo frames on ports 1:1-1:5:

```
DGS-3000-28SC:admin# config jumbo_frame ports 1:1-1:5 state enable
Command: config jumbo_frame ports 1:1-1:5 state enable

Success.

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

Chapter 46 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]
config l2protocol_tunnel tunneled_protocol [stp | gvrp | 01-00-0C-CC-CC-CC | 01-00-0C-CC-CC-CD | all] [mac_address <macaddr> | default]
show l2protocol_tunnel {[uni | nni]}

46-1 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-3000-28SC:admin#enable l2protocol_tunnel
Command: enable l2protocol_tunnel

Success.

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

46-2 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-3000-28SC:admin#disable l2protocol_tunnel
Command: disable l2protocol_tunnel

Success.

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

46-3 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> - Enter a list of ports on which the Layer 2 protocol tunneling to be configured.
all - Specify to have all ports to be configured
type - Specify the type of the ports. **uni** - Specify the ports as UNI ports. **tunneled_protocol** - Specify tunneled protocols on the UNI ports. **stp** - Specify to use the STP protocol. **gvrp** - Specify to use the GVRP protocol. **protocol_mac** - Specify the destination MAC address of the L2 protocol packets that will tunneled on these UNI ports.

01-00-0C-CC-CC-CC - Specify the MAC address as 01-00-0C-CC-CC-CC.
01-00-0C-CC-CC-CD - Specify 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) Specify the drop threshold for packets-per-second accepted on the UNI ports. The ports drop the PDU if the protocol's threshold is exceeded.
<value 0-65535> - Enter the threshold range value between 0 to 65535 (packet/second). 0 means no limit. By default, the value is 0.
nni - Specify 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-3000-28SC: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-3000-28SC:admin#
```

46-4 config l2protocol_tunnel tunneled protocol

Description

This command is used to configure the layer 2 protocol tunneling multicast address for the specified protocol. If configured to default, the layer 2 protocol tunneling multicast addresses are as following:

1. The layer 2 protocol tunneling multicast address for STP is 01-05-5D-00-00-00.
2. The layer 2 protocol tunneling multicast address for GVRP is 01-05-5D-00-00-21.
3. The layer 2 protocol tunneling multicast address for CISCO protocol MAC 01-00-0C-CC-CC-CC is 01-05-5D-00-00-10.
4. The layer 2 protocol tunneling multicast address for CISCO protocol MAC 01-00-0C-CC-CC-CD is 01-05-5D-00-00-11

When configure the tunneling multicast address, some MAC addresses which are reserved or used by other protocols should not be configured. Such as Broadcast MAC address, Zero MAC address, Unicast MAC address and so on. The detail information is as following:

FF-FF-FF-FF-FF-FF, 00-00-00-00-00-00, Unicast MAC address, 01-00-08-06-0F-0F

01-00-0C-CC-CC-CC, 01-00-0C-CC-CC-CD, 01-19-A7-00-00-01, 01-1B-19-00-00-00

01-80-C2-00-00-00 to 01-80-C2-00-00-0F, 01-80-C2-00-00-10, 01-80-C2-00-00-20 to 01-80-C2-00-00-2F, 01-00-5E-00-00-00 to 01-00-5E-FF-FF-FF, 33-33-00-00-00-04, 33-33-00-00-00-05

33-33-00-00-00-06, 33-33-00-00-00-09, 33-33-00-00-00-0D, CF-00-00-00-00-00

Format

config l2protocol_tunnel tunneled_protocol [stp | gvrp | 01-00-0C-CC-CC-CC | 01-00-0C-CC-CC-CD | all] [mac_address <macaddr> | default]

Parameters

stp - Specify the BPDU received on the UNI will be tunneled to the configured address.
gvrp - Specify the GVRP PDU received on the UNI will be tunneled to the configured address.
01-00-0C-CC-CC-CC - Specify another vendor's PDU received on the UNI will be tunneled to the configured address.
01-00-0C-CC-CC-CD - Specify another vendor's PDU received on the UNI will be tunneled to the configured address.
all - Specify all supported protocols.
mac_address - Specify the address which the specified protocol will be tunneled to. This address should not be the address which is reserved or used by other protocols. **<macaddr>** - Enter the MAC address here.
default - Specify the specified protocol to be tunneled to the default address.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure tunneling multicast address of STP to 01-00-0c-cd-cd-d0:

```
DGS-3000-28SC:admin# config l2protocol_tunnel tunneled_protocol stp mac_address
01-00-0C-CD-CD-D0
Command: config l2protocol_tunnel tunneled_protocol stp mac_address 01-00-0C-
CD-CD-D0

Success.

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

46-5 show l2protocol_tunnel

Description

This command is used to display Layer 2 protocol tunneling information.

Format

show l2protocol_tunnel {[uni | nni]}

Parameters

uni - Specify to show UNI detail information.
nni - Specify to show NNI detail information.

Restrictions

None.

Example

To show Layer 2 protocol tunneling information summary:

```
DGS-3000-28SC:admin#show l2protocol_tunnel
Command: show l2protocol_tunnel

Global State :Global State : Enabled
UNI Ports    : 1-4
NNI Ports    :
Protocol           Tunneling Address
-----------------  -----------------
STP                01-05-5D-00-00-00
GVRP               01-05-5D-00-00-21
01-00-0C-CC-CC-CC  01-05-5D-00-00-10
01-00-0C-CC-CC-CD  01-05-5D-00-00-11

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

To show Layer 2 protocol tunneling information summary:

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

Chapter 47 Link Aggregation Command List

create link_aggregation group_id <value 1-32> {type [lacp | static]}
delete link_aggregation group_id <value 1-32>
config link_aggregation group_id <value> {master_port <port> | ports <portlist> | state [enable | disable] | trap [enable | disable]}
config link_aggregation algorithm [mac_source | mac_destination | mac_source_dest | ip_source | ip_destination | ip_source_dest]
show link_aggregation {group_id <value 1-32> | algorithm}
config lacp_port <portlist> {mode [active | passive] | lacp_timeout [short | long]} (1)
show lacp_port {<portlist>}

47-1 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 1-32> {type [lacp | static]}

Parameters

<value 1-32> - Enter the group ID value here. This value must be between 1 and 32.
type - (Optional) Specify the group type is belong to static or LACP. If type is not specified, the default is static type. **lacp** - Specify to use LACP as the group type. **static** - Specify 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-3000-28SC:admin#create link_aggregation group_id 1 type lacp
Command: create link_aggregation group_id 1 type lacp

Success.

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

47-2 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 1-32>

Parameters

<value 1-32> - Enter the group ID value here. The value can be between 1 to 32 characters.

Restrictions

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

Example

To delete link aggregation group:

```
DGS-3000-28SC:admin#delete link_aggregation group_id 3
Command: delete link_aggregation group_id 3

Success.

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

47-3 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] | trap [enable | disable]}

Parameters

<value> - Enter the group ID value here. This value must be between 1 and 32.
master_port - (Optional) Master port ID. Specify 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) Specify a range of ports that will belong to the link aggregation group. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 would specify switch number 1, port 3. 2:4 specifies switch number 2, port 4.

<portlist> - Enter the list of port used for the configuration here.
state - (Optional) 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** - Enable the specified link aggregation group. **disable** - Disable the specified link aggregation group.
trap - (Optional) Specify the state of Link Up and Link Down notifications. **enable** - Enable Link Up and Link Down notifications. **disable** - Disable Link Up and Link Down notifications.

Restrictions

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

Example

To configure a previously created link aggregation group:

```
DGS-3000-28SC:admin# config link_aggregation group_id 1 master_port 1:5 ports
1:5-1:7
Command: config link_aggregation group_id 1 master_port 1:5 ports 1:5-1:7

Success.

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

47-4 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-3000-28SC:admin#config link_aggregation algorithm mac_source_dest
Command: config link_aggregation algorithm mac_source_dest

Success.

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

47-5 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 1-32> | algorithm}

Parameters

group_id - (Optional) Specify the group ID. The group number identifies each of the groups. **<value 1-32>** - Enter the group ID value here. There can be up to 32.
algorithm - (Optional) Allows you to specify the display of link aggregation by the algorithm in use by that group.
If no parameter is specified, system will display all link aggregation information.

Restrictions

None.

Example

Link aggregation group enabled:

```
DGS-3000-28SC:admin#show link_aggregation
Command: show link_aggregation

Link Aggregation Algorithm = MAC-source-dest
Group ID     : 1
Type   : LACP
Master Port   : 1
Member Port   : 1-8
Active Port   : 7
Status        : Enabled
Flooding Port       : 7
Trap                : Disabled

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

Link aggregation group enable and no member linkup:

```
DGS-3000-28SC:admin#show link_aggregation
Command: show link_aggregation

Link Aggregation Algorithm = MAC-source-dest
Group ID     : 1
Type   : LACP
Master Port   : 1
Member Port   : 1-8
Active Port   :
Status : Enabled
Flooding Port :
Trap                : Disabled

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

Link aggregation group disabled:

```
DGS-3000-28SC:admin#show link_aggregation
Command: show link_aggregation

Link Aggregation Algorithm = MAC-source-dest
Group ID     : 1
Type   : LACP
Master Port   : 1
Member Port   : 1-8
Active Port   :
Status : Disabled
Flooding Port :
Trap                : Disabled

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

47-6 config lacp_port

Description

This command is used to configure per-port LACP mode.

Format

config lacp_port <portlist> {mode [active | passive] | lacp_timeout [short | long]}(1)

Parameters

<portlist> - Enter the list of port used for the configuration here.
mode - Specify the LACP mode used. **active** - Specify to set the LACP mode as active. **passive** - Specify to set the LACP mode as passive.
lacp_timeout - (Optional) Specify the LACP timeout. **short** - Specify to be 3 seconds before LACP invalidating received LACPDU information and there will be 1 second between LACP PDU periodic transmissions when using Short Timeouts. **long** - Specify to be 90 seconds before LACP invalidating received LACPDU information and there will be 30 seconds between LACP PDU periodic transmissions when using Long Timeouts

Restrictions

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

Example

To config port LACP activity mode:

```
DGS-3000-28SC:admin# config lacp_port 1-12 mode active
Command: config lacp_port 1-12 mode active

Success.

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

To config port LACP timeout mode:

```
DGS-3000-28SC:admin# config lacp_port 1-12 lacp_timeout long
Command: config lacp_port 1-12 lacp_timeout long

Success.

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

47-7 show lacp_port

Description

This command is used to display the current mode of LACP of the ports.

Format

show lacp_port {<portlist>}

Parameters

<portlist> - (Optional) Enter the list of ports to be displayed here.
If no parameter is specified, the system will display current LACP and all port status.

Restrictions

None.

Example

To show port LACP activity and timeout mode:

```
DGS-3000-28SC:admin# show lacp_port
Command: show lacp_port

Port    Activity  LACP_Timeout
------  --------  -------------
1       Active     Short
2       Active     Short
3       Active     Short
4       Active     Long
5       Active     Long
6       Active     Long
7       Active     Long
8       Active     Long
9       Active     Long
10      Active     Long
11      Active     Short
12      Active     Short

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

Chapter 48 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] | port_id_subtype [mac_address | local]] | dot1_tlv_pvid [enable | disable] | dot1_tlv_protocol_vid [vlan [all | <vlan_name32>] | vlanid <vidlist>] [enable | disable] | dot1_tlv_vlan_name [vlan [all | <vlan_name32>] | vlanid <vidlist>] [enable | disable] | dot1_tlv_protocol_identity [all | {eapol | lacp | gvrp | stp}] [enable | disable] | dot3_tlvs [{all} | {mac_phy_configuration_status | link_aggregation | maximum_frame_size}] [enable | disable]]
config lldp forward_message [enable | disable]
show lldp
show lldp mgt_addr {[ipv4 {<ipaddr>} | ipv6 {<ipv6addr>}]}
show lldp ports {<portlist>}
show lldp local_ports {<portlist>} {mode [brief | normal | detailed]}
show lldp remote_ports {<portlist>} {mode [brief | normal | detailed]}
show lldp statistics
show lldp statistics ports {<portlist>}

48-1 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-3000-28SC:admin#enable lldp
Command: enable lldp

Success.

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

48-2 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-3000-28SC:admin#disable lldp
Command: disable lldp

Success.

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

48-3 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 - Specify to configure the message hold multiplier. The default setting 4. **<int 2-10>** - Enter the message transmit hold multiplier value here. This value must be between 2 and 10.
tx_delay - Specify 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 - Specify 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-3000-28SC:admin#config lldp message_tx_interval 30
Command: config lldp message_tx_interval 30

Success.

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

48-4 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

<sec 5-3600> - Enter the notification interval for sending notification to configured SNMP trap receiver(s) here. This value must be between 5 and 3600 seconds. The default setting is 5

seconds.

Restrictions

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

Example

To changes the notification interval to 10 second:

```
DGS-3000-28SC:admin#config lldp notification_interval 10
Command: config lldp notification_interval 10

Success.

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

48-5 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] | port_Id_subtype [mac_address | local]] | dot1_tlv_pvid [enable | disable] | dot1_tlv_protocol_vid [vlan [all | <vlan_name32>] | vlanid <vidlist>] [enable | disable] | dot1_tlv_vlan_name [vlan [all | <vlan_name32>] | vlanid <vidlist>] [enable | disable] | dot1_tlv_protocol_identity [all | {eapol | lacp | gvrp | stp}] [enable | disable] |dot3_tlvs [{all} | {mac_phy_configuration_status | link_aggregation | maximum_frame_size}] [enable | disable]]

Parameters

<portlist> - Enter a list of ports used for the configuration here.
all - Specify 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** - Specify that the SNMP trap notification of LLDP data changes detected will be enabled. **disable** - Specify that the SNMP trap notification of LLDP data changes detected will be disabled.
admin_status - Specify the per-port transmit and receive modes. **tx_only** - Configure the specified port(s) to transmit LLDP packets, but block inbound LLDP packets from neighbor devices. **rx_only** - Configure the specified port(s) to receive LLDP packets from neighbors, but block outbound packets to neighbors. **tx_and_rx** - Configure the specified port(s) to both transmit and receive LLDP packets. **disable** - Disable LLDP packet transmit and receive on the specified port(s).
mgt_addr - Specify the management address used.

ipv4 - Specify the IPv4 address used.
<ipaddr> - (Optional) Enter the IP address used for this configuration here.
ipv6 - Specify the IPv6 address used.
<ipv6addr> - (Optional) Enter the IPv6 address used for this configuration here.
enable - Specify that the advertising indicated management address instance will be enabled.
disable - Specify that the advertising indicated management address instance will be disabled.

basic_tlvs - Specify the basic TLV data types used from outbound LLDP advertisements.
all - (Optional) Specify 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 - Specify that the basic TLV data types used from outbound LLDP advertisements will be enabled.
disable - Specify that the basic TLV data types used from outbound LLDP advertisements will be disabled.
port_Id_subtype - Specify the port ID TLV sub-type. The default subtype is local.
mac_address - Specify the sub-type of the port ID TLV using 'MacAddress(3)' and the value uses 'MacAddress'.
local - Specify the sub-type of the port ID TLV using 'Local(7)' and the value uses the port number. This is the default option.

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 - Specify that the Dot1 TLV PVID option will be enabled.
disable - Specify 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 - Specify the VLAN used for this configuration.
all - Specify 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 - Specify the VLAN ID used for this configuration.
<vlanid_list> - Enter the ID of the VLAN here.
enable - Specify that the Dot1 TLV protocol VID will be enabled.
disable - Specify 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 - Specify the VLAN used for this configuration.
all - Specify 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 - Specify the VLAN ID used for this configuration.
<vlanid_list> - Enter the ID of the VLAN here.
enable - Specify that the Dot1 TLV VLAN name will be enabled.
disable - Specify 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** - Specify that all the vendor proprietary protocols will be advertised. **eapol** - (Optional) Specify that the EAPOL protocol will be advertised. **lacp** - (Optional) Specify that the LACP protocol will be advertised. **gvrp** - (Optional) Specify that the GVRP protocol will be advertised. **stp** - (Optional) Specify that the STP protocol will be advertised. **enable** - Specify that the protocol identity TLV according to the protocol specified will be adverstised. **disable** - Specify that the protocol identity TLV according to the protocol specified will not be adverstised.
dot3_tlvs - Specify that the IEEE 802.3 specific TLV data type will be configured.	
	all - (Optional) Specify 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. **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** - Specify that the IEEE 802.3 specific TLV data type selected will be advertised. **disable** - Specify 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 1:1-1:5:

```
DGS-3000-28SC:admin# config lldp ports 1:1-1:5 notification enable
Command: config lldp ports 1:1-1:5 notification enable

Success.

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

To configure port 1:1-1:5 to transmit and receive:

```
DGS-3000-28SC:admin#config lldp ports 1:1-1:5 admin_status tx_and_rx
Command: config lldp ports 1:1-1:5 admin_status tx_and_rx

Success.

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

To enable ports 1-2 for manage address entry:

```
DGS-3000-28SC:admin#config lldp ports 1:1-1:2 mgt_addr ipv4 192.168.254.10
enable
Command: config lldp ports 1:1-1:2 mgt_addr ipv4 192.168.254.10 enable

Success

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

To configure exclude the system name TLV from the outbound LLDP advertisements for all ports:

```
DGS-3000-28SC:admin#config lldp ports all basic_tlvs system_name enable
Command: config lldp ports all basic_tlvs system_name enable

Success.

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

To configure exclude the vlan nameTLV from the outbound LLDP advertisements for all ports:

```
DGS-3000-28SC:admin#config lldp ports all dot1_tlv_protocol_vid vlan default
enable
Command: config lldp ports all dot1_tlv_protocol_vid vlan default enable

Success.

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

To configure exclude the port and protocol VLAN ID TLV from the outbound LLDP advertisements for all ports:

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

To configure exclude the VLAN name TLV from the outbound LLDP advertisements for all ports:

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

To configure exclude the protocol identity TLV from the outbound LLDP advertisements for all ports:

```
DGS-3000-28SC:admin#  config lldp ports all dot1_tlv_protocol_identity all
enable
Command: config lldp ports all dot1_tlv_protocol_identity all enable

Success.

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

To configure exclude the MAC/PHY configuration/status TLV from the outbound LLDP advertisements for all ports:

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

48-6 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

enable - Enable the forwarding of LLDP PDU configuration events.
disable - Disable the forwarding of LLDP-PDU events. By default it is disabled.

Restrictions

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

Example

To configure LLDP to forward LLDP PDUs:

```
DGS-3000-28SC:admin#config lldp forward_message enable
Command: config lldp forward_message enable

Success.

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

48-7 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-3000-28SC: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-3000-28SC:admin#
```

48-8 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) Specify the IPv4 address used for the display. **<ipaddr>** - (Optional) Enter the IPv4 address used for this configuration here.
ipv6 - (Optional) Specify the IPv6 address used for the display. **<ipv6addr>** - (Optional) Enter the IPv6 address used for this configuration here.

Restrictions

None.

Example

To display management address information:

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

48-9 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) Enter 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-3000-28SC: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-3000-28SC:admin#
```

48-10 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) Enter a range of ports to be configured. When port list is not specified, information for all ports will be displayed.
mode - (Optional) Specify the display mode. **brief** - Display the information in brief mode. **normal** - Display the information in normal mode. This is the default display mode. **detailed** - Display the information in detailed mode.

Restrictions

None.

Example

To display outbound LLDP advertisements for port 1 in detailed mode. Port description on the display should use the same value as ifDescr.

```
DGS-3000-28SC: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-3000-28SC R5.00.020
                                            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-3000-28SC: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-3000-28SC R5.00.020
                                           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-3000-28SC:admin#
```

To display outbound LLDP advertisements for port 1 in brief mode:

```
DGS-3000-28SC: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-3000-28SC R5.00.020
                                           Port 1

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

48-11 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) Enter a range of ports to be configured. When port list is not specified, information for all ports will be displayed.
mode - (Optional) Specify to display the information in various modes.

brief - Display the information in brief mode.
normal - Display the information in normal mode. This is the default display mode.
detailed - Display the information in detailed mode.

Restrictions

None.

Example

To display remote table in brief mode:

```
DGS-3000-28SC: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-3000-28SC R5.00.020
                                                  Port 3

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

To display remote table in normal mode:

```
DGS-3000-28SC: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-3000-28SC R5.00.020
                                                  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-3000-28SC:admin#
```

To display remote table in detailed mode:

```
DGS-3000-28SC: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-3000-28SC R5.00.020
                                                  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-3000-28SC:admin#
```

48-12 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-3000-28SC: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-3000-28SC:admin#
```

48-13 show lldp statistics ports

Description

This command is used to display per-port LLDP statistics

Format

show lldp statistics ports {<portlist>}

Parameters

<portlist> - (Optional) Enter a range of ports to be configured. When port list is not specified, information for all ports will be displayed.
If no parameter is specified, information for all ports will be displayed.

Restrictions

None.

Example

To display statistics information of port 1:

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

Chapter 49 LLDP-MED Command List

config lldp_med fast_start repeat_count <value 1-10>
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]
config lldp_med log state [enable | disable]
show lldp_med
show lldp_med ports {<portlist>}
show lldp_med local_ports {<portlist>
show lldp_med remote_ports {<portlist>}}

49-1 config lldp_med fast_start repeat_count

Description

This command is used to configure the fast start repeat count. When an LLDP-MED Capabilities TLV is detected for an MSAP identifier not associated with an existing LLDP remote system MIB, the application layer shall start the fast start mechanism and set the 'medFastStart' timer to 'medFastStartRepeatCount' times 1.

Format

config lldp_med fast_start repeat_count <value 1-10>

Parameters

<value 1-10> - Enter a fast start repeat count value between 1 and 10. The default value is 4.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure a LLDP-MED fast start repeat count of 5:

```
DGS-3000-28SC:admin#config lldp_med fast_start repeat_count 5
Command: config lldp_med fast_start repeat_count 5

Success.

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

49-2 config lldp_med notification topo_change ports

Description

This command is used to enable or disable the topology change notification.

Format

config lldp_med notification topo_change ports [<portlist> | all] state [enable | disable]

Parameters

<portlist> - Enter a range of ports to be configured.
all - Specify all ports in the system.
state - Specify to enables or disables the SNMP trap notification of topology change detected. **enable** - Specify to enable the SNMP trap state. **disable** - Specify to disable the SNMP trap state.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable topology change notification on all ports:

```
DGS-3000-28SC:admin# config lldp_med notification topo_change ports all state
enable
Command: config lldp_med notification topo_change ports all state enable

Success.

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

49-3 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> - Specify a range of ports to be configured.
all - Specify to set all ports in the system.
med_transit_capabilities - Select to send the LLDP-MED TLV capabilities specified. **all** - Select to send capabilities, network policy, and inventory. **capabilities** - Specify 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** - Specify that the LLDP agent should transmit "LLDP-MED network policy TLV."

power_pse - Specify that the LLDP agent should transmit 'LLDP-MED extended Power via MDI TLV' if the local device is a PSE device. **inventory** - Specify that the LLDP agent should transmit “LLDP-MED inventory TLV.”
state - Enable or disable the transmitting of LLDP-MED TLVs. **enable** - Enable the transmitting of LLDP-MED TLVs. **disable** - Disable 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-3000-28SC: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-3000-28SC:admin#
```

49-4 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-3000-28SC:admin#config lldp_med log state enable
Command: config lldp_med log state enable

Success.

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

49-5 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-3000-28SC:admin# show lldp_med
Command: show lldp_med

LLDP-MED System Information:
    Device Class              : Network Connectivity Device
    Hardware Revision         : A1
    Firmware Revision         : 5.00.003
    Software Revision         : 5.00.020
    Serial Number             :
    Manufacturer Name         : D-Link
    Model Name                : DGS-3000-28SC Gigabit Ethernet Switch
    Asset ID                  :

LLDP-MED Configuration:
    Fast Start Repeat Count   : 4

LLDP-MED Log State:Disabled

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

49-6 show lldp_med ports

Description

This command is used to display LLDP-MED per port configuration for advertisement options.

Format

show lldp_med ports {<portlist>}

Parameters

<portlist> - (Optional) Enter a range of ports to be displayed.
If no parameter is specified, information for all ports will be displayed.

Restrictions

None.

Example

To display LLDP-MED configuration information for port 1:

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

49-7 show lldp_med local_ports

Description

This command is used to display the per-port LLDP-MED information currently available for populating outbound LLDP-MED advertisements.

Format

show lldp_med local_ports {<portlist>}

Parameters

<portlist> - (Optional) Enter a range of ports to be displayed.
If no parameter is specified, information for all ports will be displayed.

Restrictions

None.

Example

To display LLDP-MED information currently available for populating outbound LLDP-MED advertisements for port 1:

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

49-8 show lldp_med remote_ports

Description

This command is used to display LLDP-MED information learned from neighbors.

Format

show lldp_med remote_ports {<portlist>}

Parameters

<portlist> - (Optional) Enter a range of ports to be displayed.
If no parameter is specified, information for all ports will be displayed.

Restrictions

None.

Example

To display remote entry information:

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

Chapter 50 Local Loop Back (LLB) Command List

config local_loopback ports [<portlist> | all] [mac | phy {medium_type [copper | fiber]}] [internal | external] [enable | disable]
show local_loopback ports [<portlist> | all]

50-1 config local_loopback ports

Description

This command is used to start/stop internal loopback tests on the selected ports; or to set to /to recover from external loopback mode.

Format

config local_loopback ports [<portlist> | all] [mac | phy {medium_type [copper | fiber]}] [internal | external] [enable | disable]

Parameters

<portlist> - Enter a range of ports to be configured.
all - Specify to set all ports in the system.
mac - Specify the mac on which the loopback is performed.
phy - Specify the layer on which the loopback is performed. **medium_type** - Specify the medium on which the loopback test is taken on the combo ports. If it's not specified, by default, the loopback test will be performed on copper. **copper** - Specify copper as the loopback test medium. **fiber** - Specify fiber as the loopback test medium.
internal - Specify the local loopback mode as internal.
external - Specify the local loopback mode as external.
enable - Enables for internal loopback, start loopback test; for external loopback, set port(s) to external loopback mode.
disable - Disables for internal loopback, stop loopback test; for external loopback, recover.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable loopback tests:

```
DGS-3000-28SC:admin# config local_loopback ports 1 phy medium_type fiber
internal enable
Command: config local_loopback ports 1 phy medium_type fiber internal enable

Success.

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

To disable loopback tests:

```
DGS-3000-28SC:admin# config local_loopback ports 1 phy medium_type fiber
internal disable
Command: config local_loopback ports 1 phy medium_type fiber internal disable

Port     64 Bytes     512 Bytes     1024 Bytes     1536 Bytes
           TX   RX         TX   RX         TX   RX          TX   RX
-----   ---- ----    ---- ----     ---- ----      ---- ----
1       100   100     100   100      100   100       100   100

Loopback Test Result : Success

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

50-2 show local_loopback ports

Description

This command is used to show Local Loopback configuration.

Format

show local_loopback ports [<portlist> | all]

Parameters

<portlist> - Enter the port to display the local loopback
all - Specify all the ports to be displayed.

Restrictions

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

Example

To display the local_loopback global setting of ports 1-6.

```
DGS-3000-28SC:admin# show local_loopback ports 1-6
Command: show local_loopback ports 1-6

 Port      Loopback Mode
-----    ---------------------
1         Internal  PHY
2         External  MAC
3         Internal  MAC
4         External  PHY Fiber
5         External  PHY Copper
6         Disable

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

Chapter 51 Loop Back Detection (LBD) Command List

config loopdetect {recover_timer [0 | <sec 60-1000000>] | interval <sec 1-32767> | mode [port-based | vlan-based]}(1)
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 vlan [<vid_list> | all] state [enable | disable]
config loopdetect log state [enable | disable]
config loopdetect action [shutdown | none]

51-1 config loopdetect

Description

This command is used to setup the loop-back detection function (LBD) for the entire Switch.

Format

config loopdetect {recover_timer [0 | <sec 60-1000000>] | interval <sec 1-32767> | mode [port-based | vlan-based]}(1)

Parameters

recover_timer - 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 Specify 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. **0** - Enter 0 to specify 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 - 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 - Specify 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** - Specify that the loop-detection operation mode will be set to port-based mode. **vlan-based** - Specify 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-3000-28SC:admin#config loopdetect recover_timer 0 interval 20 mode vlan-
based
Command: config loopdetect recover_timer 0 interval 20 mode vlan-based

Success.

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

51-2 config loopdetect ports

Description

This command is used to setup the loop-back detection function for the interfaces on the Switch.

Format

config loopdetect ports [<portlist> | all] state [enable | disable]

Parameters

<portlist> - Enter a list of ports
all - Specify to set all ports in the system.
state - Specify whether the LBD function should be enabled or disabled on the ports specified in the port list. The default state is disabled. **enable** - Specify to enable the LBD function. **disable** - Specify 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-3000-28SC:admin#config loopdetect ports 1-5 state enable
Command: config loopdetect ports 1-5 state enable

Success.

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

51-3 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-3000-28SC:admin#enable loopdetect
Command: enable loopdetect

Success.

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

51-4 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-3000-28SC:admin#disable loopdetect
Command: disable loopdetect

Success.

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

51-5 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-3000-28SC:admin#show loopdetect
Command: show loopdetect

LBD Global Settings
---------------------------
Status : Disabled
Mode : Port-based
Interval : 10 sec
Recover Time : 60 sec
Trap State : None
Enabled VLANs  : 1-4094
Log State : Enabled
Action Mode : None
Function Version : 4.06

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

51-6 show loopdetect ports

Description

This command is used to display the LBD per-port configuration.

Format

show loopdetect ports {<portlist>}

Parameters

<portlist> - (Optional) 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-3000-28SC: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-3000-28SC:admin#
```

51-7 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-3000-28SC:admin#config loopdetect trap both
Command: config loopdetect trap both

Success.

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

51-8 config loopdetect vlan

Description

This command is used configure the loop-back detection function for the VLANs on vlan-based mode.

Format

config loopdetect vlan [<vid_list> | all] state [enable | disable]

Parameters

vid - Specify the loop-back detection function. **<vid_list>** - Specify the range of VLANs that LBD will be configured on.
all - Specify to set all VLANs in the system, you may use the “all” parameters.
state - Specify whether the LBD function should be enabled or disabled on the VLANs specified in the vlan id list. The default state is enabled. **enable** - Specify to enable the LBD function. **disable** - Specify to disable the LBD function.

Restrictions

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

Example

To enable the LBD function on VLAN 2-5:

```
DGS-3000-28SC:admin# config loopdetect vlan 2-5 state enable
Command: config loopdetect vlan 2-5 state enable

Success.

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

51-9 config loopdetect log

Description

This command is used to configure the log state for LBD. The default value is enabled.

Format

config loopdetect log state [enable | disable]

Parameters

enable - Specify to enable the LBD log feature.
disable - Specify to disable the LBD log feature. All LBD-related logs will not be recorded.

Restrictions

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

Example

To enable the log state for LBD:

```
DGS-3000-28SC:admin#config loopdetect log state enable
Command: config loopdetect log state enable

Success.

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

51-10 config loopdetect action

Description

This command is used to configure the loop-back detection function action mode.

Format

config loopdetect action [shutdown | none]

Parameters

shutdown - Specify the loop has been detected, the port will be shut down (disabled) in port-based mode, the traffic will be block on specific VLAN in VLAN-based mode. This is the default value.
none - Specify the loop has been detected, the port will NOT be disabled in port-based mode, the traffic will NOT be block on specific VLAN in VLAN-based mode. Just send log and trap.

Restrictions

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

Example

To configure the LBD action mode to none:

```
DGS-3000-28SC:admin# config loopdetect action none
Command: config loopdetect action none

Success.

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

Chapter 52 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>}

52-1 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-3000-28SC:admin#enable mac_notification
Command: enable mac_notification

Success.

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

52-2 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-3000-28SC:admin#disable mac_notification
Command: disable mac_notification

Success.

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

52-3 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) Specify 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) Specify 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-3000-28SC:admin#config mac_notification interval 1 historysize 500
Command: config mac_notification interval 1 historysize 500

Success.

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

52-4 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 - Specify 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-3000-28SC:admin#config mac_notification ports 7 enable
Command: config mac_notification ports 7 enable

Success.

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

52-5 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-3000-28SC:admin#show mac_notification
Command: show mac_notification

Global MAC Notification Settings

State        : Disabled
Interval     : 1
History Size : 1

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

52-6 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-3000-28SC: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 53 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 password_type [manual_string | client_mac_address]
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]

53-1 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-3000-28SC:admin#enable mac_based_access_control
Command: enable mac_based_access_control

Success.

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

53-2 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-3000-28SC:admin#disable mac_based_access_control
Command: disable mac_based_access_control

Success.

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

53-3 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

<passwd 16> - Enter the password used here. In the RADIUS mode, the Switch will communicate with the RADIUS server using this password. The maximum length of the key is 16. The default password is “default”.

Restrictions

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

Example

To set the MAC-based Access Control password:

```
DGS-3000-28SC:admin#config mac_based_access_control password switch
Command: config mac_based_access_control password switch

Success.

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

53-4 config mac_based_access_control password_type

Description

This command is used to chose the password type used for authentication via the RADIUS server.

Format

config mac_based_access_control password_type [manual_string | client_mac_address]

Parameters

manual_string - Use the same password for all clients to communicate with the RADIUS server.
client_mac_address - Use the client’s MAC address as the password to communicate with the RADIUS server.

Restrictions

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

Example

To configure the MAC-based Access Control using client’s MAC address as authentication password:

```
DGS-3000-28SC:admin#config mac_based_access_control password_type
client_mac_address
Command: config mac_based_access_control password_type client_mac_address

Success.

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

53-5 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 - Specify to authenticate via the local database.
radius - Specify 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-3000-28SC:admin#config mac_based_access_control method local
Command: config mac_based_access_control method local

Success.

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

53-6 config mac_based_access_control guest_vlan ports

Description

This command is used to assign a specified port list to the MAC-based Access Control guest VLAN. Ports that are not contained in port list will be removed from the MAC-based Access Control guest VLAN.

For detailed information on the operation of MAC-based Access Control guest VLANs, please see the description for the “config mac_based_access_control ports” command.

Format

config mac_based_access_control guest_vlan ports <portlist>

Parameters

<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-3000-28SC:admin#config mac_based_access_control guest_vlan ports 1-8
Command: config mac_based_access_control guest_vlan ports 1-8

Success.

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

53-7 config mac_based_access_control ports

Description

This command is used to configure MAC-based Access Control port's setting.

When the MAC-based Access Control function is enabled for a port and the port is not a MAC-based Access Control guest VLAN member, the user who is attached to this port will not be forwarded unless the user passes the authentication.

- A user that does not pass the authentication will not be serviced by the Switch.
- If the user passes the authentication, the user will be able to forward traffic operated under the assigned VLAN.

When the MAC-based Access Control function is enabled for a port, and the port is a MAC-based Access Control guest VLAN member, the port(s) will be removed from the original VLAN(s) member ports, and added to MAC-based Access Control guest VLAN member ports.

- Before the authentication process starts, the user is able to forward traffic under the guest VLAN.
- After the authentication process, the user will be able to access the assigned VLAN.

If the port authorize mode is port based mode, when the port has been moved to the authorized VLAN, the subsequent users will not be authenticated again. They will operate in the current authorized VLAN.

If the port authorize mode is host based mode, then each user will be authorized individually and be capable of getting its own assigned VLAN.

If port's block time is set to" infinite", it means that a failed authentication client will never be blocked. Block time will be set to "0".

Format

config mac_based_access_control ports [<portlist> | all] {state [enable | disable] | mode [port_based | host_based] | aging_time [infinite | <min 1-1440>] | block_time <sec 0-300> | max_users [<value 1-1000> | no_limit]}(1)

Parameters

<portlist> - Enter the list of port used for this configuration here.
all - Specify all existed ports of switch for configuring the MAC-based Access Control function parameters.
state - Specify whether the port's MAC-based Access Control function is enabled or disabled. **enable** - Specify that the port's MAC-based Access Control states will be enabled. **disable** - Specify that the port's MAC-based Access Control states will be disabled.
mode - Specify the MAC-based access control port mode used. **port_based** - Specify that the MAC-based access control port mode will be set to port-based. **host_based** - Specify that the MAC-based access control port mode will be set to host-based.
aging_time - 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** - Specify 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 - 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 - Specify 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** - Specify 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-3000-28SC: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-3000-28SC: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-3000-28SC: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-3000-28SC:admin#
```

53-8 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 - Specify 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 - Specify 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-3000-28SC:admin#create mac_based_access_control guest_vlan VLAN8
Command: create mac_based_access_control guest_vlan VLAN8

Success.

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

53-9 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 - Specify 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 - Specify 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-3000-28SC:admin#delete mac_based_access_control guest_vlan default
Command: delete mac_based_access_control guest_vlan default

Success.

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

53-10 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 - Specify the port range to delete MAC addresses on them. **all** - Specify 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 - Specify 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-3000-28SC:admin#clear mac_based_access_control auth_state ports all
Command: clear mac_based_access_control auth_state ports all

Success.

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

53-11 create mac_based_access_control_local mac

Description

This command is used to create a MAC-based Access Control local database entry that will be used for authentication. This command can also specify the VLAN that an authorized host will be assigned to.

Format

create mac_based_access_control_local mac <macaddr> {[vlan <vlan_name 32> | vlanid < vlanid 1-4094>]}

Parameters

<macaddr> - Enter the MAC address that can pass local authentication here.
vlan - (Optional) Specify 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) Specify the target VLAN by using the VID. When this host is authorized, it will be assigned to this VLAN if the target VLAN exists. **<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-3000-28SC: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-3000-28SC:admin#
```

53-12 config mac_based_access_control_local mac

Description

This command is used to configure a MAC-based Access Control local database entry.

Format

config mac_based_access_control_local mac <macaddr> [vlan <vlan_name 32> | vlanid <vlanid 1-4094> | clear_vlan]

Parameters

<macaddr> - Enter the authenticated host’s MAC address used here.
vlan - Specify 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 - Specify 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 00-00-00-00-00-01:

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

53-13 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-3000-28SC: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-3000-28SC:admin#
```

To delete the MAC-based Access Control local database entry for the VLAN name VLAN3:

```
DGS-3000-28SC:admin#delete mac_based_access_control_local vlan VLAN3
Command: delete mac_based_access_control_local vlan VLAN3

Success.

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

53-14 config mac_based_access_control authorization attributes

Description

This command is used to enable or disable the acceptation of an authorized configuration.

When authorization is enabled for MAC-based Access Controls with RADIUS authentication, the authorized attributes (for example VLAN, 802.1p default priority, and ACL) assigned by the RADUIS server will be accepted if the global authorization status is enabled.

When authorization is enabled for MAC-based Access Controls with local authentication, the authorized attributes assigned by the local database will be accepted.

Format

config mac_based_access_control authorization attributes {radius [enable | disable] | local [enable | disable]}(1)

Parameters

radius - (Optional) If specified to enable, the authorized attributes (for example VLAN, 802.1p default priority, and ACL) assigned by the RADUIS server will be accepted if the global authorization status is enabled. The default state is enabled. **enable** - Specify that the RADIUS attributes will be enabled. **disable** - Specify 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** - Specify that the local attributes will be enabled. **disable** - Specify 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-3000-28SC:admin#config mac_based_access_control authorization attributes
local disable
Command: config mac_based_access_control authorization attributes local disable

Success.

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

53-15 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-3000-28SC:admin#show mac_based_access_control ports 1-4
Command: show mac_based_access_control ports 1-4


Port    State     Aging Time   Block Time  Auth Mode    Max User
                    (min)        (sec)
-----  --------   ----------   ---------   ----------   --------
1      Disabled   1440         300         Host-based   128
2      Disabled   1440         300         Host-based   128
3      Disabled   1440         300         Host-based   128
4      Disabled   1440         300         Host-based   128

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

53-16 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 no parameter is specified, all MAC-based Access Control local database entries will be displayed.

Restrictions

None.

Example

To show MAC-based Access Control local database for the VLAN called 'default':

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

53-17 show mac_based_access_control auth_state ports

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

<portlist> - (Optional) Enter the list of port used for this configuration here.
If no parameter is specified, all of MAC-based Access Control ports authentication status will be displayed.

Restrictions

None.

Example

To display the MAC-based Access Control authentication status on port 1-4

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

53-18 config mac_based_access_control max_users

Description

This command is used to configure the maximum number of authorized clients.

Format

config mac_based_access_control max_users [<value 1-1000> | no_limit]

Parameters

<value 1-1000> - Enter the maximum number of authorized clients on the whole device here. This value must be between 1 and 1000.	
no_limit - Specify to not limit the maximum number of users on the system. By default, there is no limit on the number of users.	

Restrictions

Only 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-3000-28SC:admin#config mac_based_access_control max_users 128
Command: config mac_based_access_control max_users 128

Success.

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

53-19 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 - Specify to enable trap for MAC-based Access Control. The trap of MAC-based Access Control will be sent out.
disable - Specify to disable 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-3000-28SC:admin#config mac_based_access_control trap state enable
Command: config mac_based_access_control trap state enable

Success.

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

53-20 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 - Specify to enable log for MAC-based Access Control. The log of MAC-based Access Control will be generated.
disable - Specify to disable 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-3000-28SC:admin#config mac_based_access_control log state disable
Command: config mac_based_access_control log state disable

Success.

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

Chapter 54 MAC-based VLAN Command List

create mac_based_vlan mac_address <macaddr> {mask <macaddr>} [vlan <vlan_name 32> | vlanid <vlanid 1-4094>] {priority <value 0-7>}
delete mac_based_vlan {mac_address <macaddr> {mask <macaddr>} [vlan <vlan_name 32> | vlanid <vlanid 1-4094>]}
show mac_based_vlan {mac_address <macaddr> | [vlan <vlan_name 32> | vlanid <vlanid 1-4094>]}
show mac_based_vlan configuration {mac_address <macaddr> {mask <macaddr>} | [vlan <vlan_name 32> | vlanid <vlanid 1-4094>]}

54-1 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> {mask <macaddr>} [vlan <vlan_name 32> | vlanid <vlanid 1-4094>] {priority <value 0-7>}

Parameters

<macaddr> - Enter the MAC address here.
mask - (Optional) Specify the MAC address mask. If not specified, use FF-FF-FF-FF-FF-FF. **<macaddr>** - Enter the MAC address mask 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 - Specify the VLAN by VLAN ID. **<vlanid 1-4094>** - Enter the VLAN ID here. This value must be between 1 and 4094.
priority - (Optional) Specifies the priority assigned to the untagged packets. If unspecified, the priority is default value 0. **<value 0-7>** - Enter a value between 0 to 7.

Restrictions

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

Example

To create a static MAC-based VLAN entry:

```
DGS-3000-28SC:admin#create mac_based_vlan mac_address 00-11-22-33-44-55 vlanid
100
Command: create mac_based_vlan mac_address 00-11-22-33-44-55 vlanid 100

Success.

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

To create a static MAC-based VLAN entry with mask:

```
DGS-3000-28SC:admin# create mac_based_vlan mac_address 00-00-22-33-44-55 mask
00-00-FF-FF-FF-FF vlanid 100 priority 4
Command: create mac_based_vlan mac_address 00-00-22-33-44-55 mask 00-00-FF-FF-
FF-FF vlanid 100 priority 4

Success.

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

54-2 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> {mask <macaddr>} [vlan <vlan_name 32> | vlanid <vlanid 1-4094>]}

Parameters

mac_address - (Optional) Specify the MAC address used.
- **<macaddr>** - Enter the MAC address used here.
- **mask** - (Optional) Specify the mask MAC address to be deleted. If unspecified, use FF-FF-FF-FF-FF-FF.
  - **<macaddr>** - Enter the mask MAC address to be deleted.
- **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** - Specify 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-3000-28SC: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-3000-28SC:admin#
```

54-3 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) Specify the entry that you would like to display. **<macaddr>** - Enter the MAC address used here.
vlan - (Optional) Specify 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) Specify 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-3000-28SC: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-3000-28SC:admin#
```

54-4 show mac_based_vlan configuration

Description

This command is used to display the MAC-based VLAN configuration.

Format

show mac_based_vlan {mac_address <macaddr> {mask <macaddr>} | [vlan <vlan_name 32> | vlanid <vlanid 1-4094>]}

Parameters

mac_address - (Optional) Specify the entry that you would like to display. **<macaddr>** - Enter the MAC address used here. **mask** - (Optional) Specify the MAC mask. If unspecified, display the specified MAC address mask configuration using FF-FF-FF-FF-FF-FF. **<macaddr>** - Enter the MAC mask address here.
vlan - (Optional) Specify 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) Specify the VLAN by VLAN ID. **<vlanid 1-4094>** - Enter the VLAN ID here. This value must be between 1 and 4094.

Restrictions

None.

Example

To display the MAC-based VLAN configuration:

```
DGS-3000-28SC: show mac_based_vlan configuration

    MAC Address           MAC Mask          VLAN ID   Priority
-----------------     -----------------     -------   --------
00-80-e0-14-a7-57     FF-FF-FF-FF-FF-FF     200       3
00-80-c2-33-c3-45     FF-FF-FF-FF-FF-FF     300       0
00-80-c2-33-c3-45     FF-FF-FF-FF-FF-FF     400       5
00-00-00-17-32-98     00-00-00-FF-FF-FF     400       0
00-11-a2-b3-13-25     00-FF-FF-FF-FF-FF     500       4

Total Entries : 5

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

Chapter 55 Mirror Command List

config mirror port <port> {[add | delete] source ports <portlist> [rx | tx | both]}
enable mirror
disable mirror
show mirror {group_id <value 1-4>}
create mirror group_id <value 1-4>
config mirror group_id <value 1-4> {target_port <port> | [add | delete] source ports <portlist> [rx | tx | both] | state [enable | disable]} (1)
delete mirror group_id <value 1-4>

55-1 config mirror port

Description

This command is used to configure a mirror port − source port pair primarily on the switch which only supports single mirror group. To support multiple configured mirror groups, configure group 1. If group 1 does not exist, this command will create it firstly and then configure it. 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 the target port to study the traffic crossing the source port in a completely unobtrusive manner.

Format

config mirror port <port> {[add | delete] source ports <portlist> [rx | tx | both]}

Parameters

<port> - Enter the port that will receive the packets duplicated at the mirror port.
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-3000-28SC:admin#config mirror port 1:3 add source ports 1:7-1:12 both
Command: config mirror port 1:3 add source ports 1:7-1:12 both

Success.

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

55-2 enable mirror

Description

This command is used to enable mirror function without having to modify the mirror group configuration.

Format

enable mirror

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable mirroring function:

```
DGS-3000-28SC:admin#enable mirror
Command: enable mirror

Success.

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

55-3 disable mirror

Description

This command is used to disable mirror function without having to modify the mirror group configuration.

Format

disable mirror

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To disable mirroring function:

```
DGS-3000-28SC:admin#disable mirror
Command: disable mirror

Success.

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

55-4 show mirror

Description

This command is used to display the current mirror function state and mirror group configuration on the Switch.

Format

show mirror {group_id <value 1-4>}

Parameters

group_id - (Optional) Specify a mirror group ID. **<value 1-4>** - Enter a mirror group identify value.
If no parameter is specifies, configurations for all mirror groups will be displayed

Restrictions

Only Administrators and Operators can issue this command.

Example

To display mirroring configuration:

```
DGS-3000-28SC:admin# show mirror
Command: show mirror

 Mirror Global State: Enabled

 Group ID       : 1
 State          : Enabled
 Target Port    : 1:10
 Source Ports
     RX         : 1:11-1:14
     TX         : 1:11-1:14

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

55-5 create mirror group_id

Description

This command is used to create a mirror group by entering the group ID.

Format

create mirror group_id <value 1-4>

Parameters

<value 1-4> - Enter the mirror group ID here. This value must be between 1 and 4.

Restrictions

Only Administrators and Operators can issue this command.

Example

To create a mirror group with the ID of 3:

```
DGS-3000-28SC:admin# create mirror group_id 3
Command: create mirror group_id 3

Success.

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

55-6 config mirror group_id

Description

This command is used to configure mirror group's parameters. It can configure mirror group's target port, state and source ports. The mirror group target port can't be a member of all mirror groups' source ports. Each mirror group's target port can be the same port. But each mirror group's source ports can't overlap.

Format

config mirror group_id <value 1-4> {target_port <port> | [add | delete] source ports <portlist> [rx | tx | both] | state [enable | disable]}(1)

Parameters

<value 1-4> - Enter a mirror group identify value.
target_port - The port that receives the packets duplicated at the mirror port. **<port>** - Specify the port.
add - Specify to add the mirror source ports. **delete** - Specify to delete mirror source ports. **source ports** - Specify the source ports of the mirror group ID. **<portlist>** - Enter a list of ports. **rx** - Only the received packets on the mirror group source ports will be mirrored to the mirror group target port. **tx** - Only the sent packets on the mirror group source ports will be mirrored to the mirror group target port. **both** - Both the received and sent packets on the mirror group source ports will be mirrored to the mirror group target port.
state - Specify the mirror group state. **enable** - Enable the mirror group function. **disable** - Disable the mirror group function.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure mirror group 3 with state enable and add source ports 1:4-1:9:

```
DGS-3000-28SC: config mirror group_id 3 state enable add source ports 1:4-1:9
both
Command: config mirror group_id 3 state enable add source ports 1:4-1:9 both

Success.

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

55-7 delete mirror group_id

Description

This command is used to delete a mirror group.

Format

delete mirror group_id <value 1-4>

Parameters

<value 1-4> - Enter a mirror group identify value.

Restrictions

Only Administrators and Operators can issue this command.

Example

To delete mirror group 3:

```
DGS-3000-28SC: delete mirror group_id 3
Command: delete mirror group_id 3

Success.

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

Chapter 56 MLD Proxy Command List

enable mld_proxy
disable mld_proxy
config mld_proxy downstream_if [add | delete] vlan [<vlan_name 32> | vlanid <vidlist>]
config mld_proxy upstream_if {vlan [<vlan_name 32> | vlanid <vlanid 1-4094>] | router_ports [add | delete] <portlist> | source_ip <ipv6addr> | unsolicited_report_interval <sec 0-25>}(1)
show mld_proxy {group}

56-1 enable mld_proxy

Description

This command is used to enable the MLD proxy on the switch.

Format

enable mld_proxy

Parameters

None.

Restrictions

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

Example

To enable the MLD proxy:

```
DGS-3000-28SC:admin#enable mld_proxy
Command: enable mld_proxy

Success.

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

56-2 disable mld_proxy

Description

This command is used to disable the MLD proxy on the switch.

Format

disable mld_proxy

Parameters

None.

Restrictions

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

Example

To disable the MLD proxy:

```
DGS-3000-28SC:admin#disable mld_proxy
Command: disable mld_proxy

Success.

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

56-3 config mld_proxy downstream_if

Description

This command configures the MLD proxy downstream interfaces. The MLD proxy plays the server role on the downstream interfaces. The downstream interface must be an MLD Snooping enabled VLAN.

Format

config mld_proxy downstream_if [add | delete] vlan [<vlan_name 32> | vlanid <vidlist>]

Parameters

add - Specify to add a downstream interface.
delete - Specify to delete a downstream interface .
vlan - Specify the VLAN by name or ID. **<vlan_name 32>** - Specify a name of VLAN which belong to the MLD proxy downstream interface. The maximum length is 32 characters. **vlanid** - Specify a list of VLAN IDs which belong to the MLD proxy downstream interface. **<vidlist>** - Specify a list of VLAN IDs which belong to the MLD proxy downstream interface.

Restrictions

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

Example

To configure the MLD Proxy's downstream interface:

```
DGS-3000-28SC:admin# config mld_proxy downstream_if add vlan vlanid 2-7
Command: config mld_proxy downstream_if add vlan vlanid 2-7

Success.

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

56-4 config mld_proxy upstream_if

Description

This command is used to configure the setting for the MLD proxy's upstream interface. The MLD proxy plays the host role on the upstream interface. It will send MLD report packets to the router port. The source IP address determines the source IP address to be encoded in the MLD protocol packet. If the router port is empty, the upstream will send the MLD protocol packet to all member ports on the upstream interface.

Format

config mld_proxy upstream_if {vlan [<vlan_name 32> | vlanid <vlanid 1-4094>] | router_ports [add | delete] <portlist> | source_ip <ipv6addr> | unsolicited_report_interval <sec 0-25>}(1)

Parameters

vlan - Specify the VLAN for the upstream interface. **<vlan_name 32>** - Specify a VLAN name between 1 and 32 characters. **vlanid** - Specify the VLAN ID for the upstream interface. **<vlanid 1-4094>** - Specify the VLAN ID between 1 and 4094.
router_ports - Specify a list of ports that are connected to multicast-enabled routers. **add** - Specify to add the router ports. **delete** - Specify to delete the router ports. **<portlist>** - Specify a range of ports to be configured.
source_ip - Specify the source IPv6 address of the upstream protocol packet. If it is not specified, zero IP address will be used as the protocol source IP address. **<ipv6addr>>** - Specify the IPv6 address.
unsolicited_report_interval - Specify the time between repetitions of the host's initial report of membership in a group. The default is 10 seconds. If set to 0, only one report packet is sent. **<sec 0-25>** - Specify the time between 0 and 25 seconds.

Restrictions

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

Example

To configure the router port of MLD proxy's upstream interface:

```
DGS-3000-28SC:admin# config mld_proxy upstream_if vlan default router_ports add
1:3

Command: config mld_proxy upstream_if vlan default router_ports add 1:3

Success.

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

56-5 show mld_proxy

Description

This command is used to display the MLD proxy's configuration or group information. The display status item means group entry is determined by whether or not the chip has been inserted.

Format

show mld_proxy {group}

Parameters

group - (Optional) Specify the group information.

Restrictions

None.

Example

To display the MLD proxy's information:

```
DGS-3000-28SC:admin#show mld_proxy
Command: show mld_proxy

 MLD Proxy Global State                 : Enabled

Upstream Interface
 VLAN ID                               : 1
 Dynamic Router Ports                  : 1:1-1:4
 Static Router Ports                   : 1:5
 Unsolicited Report Interval           : 10
 Source IP Address                     : ::

Downstream Interface
 VLAN List                             : 2-4

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

To display the MLD proxy's group information:

```
DGS-3000-28SC:admin#show mld_proxy group
Command: show mld_proxy group

Source           : NULL
Group            : FF1E::0202
Downstream VLAN  : 4
Member Ports     : 3,6
Status           : Active

Source           : FF80::200
Group            : FF1E::0202
Downstream VLAN  : 2
Member Ports     : 2,5,8
Status           : Inactive

Total Entries: 2

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

Chapter 57 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] | topology_changes_notification [ignore | process] | fast_done [enable | disable] | report_supression [enable | disable] suppression_time <sec 0-300> | 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>
config mld_snooping forward_lookup_mode [ipv6 | mac]
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 forward_lookup_mode
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 32> | 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 1-960>
clear mld_snooping data_driven_group [all | [vlan_name <vlan_name32> | 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>]

57-1 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] | topology_changes_notification [ignore | process] | fast_done [enable | disable] | report_supression [enable | disable] suppression_time <sec 0-300> | proxy_reporting {state [enable | disable] | source_ip <ipv6addr>}(1)}(1)

Parameters

vlan_name - Specify 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 - Specify the ID of the VLAN for which MLD snooping is to be configured. **<vlanid_list>** - Enter the VLAN ID list here.
all - Specify all VLANs for which MLD snooping is to be configured.
state - Enable or disable MLD snooping for the chosen VLAN. **enable** - Enter enable here to enable MLD snooping for the chosen VLAN. **disable** - Enter disable here to disable MLD snooping for the chosen VLAN.
topology_changes_notification - (Optional) Specify that MLD snooping should be aware of link-layer topology changes caused by Spanning Tree operation or not. **ignore** - Specify that MLD snooping will ignore link-layer topology changes caused by Spanning Tree operation. General queries won't be sent on the same domain of link-layer topology changes. **process** - Specify that MLD snooping will process link-layer topology changes caused by Spanning Tree operation. General queries will be sent on the same domain of link-layer topology changes.
fast_done - Enable or disable MLD snooping fast_leave function. **enable** - Enter enable here to enable MLD snooping fast_leave function. If enable, the membership is immediately removed when the system receive the MLD leave message. **disable** - Enter disable here to disable MLD snooping fast_leave function.
report_suppression - Specify that the MLD report suppression is enabled (the default), 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. **enable** - Specify to enable the MLD report suppression function. **disable** - Specify to disable the MLD report suppression function.
suppression_time - Specify the interval of suppression duplicates reports. If this time is set to zero, report suppression function can't take effect. **<sec 0-300>** - Enter the suppression duplicate intercal time in seconds. The value can be between 0 to 300.
proxy reporting - Specify MLD proxy reporting. **state** - Enable or disable the proxy reporting. **enable** - Enable the proxy reporting. **disable** - Disable the proxy reporting. **source_ip** - Specify 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-3000-28SC:admin#config mld_snooping vlan_name default state enable
Command: config mld_snooping vlan_name default state enable

Success.

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

57-2 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 - Specify 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 - Specify the ID of the VLAN for which MLD snooping querier is to be configured.
<vlanid_list> - Enter the VLAN ID list here.

all - Specify all VLANs for which MLD snooping querier is to be configured.

query_interval - Specify 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 - Specify 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.

- 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) Specify the maximum amount of time between group-specific query messages, including those sent in response to done-group messages. You

might lower this interval to reduce the amount of time it takes a router to detect the loss of the last listener of a group. 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) Specify 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-3000-28SC: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-3000-28SC:admin#
```

57-3 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.

Format

config mld_snooping mrouter_ports [vlan <vlan_name 32> | vlanid <vlanid_list>] [add | delete] <portlist>

Parameters

vlan - Specify 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 - Specify the ID of the VLAN on which the router port resides. **<vlanid_list>** - Enter the VLAN ID list here.
add - Specify to add the router ports.
delete - Specify to delete the router ports.
<portlist> - Enter a range of ports to be configured.

Restrictions

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

Example

To set up static router ports:

```
DGS-3000-28SC:admin#config mld_snooping mrouter_ports vlan default add 1-10
Command: config mld_snooping mrouter_ports vlan default add 1-10

Success.

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

57-4 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 - Specify 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 - Specify the ID of the VLAN on which the forbidden router port resides. **<vlanid_list>** - Enter the VLAN ID list here.
add - Specify to add the forbidden router ports.
delete - Specify to delete the forbidden router ports.
<portlist> - Enter a range of ports to be configured.

Restrictions

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

Example

To set up port 11 as the forbidden router port of the default VLAN:

```
DGS-3000-28SC:admin#config mld_snooping mrouter_ports_forbidden vlan default
add 11
Command: config mld_snooping mrouter_ports_forbidden vlan default add 11

Success.

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

57-5 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-3000-28SC:admin#enable mld_snooping
Command: enable mld_snooping

Success.

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

57-6 config mld_snooping forward_lookup_mode

Description

This command is used to configure MLD snooping forward lookup mode on the switch.

Format

config mld_snooping forward_lookup_mode [ipv6 | mac]

Parameters

ipv6 - Specify the IPv6 snoop forward lookup address.
mac - Specify the .mac address here.

Restrictions

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

Example

To configure MLD snooping for IPv6:

```
DGS-3000-28SC:admin#config mld_snooping forward_lookup_mode ipv6
Command: config mld_snooping forward_lookup_mode ipv6

Success.

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

57-7 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-3000-28SC:admin#disable mld_snooping
Command: disable mld_snooping

Success.

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

57-8 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) Specify 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) Specify 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-3000-28SC:admin# show mld_snooping
Command: show mld_snooping

 MLD Snooping Global State               : Disabled
 Data Driven Learning Max Entries        : 120

 VLAN Name                           : default
 Query Interval                      : 125
 Max Response Time                   : 10
 Robustness Value                    : 2
 Last Listener Query Interval        : 1
 Querier State                       : Disabled
 Querier Role                        : Non-Querier
 Querier IP                          : ::
 Querier Expiry Time                 : 0 secs
 State                               : Disabled
 Topology Changes Notification  : Process
 Fast Done                           : Disabled
 Rate Limit(pkt/sec)                 : No Limitation
 Report Suppression                  : Enabled
 Suppression Time                    : 10
 Proxy Reporting                     : Disabled
 Proxy Reporting Source IP           : ::
 Version                             : 2
 Data Driven Learning State          : Enabled
 Data Driven Learning Aged Out : Disabled
 Data Driven Group Expiry Time : 260

Total Entries: 1

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

57-9 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) Specify the name of the VLAN for which you want to view MLD snooping group information. If VLAN and ports and IP address are not specified, the system will display all current MLD snooping group information. **<vlan_name 32>** - Enter the VLAN name here. The VLAN name can be up to 32 characters long.
vlanid - (Optional) Specify 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) Specify a list of ports for which you want to view MLD snooping group information. **<portlist>** - Enter the list of port here.
<ipv6addr> - (Optional) Enter 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-3000-28SC: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-3000-28SC:admin#
```

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

57-10 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) Specify 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) Specify 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-3000-28SC: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-3000-28SC:admin#
```

57-11 show mld_snooping forward_lookup_mode

Description

This command is used to display MLD snooping forward lookup mode on the switch.

Format

show mld_snooping forward_lookup_mode

Parameters

None.

Restrictions

None.

Example

To show all MLD snooping forwarding entries located on the Switch.

```
DGS-3000-28SC:admin# show mld_snooping forward_lookup_mode
Command: show mld_snooping forward_lookup_mode

MLD snooping forward lookup mode: MAC address

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

57-12 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 - Specify 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 - Specify the ID of the VLAN on which the router port resides. **<vlanid_list>** - Enter the VLAN ID list here.
all - Specify 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-3000-28SC: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-3000-28SC:admin#
```

57-13 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 - Specify 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 - Specify the ID of the VLAN on which the static group resides. **<vlanid_list>** - Enter the VLAN ID list here.
<ipv6addr> - Enter the multicast group IPv6 address.

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-3000-28SC:admin#create mld_snooping static_group vlan default FF1E::1
Command: create mld_snooping static_group vlan default FF1E::1

Success.

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

57-14 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 - Specify 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 - Specify the ID of the VLAN on which the static group resides. **<vlanid_list>** - Enter the VLAN ID list here.
<ipv6addr> - Enter the multicast group IP address.

Restrictions

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

Example

To delete an MLD snooping static group for VLAN 1, group FF1E::1:

```
DGS-3000-28SC:admin#delete mld_snooping static_group vlan default FF1E::1
Command: delete mld_snooping static_group vlan default FF1E::1

Success.

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

57-15 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 - Specify 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 - Specify the ID of the VLAN on which the static group resides. **<vlanid_list>** - Enter the VLAN ID list here.
<ipv6addr> - Enter the multicast group IPv6 address.
add - Specify to add the member ports.
delete - Specify to delete the member ports.
<portlist> - Enter 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-3000-28SC: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-3000-28SC:admin#
```

57-16 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) Specify 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) Specify the ID of the VLAN on which the static group resides.

<vlanid_list> - Enter the VLAN ID list here.
<ipv6addr> - (Optional) Enter the multicast group IPv6 address.

Restrictions

None.

Example

To display all the MLD snooping static groups:

```
DGS-3000-28SC:admin# show mld_snooping static_group
Command: show mld_snooping static_group
VLAN ID/Name         IP Address            Static Member Ports
--------------   ------------------    ------------------------
1 / Default          FF1E ::1              9-10

Total Entries : 1

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

57-17 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 32> | vlanid <vlanid_list>] { state [enable | disable] | aged_out [enable | disable] | expiry_time <sec 1-65535>}(1)

Parameters

all - Specify that all VLANs are to be configured.
vlan_name - Specify the VLAN name to be configured. **<vlan_name 32>** - Enter the VLAN name here.
vlanid - Specify the VLAN ID to be configured. **<vlanid_list>** - Enter the VLAN ID list here.

state - Specify to enable or disable the data driven learning of MLD snooping groups. By default, the state is enabled. **enable** - Specify to enable the data driven learning state. **disable** - Specify to disable the data driven learning state.
aged_out - Specify to enable or disable the aging out of entries. By default, the state is disabled. **enable** - Specify to enable the aged out option. **disable** - Specify to disable the aged out option.
expiry_time - Specify the data driven group lifetime, in seconds. This parameter is valid only when aged_out is enabled. **<sec 1-65535>** - Enter the expiry time 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-3000-28SC:admin# config mld_snooping data_driven_learning vlan_name default
state enable
Command: config mld_snooping data_driven_learning vlan_name default state
enable

Success.

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

57-18 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 1-960>

Parameters

<value 1-960> - Enter the maximum learned entry value here. This value must be between 1 and 960. The default setting is 128.

Restrictions

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

Example

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

```
DGS-3000-28SC:admin#config mld_snooping data_driven_learning max_learned_entry
50
Command: config mld_snooping data_driven_learning max_learned_entry 50

Success.

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

57-19 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_name32> | vlanid <vlanid_list>] [<ipv6addr> | all]]

Parameters

all - Specify all VLANs to which MLD snooping groups will be deleted.
vlan_name - Specify the VLAN name. **<vlan_name32>** - Enter the VLAN name here.
vlanid - Specify the VLAN ID. **<vlanid_list>** - Enter the VLAN ID list here.
<ipv6addr> - Enter the group's IP address learned by data driven.
all - Specify 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-3000-28SC:admin#clear mld_snooping data_driven_group all
Command: clear mld_snooping data_driven_group all

Success.

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

57-20 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 - Specify a VLAN to be displayed. **<vlan_name>** - Enter the VLAN name here.
vlanid - Specify a list of VLANs to be displayed. **<vlanid_list>** - Enter the VLAN ID list here.
ports - Specify a list of ports to be displayed. **<portlist>** - Enter the list of port here.

Restrictions

None.

Example

To show MLD snooping statistics counters:

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

57-21 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-3000-28SC:admin#clear mld_snooping statistics counter
Command: clear mld_snooping statistics counter

Success.

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

57-22 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 - Specify a range of ports to be configured. **<portlist>** - Enter the range of ports to be configured here.
vlanid - Specify a range of VLANs to be configured. **<vlanid_list>** - Enter the VLAN ID list here.
<value 1-1000> - Enter a value between 1-1000 to 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 - Specify 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-3000-28SC:admin#config mld_snooping rate_limit ports 1 100
Command: config mld_snooping rate_limit ports 1 100

Success.

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

57-23 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 - Specify a list of ports. **<portlist>** - Enter the range of ports to be configured here.
vlanid - Specify 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-3000-28SC: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-3000-28SC:admin#
```

Chapter 58 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]

58-1 debug stp config ports

Description

This command is used to configure per-port STP debug level on the specified ports.

Format

debug stp config ports [<portlist> | all] [event | bpdu | state_machine | all] state [disable | brief | detail]

Parameters

<portlist> - Enter the STP port range to debug.
all - Specify to debug all ports on the Switch.
event - Specify to debug the external operation and event processing.
bpdu - Specify to debug the BPDU's that have been received and transmitted.
state_machine - Specify to debug the state change of the STP state machine.
all - Specify to debug all of the above.
state - Specify 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-3000-28SC:admin#debug stp config ports all all state brief
Command: debug stp config ports all all state brief

Success.

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

58-2 debug stp show information

Description

This command is used to display STP detailed information.

Format

debug stp show information

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To show STP debug information:

```
DGS-3000-28SC: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
```

58-3 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) Specify the STP ports to display. **<portlist>** - 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-3000-28SC: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-3000-28SC:admin#
```

58-4 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) Specify 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-3000-28SC:admin#debug stp show counter ports 9
Command: debug stp show counter ports 9

STP Counters
-------------------------------------
 Port 9    :
  Receive:                                  Transmit:
  Total STP Packets         : 0             Total STP Packets  : 0
  Configuration BPDU        : 0             Configuration BPDU : 0
  TCN BPDU                  : 0             TCN BPDU           : 0
  RSTP TC-Flag              : 0             RSTP TC-Flag       : 0
  RST BPDU                  : 0             RST BPDU           : 0

  Discard:
  Total Discarded BPDU      : 0
  Global STP Disabled       : 0
  Port STP Disabled         : 0
  Invalid packet Format     : 0
  Invalid Protocol          : 0
  Configuration BPDU Length : 0
  TCN BPDU Length           : 0
  RST BPDU Length           : 0
  Invalid Type              : 0
  Invalid Timers            : 0

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

58-5 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)Specify 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-3000-28SC:admin#debug stp clear counter ports all
Command: debug stp clear counter ports all

Success.

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

58-6 debug stp state

Description

This command is used to enable or disable the STP debug state.

Format

debug stp state [enable | disable]

Parameters

enable - Specify to enable the STP debug state.
disable - Specify to disable the STP debug state.

Restrictions

Only Administrators can issue this command.

Example

To configure the STP debug state to enable, and then disable the STP debug state:

```
DGS-3000-28SC:admin#debug stp state enable
Command: debug stp state enable

Success.

DGS-3000-28SC:admin#debug stp state disable
Command: debug stp state disable

Success.

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

Chapter 59 Multicast Filter Command List

create mcast_filter_profile {[ipv4 | ipv6]} profile_id <value 1-24> profile_name <name 32>
config mcast_filter_profile [profile_id <value 1-24> | profile_name <name32>] {profile_name <name32> | [add | delete] <mcast_address_list>}
config mcast_filter_profile ipv6 [profile_id <value 1-24> | profile_name <name32>] {profile_name <name32> | [add | delete] <mcastv6_address_list>}(1)
delete mcast_filter_profile {[ipv4 | ipv6]} [profile_id [<value 1-24> | all] | profile_name <name 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 [profile_id <value 1-24> | profile_name <name 32>] | delete [profile_id <value 1-24> | profile_name <name 32> | all]] | access [permit | deny]}(1)
config max_mcast_group [ports <portlist> | vlanid <vlanid_list>] {[ipv4 | ipv6]} {max_group [<value 1-960> | infinite] | action [drop | replace]}
show max_mcast_group [ports <portlist> | vlanid <vlanid_list>] {[ipv4 | ipv6]}
show limited_multicast_addr [ports <portlist> | vlanid <vlanid_list>] {[ipv4 | ipv6]}
config cpu_filter l3_control_pkt <portlist> [{dvmrp | pim | igmp_query} | all] state [enable | disable]
show cpu_filter l3_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]}

59-1 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 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 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-3000-28SC:admin#create mcast_filter_profile profile_id 2 profile_name MOD
Command: create mcast_filter_profile profile_id 2 profile_name MOD

Success.

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

59-2 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 32>] {profile_name <name 32> | [add | delete] <mcast_address_list>}

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 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 32>** - Enter the profile name here. The profile name can be up to 32 characters long.
add - (Optional) Specify to add a multicast address.
delete - (Optional) Specify 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-3000-28SC: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-3000-28SC:admin#
```

59-3 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 32>] {profile_name <name 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 - Specify a meaningful description for the profile. **<name 32>** - Enter the profile name here. The profile name can be up to 32 characters long.
profile_name - Specify a meaningful description for the profile. **<name 32>** - Enter the profile name here. The profile name can be up to 32 characters long.
add - Specify to add an IPv6 multicast address.
delete - Specify to delete an IPv6 multicast address.
<mcastv6_address_list> - Enter a single IPv6 multicast IP address or a range of IPv6 multicast addresses This lists the IPv6 multicast addresses to put in the profile.

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-3000-28SC:admin#config mcast_filter_profile ipv6 profile_id 3 add
FF0E::100:0:0:20– FFF0E::100:0:0:22
Command: config mcast_filter_profile ipv6 profile_id 3 add FF0E::100:0:0:20–
FFF0E::100:0:0:22

Success.

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

59-4 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 32>]

Parameters

ipv4 - (Optional) Specify to delete an IPv4 multicast profile.
ipv6 - (Optional) Specify to delete an IPv6 multicast profile.
profile_id - Specify the ID of the profile **<value 1-24>** - Enter the profile ID value here. This value must be between 1 and 24. **all** - Specify to delete all multicast filter profiles.
profile_name - Specify to display a profile based on the profile name. **<name 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-3000-28SC:admin#delete mcast_filter_profile profile_id  3
Command: delete mcast_filter_profile profile_id  3
Success.

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

To delete the multicast address profile called MOD:

```
DGS-3000-28SC:admin#delete mcast_filter_profile profile_name MOD
Command: delete mcast_filter_profile profile_name MOD

Total entries: 2

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

59-5 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) Specify to display an IPv4 multicast profile.
ipv6 - (Optional) Specify to display an IPv6 multicast profile.
profile_id - (Optional) Specify 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) Specify 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-3000-28SC: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-3000-28SC:admin#
```

59-6 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 [profile_id <value 1-24> | profile_name <name 32>] | delete [profile_id <value 1-24> | profile_name <name 32> | all]] | access [permit | deny]}(1)

Parameters

ports - Specify the range of ports to configure the multicast address filtering function.
- **<portslist>** - Enter the list of port to be configured here.

vlanid - Specify 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) Specify the IPv4 multicast profile.

ipv6 - (Optional) Specify the IPv6 multicast profile.

add - Specify to add a multicast address profile to a port.
- **profile_id** - 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** - Specify the profile name used.
  - **<name 1-32>** - Enter the profile name here. The profile name can be up to 32 characters

long.
delete - Specify to delete a multicast address profile to a port. **profile_id** - 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** - Specify the profile name used. **<name 1-32>** - Enter the profile name here. The profile name can be up to 32 characters long. **all** - Specify to delete all multicast address profile..
access - Specify the access of packets matching the addresses defined in the profiles. **permit** - Specify that packets matching the addresses defined in the profiles will be permitted. The default mode is permit. **deny** - Specify 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 1:1 and 1:3:

```
DGS-3000-28SC:admin# config limited_multicast_addr ports 1:1,1:3 add profile_id
2

Command: config limited_multicast_addr ports 1:1,1:3 add profile_id 2

Success.

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

59-7 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 1-960> | infinite] | action [drop | replace]}

Parameters

ports - Specify the range of ports to configure the max_mcast_group. **<portlist>** - Enter the list of ports to be configured here.
vlanid - Specify the VLAN ID to configure max_mcast_group. **<vlanid_list>** - Enter the VLAN ID list here.
ipv4 - (Optional) Specify that the maximum number of IPv4 learned addresses should be limited.
ipv6 - (Optional) Specify that the maximum number of IPv6 learned addresses should be limited.

max_group - (Optional) Specify the maximum number of multicast groups. **<value 1-960>** - Enter the maximum group value here. This value must be between 1 and 960. **infinite** - Specify 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) Specify 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-3000-28SC:admin#config max_mcast_group ports 1, 3 max_group 100
Command: config max_mcast_group ports 1, 3 max_group 100

Success.

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

59-8 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 - Specify 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 - Specify the VLAN ID for displaying the maximum number of multicast groups. **<vlanid_list>** - Enter the VLAN ID list here.
ipv4 - (Optional) Specify to display the maximum number of IPv4 learned addresses.
ipv6 - (Optional) Specify 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-3000-28SC: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-3000-28SC:admin#
```

To display the maximum number of multicast groups that VLANs 1 and 2 can join:

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

59-9 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 - Specify 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 - Specify 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) Specify to display the IPv4 multicast profile associated with the port.
ipv6 - (Optional) Specify 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-3000-28SC: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
---------- ------------------------------- -------------------------------
2          MOD                             225.1.1.1-225.1.1.10


Port    : 3
Access  : Permit

Profile ID Name                            Multicast Addresses
---------- ------------------------------- -------------------------------
2          MOD                             225.1.1.1-225.1.1.10


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

To show the limited multicast settings configured on VLAN 1:

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

VLAN ID : 1
Access  : Permit

Profile ID Name                            Multicast Addresses
---------- ------------------------------- -------------------------------
2          MOD                             225.1.1.1-225.1.1.10


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

59-10 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} | all] state [enable | disable]

Parameters

<portlist> - Enter the port list to filter control packets.
dvmrp – (Optional) Specify to filter the DVMRP control packets.
pim - (Optional) Specify to filter the PIM control packets.
igmp_query - (Optional) Specify to filter the IGMP query control packets.
all - Specify to filter all the L3 protocol control packets.
state - Specify 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-3000-28SC: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-3000-28SC:admin#
```

59-11 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) Enter 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-3000-28SC: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
 ----     ----------        --------     --------
  1       Disabled        Disabled    Disabled
  2       Disabled        Disabled    Disabled

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

59-12 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 - Specify IPv4 protocols.
- **igmp** - Specify that the Switch will examine the Internet Group Management Protocol (IGMP) field within each packet.
- **vrrp** - Specify that the Switch will examine the Virtual Router Redundancy Protocol (VRRP) field within each packet.
- **rip** - Specify that the Switch will examine the Routing Information Protocol (RIP) field within each packet.
- **pim** - Specify that the Switch will examine the Protocol-Independent Multicast (PIM) field within each packet.
- **dvmrp** - Specify that the Switch will examine the Distance Vector Multicast Routing Protocol (DVMRP) field within each packet.
- **ospf** - Specify that the Switch will examine the Open Shortest Path First (OSPF) field within each packet.
- **all** - Specify that the Switch will examine all above field within each packet.

ipv6 - Specify the IPv6 protocols.
- **mld** - Specify that the Switch will examine the Multicast Listener Discovery (MLD) field within each packet.
- **pim** - Specify that the Switch will examine the Protocol-Independent Multicast (PIM) field within each packet.
- **ospf** - Specify that the Switch will examine the Open Shortest Path First (OSPF) field within each packet.
- **ripng** - Specify that the Switch will examine the IP Version 6 (IPv6) Routing Information Protocol - next generation (RIPng) field within each packet.
- **nd** - Specify that the Switch will examine the IP Version 6 (IPv6) Neighbor Discovery (ND) field within each packet.
- **all** - Specify that the Switch will examine all above field within each packet.

replace - Specify to change the priority or DSCP.
- **priority** - Specify the priority value.
  - **<value 0-7>** - Enter the value between 0 and 7.
  - **none** - Specify not to change the priority.

dscp - Specify the DSCP. **<value 0-63>** - Enter the value between 0 and 63. **none** - Specify 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-3000-28SC:admin#config control_pkt ipv4 dvmrp replace priority 3
Command: config control_pkt ipv4 dvmrp replace priority 3

Success.

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

59-13 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-3000-28SC: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-3000-28SC:admin#
```

Chapter 60 Multicast VLAN Command List

enable igmp_snooping multicast_vlan
enable mld_snooping multicast_vlan
disable igmp_snooping multicast_vlan
disable mld_snooping multicast_vlan
create igmp_snooping multicast_vlan <vlan_name 32> <vlanid 2-4094> {remap_priority [<value 0-7> | none] {replace_priority}}
create igmp_snooping multicast_vlan_group_profile <profile_name 1-32>
create mld_snooping multicast_vlan <vlan_name 32> <vlanid 2-4094> {remap_priority [<value 0-7> | none] {replace_priority}}
create mld_snooping multicast_vlan_group_profile <profile_name 1-32>
config igmp_snooping multicast_vlan <vlan_name 32> {[add | delete] [member_port <portlist> | [source_port <portlist> | untag_source_port <portlist>] | tag_member_port <portlist>] | state [enable | disable] | replace_source_ip [<ipaddr> | none] | remap_priority [<value 0-7> | none] { replace_priority}}(1)
config igmp_snooping multicast_vlan auto_assign_vlan [enable | disable]
config igmp_snooping multicast_vlan_group_profile <profile_name 1-32> [add | delete] <mcast_address_list>
config igmp_snooping multicast_vlan_group <vlan_name 32> [add | delete] profile_name <profile_name 1-32>
config igmp_snooping multicast_vlan forward_unmatched [disable | enable]
config mld_snooping multicast_vlan <vlan_name32> {[add | delete] [member_port <portlist> | [source_port <portlist> | untag_source_port <portlist>] | tag_member_port <portlist>] | state [enable | disable] | replace_source_ipv6 [<ipv6addr> | none] | remap_priority [<value0-7> | none] {replace_priority}}(1)
config mld_snooping multicast_vlan_group_profile <profile_name 1-32> [add | delete] <mcastv6_address_list>
config mld_snooping multicast_vlan_group <vlan_name 32> [add | delete] profile_name <profile_name 1-32>
config mld_snooping multicast_vlan forward_unmatched [disable | enable]
config mld_snooping multicast_vlan auto_assign_vlan [enable | disable]
delete igmp_snooping multicast_vlan_group_profile [profile_name <profile_name 1-32> | all]
delete igmp_snooping multicast_vlan <vlan_name 32>
delete mld_snooping multicast_vlan_group_profile [profile_name <profile_name 1-32> | all]
delete mld_snooping multicast_vlan <vlan_name 32>
show igmp_snooping multicast_vlan_group_profile {< profile_name 1-32>}
show igmp_snooping multicast_vlan_group {<vlan_name 32>}
show igmp_snooping multicast_vlan {<vlan_name 32>}
show mld_snooping multicast_vlan_group_profile {<profile_name 1-32>}
show mld_snooping multicast_vlan_group {<vlan_name 32>}
show mld_snooping multicast_vlan {<vlan_name 32>}

60-1 enable igmp_snooping multicast_vlan

Description

This command is used to control the status of the multicast VLAN function.

Format

enable igmp_snooping multicast_vlan

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To enable the IGMP snooping multicast VLAN function globally:

```
DGS-3000-28SC:admin#enable igmp_snooping multicast_vlan
Command: enable igmp_snooping multicast_vlan

Success.

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

60-2 enable mld_snooping multicast_vlan

Description

This command is used to enable the MLD snooping multicast VLAN function. By default, the multicast VLAN is disabled.

Format

enable mld_snooping multicast_vlan

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To enable MLD snooping multicast VLAN:

```
DGS-3000-28SC:admin#enable mld_snooping multicast_vlan
Command: enable mld_snooping multicast_vlan

Success.

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

60-3 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-3000-28SC:admin#disable igmp_snooping multicast_vlan
Command: disable igmp_snooping multicast_vlan

Success.

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

60-4 disable mld_snooping multicast_vlan

Description

This command is used to disable the MLD snooping multicast VLAN function. By default, the multicast VLAN is disabled.

Format

disable mld_snooping multicast_vlan

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To disable MLD snooping multicast VLAN:

```
DGS-3000-28SC:admin#disable mld_snooping multicast_vlan
Command: disable mld_snooping multicast_vlan

Success.

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

60-5 create igmp_snooping multicast_vlan

Description

This command is used to create a multicast VLAN and implements relevant parameters as specified. More than one multicast VLANs can be configured. The maximum number of configurable VLANs is 5.

Newly created IGMP snooping multicast VLANs must use a unique VLAN ID and name, i.e. they cannot use the VLAN ID or name of any existing 802.1Q VLAN.

Also keep in mind the following conditions:

- Multicast VLANs cannot be configured or displayed using 802.1Q VLAN commands.
- An IP interface cannot be bound to a multicast VLAN.
- The multicast VLAN snooping function co-exists with the 802.1Q VLAN snooping function.

Format

create igmp_snooping multicast_vlan <vlan_name 32> <vlanid 2-4094> {remap_priority [<value 0-7> | none] {replace_priority}}

Parameters

<vlan_name 32> - Enter the multicast VLAN here. The VLAN name can be up to 32 characters long.
<vlanid 2-4094> - Enter the multicast VLAN ID 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** - Specify that the remap priority value will be set to none. **replace_priority** - (Optional) Specify that packet's priority will be changed by the Switch, based on the remap priority. This flag will only take effect when the remap priority is set.

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-3000-28SC:admin#create igmp_snoop multicast_vlan mv1 2
Command: create igmp_snoop multicast_vlan mv1 2

Success.

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

60-6 create igmp_snooping multicast_vlan_group_profile

Description

This command is used to create an IGMP snooping multicast group profile on the Switch.

Format

create igmp_snooping multicast_vlan_group_profile <profile_name 1-32>

Parameters

<profile_name 1-32> - Enter the multicast VLAN group profile name here. The name can be up to 32 characters long.

Restrictions

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

Example

To create an IGMP snooping multicast group profile with the name “test”:

```
DGS-3000-28SC:admin#create igmp_snooping multicast_vlan_group_profile test
Command: create igmp_snooping multicast_vlan_group_profile test

Success.

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

60-7 create mld_snooping multicast_vlan

Description

This command is used to create an MLD snooping multicast VLAN and implements relevant parameters as specified. More than one multicast VLAN can be configured. Newly created MLD

snooping multicast VLANs must use a unique VLAN ID and name, i.e. they cannot use the VLAN ID or name of any existing 802.1Q VLAN. Also keep in mind the following conditions: multicast VLANs cannot be configured or displayed using 802.1Q VLAN commands; an IP interface cannot be bound to a multicast VLAN; and the multicast VLAN snooping function co-exists with the 802.1Q VLAN snooping function.

Format

create mld_snooping multicast_vlan <vlan_name 32> <vlanid 2-4094> {remap_priority [<value 0-7> | none] {replace_priority}}

Parameters

<vlan_name 32> - Enter the name of the multicast VLAN to be created. Each multicast VLAN is given a name that can be up to 32 characters.
<vlanid 2-4094> - Enter the VLAN ID of the multicast VLAN to be created. The range is from 2 to 4094.
remap_priority - (Optional) Specify the remap priority here. **<value 0-7>** - Enter the remap priority (0 to 7) to be associated with the data traffic to be forwarded on the multicast VLAN. **none** - If none is specified, the packet's original priority will be used. The default setting is none. **replace_priority** - (Optional) Specify that the packet's priority will be changed by the switch, based on the remap priority. This flag will only take effect when the remap priority is set.

Restrictions

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

Example

To create an MLD snooping multicast VLAN with the VLAN name mv1 and the VID 2:

```
DGS-3000-28SC:admin#create mld_snooping multicast_vlan mv1 2
Command: create mld_snooping multicast_vlan mv1 2

Success.

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

60-8 create mld_snooping multicast_vlan_group_profile

Description

This command is used to create a multicast group profile. The profile name for MLD snooping must be unique.

Format

create mld_snooping multicast_vlan_group_profile <profile_name 1-32>

Parameters

<profile_name 1-32> - Enter the multicast VLAN profile name. The maximum length is 32 characters.

Restrictions

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

Example

To create an MLD snooping multicast group profile with the name “Knicks”:

```
DGS-3000-28SC:admin#create mld_snooping multicast_vlan_group_profile Knicks
Command: create mld_snooping multicast_vlan_group_profile Knicks

Success.

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

60-9 config igmp_snooping multicast_vlan

Description

This command is used to add member ports and source ports to a list of multicast VLAN member ports. Member ports automatically become untagged members of the multicast VLAN and source ports automatically become tagged members of the multicast VLAN. However, member ports of one multicast VLAN are allowed to overlap with member ports on a different multicast VLAN.

A multicast VLAN must first be created using the create igmp_snooping multicast_vlan command before the multicast VLAN can be configured.

Format

config igmp_snooping multicast_vlan <vlan_name 32> {[add | delete] [member_port <portlist> | [source_port <portlist> | untag_source_port <portlist>] | tag_member_port <portlist>] | state [enable | disable] | replace_source_ip [<ipaddr> | none] | remap_priority [<value 0-7> | none] { replace_priority}}(1)

Parameters

<vlan_name 32> - Enter the name of the multicast VLAN here. The VLAN name can be up to 32 characters long.
add - Specify that the entry will be added to the specified multicast VLAN.
delete - Specify that the entry will be deleted to 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 - Specify the source port or range of source ports as untagged members of the multicast VLAN. The PVID of the untagged source port is automatically changed to the multicast VLAN. Source ports must be either tagged or untagged for any single multicast VLAN, i.e. both types cannot be members of the same multicast VLAN. **<portlist>** - Enter the list of port to be configured here.

tag_member_port - Specify 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 - Used to specify if the multicast VLAN for a chosen VLAN should be enabled or disabled. **enable** - Specify to enable the multicast VLAN for a chosen VLAN. **disable** - Specify 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 none is specified, the source IP address will not be replaced. **<ipaddr>** - Enter the replace source IP address here. **none** - Specify for not replacing the source IP address.
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** - Specify that the remap priority value will be set to none.
replace_priority - (Optional) Specify that the packet priority will be changed to the remap_priority, but only if remap_priority is set.

Restrictions

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

Example

To configure an IGMP snooping multicast VLAN with the name "mv1", make ports 1 and 3 members of the VLAN, and set the state to enable:

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

60-10 config igmp_snooping multicast_vlan auto_assign_vlan

Description

This command is used to enable a new function to auto assign the IGMP control packets to the right ISM VLAN.

If the MVLAN auto_assign_vlan is disabled, the MVLAN process will be:

When an IGMP/MLD report or leave packet is received on a multicast VLAN member port, and the IGMP/MLD snooping is not enabled on the received packets' VLAN, then

a) If the packet is tagged with VLAN X:

- If VLAN X is not a MVLAN, floods this packet in VLAN X. Exit.
- Else check if the group address matches any group profile in MVLAN X. If a match is found then the result is "in profile", otherwise is "out-of-profile".

b) Else (untagged packet, first lookup all MVLANs to find the reported group belongs to)

- If found, the result is "in profile" and MVLAN will be set as the packet VLAN.
- If not found and the packet's VLAN is a MVLAN, the result is "out-of-profile".

- If not found and the packet's VLAN is not a MVLAN, this packet will be flooded in packet's VLAN. Exit.

If the MVLAN auto_assign_vlan is enabled, the MVLAN process will be:

When an IGMP/MLD report or leave packet is received on a multicast VLAN member port, and the IGMP/MLD snooping is not enabled on the received packets' VLAN, the switch will ignore the received packet VLAN and lookup all MVLANs to find the reported group belongs to.

- If found, the result is "in profile" and MVLAN will be set as the packet VLAN.
- If not found and the packet's VLAN is a MVLAN, the result is "out-of-profile".
- If not found and the packet's VLAN is not a MVLAN, this packet will be flooded in packet's VLAN. Exit.

The "in-profile" packet will be taken into the succedent group learning process, and the "out-of-profile" packet won't be learned and its forwarding action is decided by below configuration:

- "config igmp_snooping/mld_snooping multicast_vlan forward_unmatched [disable | enable]"
- Disable is discarded the IGMP/MLD packet.
- Enable is to flood IGMP/MLD packet in packet's VLAN.

Format

config igmp_snooping multicast_vlan auto-assign_vlan [enable | disable]

Parameters

enable - Specify to enable the auto assign VLAN function.
disable - Specify to disable the auto assign VLAN function.

Restrictions

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

Example

To enable the auto assign VLAN function of multicast VLAN:

```
DGS-3000-28SC:admin# config igmp_snooping multicast_vlan auto_assign_vlan
enable
Command: config igmp_snooping multicast_vlan auto_assign_vlan enable

Success.

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

60-11 config igmp_snooping multicast_vlan_group_profile

Description

This command is used to configure an IGMP snooping multicast group profile on the Switch and add or delete multicast addresses for the profile.

Format

config igmp_snooping multicast_vlan_group_profile <profile_name 1-32> [add | delete] <mcast_address_list>

Parameters

<profile_name 1-32> - Enter the multicast VLAN group name here. This name can be up to 32 characters long.
add - 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-3000-28SC: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-3000-28SC:admin#
```

60-12 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 - Specify to associate a profile to a multicast VLAN.
delete - Specify to de-associate a profile from a multicast VLAN.
profile_name - Specify 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-3000-28SC: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-3000-28SC:admin#
```

60-13 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 [disable | enable]

Parameters

disable - The packet will be dropped.
enable - The packet will be flooded on the VLAN.

Restrictions

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

Example

To configure the forwarding mode for multicast VLAN unmatched packets：

```
DGS-3000-28SC:admin#config igmp_snooping multicast_vlan forward_unmatched
enable
Command: config igmp_snooping multicast_vlan forward_unmatched enable

Success.

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

60-14 config mld_snooping multicast_vlan

Description

This command is used to configure MLD snooping multicast VLAN parameters. The member port list and source port list cannot overlap. However, the member port of one multicast VLAN can overlap with another multicast VLAN. The multicast VLAN must be created first using the **create mld_snooping multicast_vlan** command before the multicast VLAN can be configured.

Format

config mld_snooping multicast_vlan <vlan_name32> {[add | delete] [member_port <portlist> | [source_port <portlist> | untag_source_port <portlist>] | tag_member_port <portlist>] | state [enable | disable] | replace_source_ipv6 [<ipv6addr> | none] | remap_priority [<value0-7> | none] {replace_priority}}(1)

Parameters

<vlan_name 32> - Enter the name of the multicast VLAN to be configured. Each multicast VLAN is given a name that can be up to 32 characters.
add - Specify to add a port.
delete - Specify to delete a port.
member_port - Specify member port of the multicast VLAN. The specified range of ports will become untagged members of the multicast VLAN. **<portlist>** - Enter a range of ports to be configured.
source_port - Specify source port where the multicast traffic is entering the Switch. **<portlist>** - Enter a range of ports to be configured.
untag_source_port - Specify the untagged source port where the multicast traffic is entering the Switch. 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 a range of ports to be configured.
tag_member_port - Specify the tagged member port of the multicast VLAN. **<portlist>** - Enter a range of ports to be configured.
state - Specify if the multicast VLAN for a chosen VLAN should be enabled or disabled. **enable** - Enable multicast VLAN for the chosen VLAN. **disable** - Disable multicast VLAN for the chosen VLAN.
replace_source_ipv6 - With the MLD snooping function, the MLD report packet sent by the host will be forwarded to the source port. Before forwarding of the packet, the source IP address in the join packet needs to be replaced by this IP address. If none is specified, the source IP address will not be replaced. **<ipv6addr>** - Enter the IP address here. **none** - Enter none to not specify the IP address.

remap_priority - Specify the remap priority here. **<value 0-7>** - Enter a remap priority value (0 to 7) to be associated with the data traffic forwarded on the multicast VLAN. **none** - If none is specified, the packet's original priority is used. The default setting is none.
replace_priority - (Optional) Specify that the packet priority will be changed to the remap priority, when remap priority is set.

Restrictions

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

Example

To configure an MLD snooping multicast VLAN with the name "v1", make ports 1 and 3 members of the VLAN, and set the state to enable:

```
DGS-3000-28SC:admin#config mld_snooping multicast_vlan v1 add member_port 1,3
state enable
Command: config mld_snooping multicast_vlan v1 add member_port 1,3 state enable

Success.

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

60-15 config mld_snooping multicast_vlan_group_profile

Description

This command is used to configure an MLD snooping multicast group profile on the switch.

Format

config mld_snooping multicast_vlan_group_profile <profile_name 1-32> [add | delete] <mcastv6_address_list>

Parameters

<profile_name 32> - Enter the multicast VLAN profile name. The maximum length is 32 characters.
add - Specify to add a multicast address list to this multicast VLAN profile.
delete - Specify to delete a multicast address list from this multicast VLAN profile.
<mcastv6_address_list> - Enter a multicast address list. This can be a continuous single multicast address, such as FF1E::1, FF1E::2, a multicast address range, such as FF1E::3-FF1E::9, or both types, such as FF1E::11, FF1E::12-FF1E::20.

Restrictions

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

Example

To add the single multicast address FF1E::11 and multicast range FF1E::12-FF1E::20 to the MLD snooping multicast VLAN profile named "Knicks":

```
DGS-3000-28SC:admin#config mld_snooping multicast_vlan_group_profile Knicks add
FF1E::11, FF1E::12-FF1E::20
Command: config mld_snooping multicast_vlan_group_profile Knicks add FF1E::11,
FF1E::12-FF1E::20

Success.

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

60-16 config mld_snooping multicast_vlan_group

Description

This command is used to configure the multicast group which is used with the specific multicast VLAN. The following two cases can be considered as examples:

Case 1 - The multicast group is not configured, multicast VLANs do not have any member ports overlapping and the packets that are received by the member port is used only by the multicast VLAN that this port is a member of.

Case 2 - The packets are used with the multicast VLAN which contains the destination multicast group. If the destination multicast group of the added packets cannot be classified into any multicast VLAN (to which this port belongs), then the added packets will be used on the natural VLAN of the packet.

Note: A profile cannot overlap in different multicast VLANs. Multiple profiles can be added to a multicast VLAN.

Format

config mld_snooping multicast_vlan_group <vlan_name 32> [add | delete] profile_name <profile_name 1-32>

Parameters

<vlan_name 32> - Enter the name of the multicast VLAN to be configured, each multicast VLAN is given a name that can be up to 32 characters.
add - Specify to be used to associate a profile to a multicast VLAN.
delete - Specify to de-associate a profile from a multicast VLAN.
profile_name – Specify to add a multicast VLAN profile name. **<profile_name 1-32>** - The name of the MLD multicast VLAN group profile to be associated or de- associated to the specified multicast VLAN.

Restrictions

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

Example

To configure the forwarding mode for MLD snooping multicast VLAN unmatched packets:

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

60-17 config mld_snooping multicast_vlan forward_unmatched

Description

This command is used to configure the forwarding mode for MLD snooping multicast VLAN unmatched packets. When the switch receives an MLD snooping packet, it will match the packet against the multicast profile to determine which multicast VLAN to associate with. If the packet does not match all profiles, the packet will be forwarded in the natural VLAN of the packet, or dropped based on this setting. By default, the packet will be dropped.

Format

config mld_snooping multicast_vlan forward_unmatched [disable | enable]

Parameters

disable - The packet will be dropped.
enable - The packet will be flooded on the VLAN.

Restrictions

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

Example

To configure the forwarding mode for MLD snooping multicast VLAN unmatched packets:

```
DGS-3000-28SC:admin#config mld_snooping multicast_vlan forward_unmatched enable
Command: config mld_snooping multicast_vlan forward_unmatched enable

Success.

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

60-18 config mld_snooping multicast_vlan auto_assign_vlan

Description

This command is used to configure whether to enable auto assign VLAN function.

Format

config mld_snooping multicast_vlan auto_assign_vlan [enable | disable]

Parameters

enable - Specify this parameter to enable auto assign VLAN function.
disable - Specify this parameter to disable auto assign VLAN function.

Restrictions

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

Example

To configure the auto_assign_vlan to enable for MLD snooping multicast VLAN:

```
DGS-3000-28SC:admin#config mld_snooping multicast_vlan auto_assign_vlan enable
Command: config mld_snooping multicast_vlan auto_assign_vlan enable

Success.

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

60-19 delete igmp_snooping multicast_vlan_group_profile

Description

This command is used to delete an IGMP snooping multicast group profile on the Switch. Specify a profile name to delete it. Specify 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 - Specify 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** - Specify 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-3000-28SC:admin#delete igmp_snooping multicast_vlan_group_profile
profile_name MOD
Command: delete igmp_snooping multicast_vlan_group_profile profile_name MOD

Success.

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

60-20 delete igmp_snooping multicast_vlan

Description

This command is used to delete an IGMP snooping multicast VLAN.

Format

delete igmp_snooping multicast_vlan <vlan_name 32>

Parameters

<vlan_name 32> -Enter the 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-3000-28SC:admin#delete igmp_snooping multicast_vlan v1
Command: delete igmp_snooping multicat_vlan v1

Success.

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

60-21 delete mld_snooping multicast_vlan_group_profile

Description

This command is used to delete an existing MLD snooping multicast group profile on the switch. Specify a profile name to delete it.

Format

delete mld_snooping multicast_vlan_group_profile [profile_name <profile_name 1-32> | all]

Parameters

profile_name - Specify the multicast VLAN group profile name. The maximum length is 32 characters. **<profile_name 1-32>** - Enter the multicast VLAN group profile name. The profile name can be up to 32 characters long.
all - Specify to delete all the profiles.

Restrictions

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

Example

To delete an MLD snooping multicast group profile named “Knicks”:

```
DGS-3000-28SC:admin#delete mld_snooping multicast_vlan_group_profile
profile_name Knicks
Command: delete mld_snooping multicast_vlan_group_profile profile_name Knicks

Success.

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

60-22 delete mld_snooping multicast_vlan

Description

This command is used to delete an MLD snooping multicast VLAN.

Format

delete mld_snooping multicast_vlan <vlan_name 32>

Parameters

<vlan_name 32> - Enter the name of the multicast deleted VLAN.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete an MLD snooping multicast VLAN called “v1”:

```
DGS-3000-28SC:admin#delete mld_snooping multicast_vlan v1
Command: delete mld_snooping multicast_vlan v1

Success.

DGS-3000-28SC:admin#
```

60-23 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-3000-28SC: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-3000-28SC:admin#
```

60-24 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-3000-28SC: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-3000-28SC:admin#
```

60-25 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-3000-28SC:admin#show igmp_snooping multicast_vlan
Command: show igmp_snooping multicast_vlan

IGMP Multicast VLAN Global State        : Disabled
IGMP Multicast VLAN Forward Unmatched   : Disabled
IGMP Multicast VLAN Auto Assign VLAN    : Disabled

VLAN Name                     :test
VID                           :100

Member(Untagged) Ports        :
Tagged Member Ports           :
Source Ports                  :
Untagged Source Ports         :
Status                        :Disabled
Replace Source IP             :Not Replaced
Remap Priority                :None


 Total Entries: 1


DGS-3000-28SC:admin#
```

60-26 show mld_snooping multicast_vlan_group_profile

Description

This command is used to display an MLD snooping multicast group profile.

Format

show mld_snooping multicast_vlan_group_profile {<profile_name 1-32>}

Parameters

<profile_name 1-32> - (Optional) Enter the multicast VLAN profile name. The maximum length is 32 characters.

Restrictions

None.

Example

To display all MLD snooping multicast VLAN profiles:

```
DGS-3000-28SC:admin#show mld_snooping multicast_vlan_group_profile
Command: show mld_snooping multicast_vlan_group_profile

Profile Name              Multicast Addresses
------------------------  --------------------------------
rock                      FF1E::1
                          FF1E::10-FF1E::20
Total Entries : 1

DGS-3000-28SC:admin#
```

60-27 show mld_snooping multicast_vlan_group

Description

This command is used to allow group profile information for a specific multicast VLAN to be displayed.

Format

show mld_snooping multicast_vlan_group {<vlan_name 32>}

Parameters

<vlan_name 32> - (Optional) Enter the name of the group profile's multicast VLAN to be displayed.

Restrictions

None.

Example

To display all MLD snooping multicast VLANs' group profile information:

```
DGS-3000-28SC:admin#show mld_snooping multicast_vlan_group
Command: show mld_snooping multicast_vlan_group


VLAN Name                       VLAN ID        Multicast Group Profiles
------------------------------  -------  --------------------------------
test2                           20

test1                           100


DGS-3000-28SC:admin#
```

60-28 show mld_snooping multicast_vlan

Description

This command is used to allow information for a specific multicast VLAN to be displayed.

Format

show mld_snooping multicast_vlan {<vlan_name 32>}

Parameters

<vlan_name 32> - (Optional) Enter the name of the multicast VLAN to be displayed.

Restrictions

None.

Example

To display all MLD snooping multicast VLANs:

```
DGS-3000-28SC:admin#show mld_snooping multicast_vlan
Command: show mld_snooping multicast_vlan

MLD Multicast VLAN Global State         : Disabled
MLD Multicast VLAN Forward Unmatched    : Disabled
MLD Multicast VLAN Auto Assign VLAN     : Disabled

VLAN Name                     :test
VID                           :100

Member(Untagged) Ports        :
Tagged Member Ports           :
Source Ports                  :
Untagged Source Ports         :
Status                        :Disabled
Replace Source IP             :Not Replaced
Remap Priority                :None


 Total Entries: 1


DGS-3000-28SC:admin#
```

Chapter 61 Multiple Spanning Tree Protocol (MSTP) Command List

enable stp
disable stp
config stp {maxage <value 6-40> | maxhops <value 6-40> | hellotime <value 1-2> | forwarddelay <value 4-30> | txholdcount <value 1-10> | fbpdu [enable | disable] | nni_bpdu_addr [dot1d | dot1ad]}
show stp
create stp instance_id <value 1-64>
config stp instance_id <value 1-64> [add_vlan | remove_vlan] <vidlist>
delete stp instance_id <value 1-64>
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 0-64> {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] | loop_guard [true | false] | fbpdu [enable | disable]}
show stp ports {<portlist>}
config stp priority <value 0-61440> instance_id <value 0-64>
config stp version [mstp | rstp | stp]
config stp trap {topo_change [disable | enable] | new_root [enable | disable]}(1)
show stp instance {<value 0-64>}
enable stp multiprocess_rstp
disable stp multiprocess_rstp
create stp multiprocess_rstp <string>
delete stp multiprocess_rstp <string>
config stp multiprocess_rstp <string> [add | delete] ports <portlist>

61-1 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-3000-28SC:admin#enable stp
Command: enable stp

Success.

DGS-3000-28SC:admin#
```

61-2 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-3000-28SC:admin#disable stp
Command: disable stp

Success.

DGS-3000-28SC:admin#
```

61-3 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) Specify 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) Specify 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) Specify 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) Specify whether the bridge will flood STP BPDU when STP functionality is disabled. **enable** - Specify that the bridge will flood STP BPDU when STP functionality is disabled **disable** - Specify that the bridge will not flood STP BPDU when STP functionality is disabled
nni_bpdu_addr – (Optional) This address is used to determine the BPDU protocol address for an STP in service provider site. It can use either an 802.1d STP address (0180C2000000) or an 802.1ad service provider STP address (0180C2000008). **dot1d** - Specify that the NNI BPDU protocol address value will be set to Dot1d. **dot1ad** - Specify 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-3000-28SC:admin#config stp maxage 25
Command: config stp maxage 25

Success.

DGS-3000-28SC:admin#
```

61-4 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-3000-28SC:admin# show stp
Command: show stp

 STP Bridge Global Settings
 --------------------------
 STP Status           : Disabled
 STP Version          : RSTP
 Max Age              : 20
 Hello Time           : 2
 Forward Delay        : 15
 Max Hops             : 20
 TX Hold Count        : 6
 Forwarding BPDU      : Disabled
 New Root Trap        : Enabled
 Topology Change Trap : Enabled
 NNI BPDU Address     : dot1d
 RSTP Multiprocess    : Disabled

        Ring Name       Ports
        -----------     -----------
        Default         1-28

DGS-3000-28SC#
```

61-5 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 1-64>

Parameters

<value 1-64> - Enter the MSTP instance ID here. This value must be between 1 and 64.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To create MSTP instance:

```
DGS-3000-28SC:admin#create stp instance_id 2
Command: create stp instance_id 2

Success.

DGS-3000-28SC:admin#
```

61-6 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 1-64> [add_vlan | remove_vlan] <vidlist>

Parameters

<value 1-64> - Enter the MSTP instance ID here. This value must be between 1 and 64.
add_vlan - Specify to map the specified VLAN list to an existing MST instance.
remove_vlan - Specify to delete the specified VLAN list from an existing MST instance.
<vidlist> - Enter 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-3000-28SC:admin#config stp instance_id 2 add_vlan 1-3
Command: config stp instance_id 2 add_vlan 1-3

Success.

DGS-3000-28SC:admin#
```

To remove a VLAN ID from an MSTP instance:

```
DGS-3000-28SC:admin#config stp instance_id 2 remove_vlan 2
Command: config stp instance_id 2 remove_vlan 2

Success.

DGS-3000-28SC:admin#
```

61-7 delete stp instance_id

Description

This command is used to delete an MST Instance.

Format

delete stp instance_id <value 1-64>

Parameters

<value 1-64> - Enter the MSTP instance ID here. This value must be between 1 and 64.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete an MSTP instance:

```
DGS-3000-28SC:admin#delete stp instance_id 2
Command: delete stp instance_id 2

Success.

DGS-3000-28SC:admin#
```

61-8 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

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.
name - (Optional) Specify the name given for a specific MST region. **<string>** - Enter the MST region name here.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To change the name and revision level of the MST configuration identification:

```
DGS-3000-28SC: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-3000-28SC:admin#
```

61-9 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-3000-28SC: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-3000-28SC:admin#
```

61-10 config stp mst_ports

Description

This command is used to configure the ports management parameters.

Format

config stp mst_ports <portlist> instance_id <value 0-64> {internalCost [auto | <value 1-200000000>] | priority <value 0-240>}

Parameters

<portlist> - Enter a list of ports used for the configuration here.
instance_id - Specify the instance ID used. **<value 0-64>** - Enter the instance ID used here. This value must be between 0 and 64.
internalCost - (Optional) Specify the port path cost used in MSTP. **auto** - Specify 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) Specify 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-3000-28SC:admin#config stp mst_ports 1 instance_id 0 internal_cost auto
Command: config stp mst_ports 1 instance_id 0 internal_cost auto

Success.

DGS-3000-28SC:admin#
```

61-11 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] | loop_guard [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** - Specify that the external cost value will be set to automatic. **<value 1-200000000>** - Enter the external cost value here. This value must be between 1 and 200000000.
hellotime - (Optional) 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.
migrate - (Optional) Operation of management in order to specify the port to send MSTP BPDU for a delay time. **yes** - Specify that the MSTP BPDU for a delay time will be sent. **no** - Specify that the MSTP BPDU for a delay time will not be sent.
edge - (Optional) To decide if this port is connected to a LAN or a Bridged LAN. **true** - Specify that the specified port(s) is edge. **false** - Specify 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 BPUD is received. The default is auto mode.
p2p - (Optional) To decide if this port is in Full-Duplex or Half-Duplex mode. **true** - Specify that the port(s) is in Full-Duplex mode. **false** - Specify that the port(s) is in Half-Duplex mode. **auto** - Specify that the port(s) is in Full-Duplex and Half-Duplex mode.
state - (Optional) To decide if this port supports the STP functionality. **enable** - Specify that STP functionality on the port(s) is enabled. **disable** - Specify that STP functionality on the port(s) is disabled.
restricted_role - (Optional) To decide if this port not to be selected as Root Port. The default value is false. **true** - Specify that the port can not be specified as the root port. **false** - Specify that the port can be specified as the root port.
restricted_tcn - (Optional) To decide if this port not to propagate topology change. The default value is false. **true** - Specify that the port can not be set to propagate a topology change. **false** - Specify that the port can be set to propagate a topology change.
loop_guard – To decide if this port can loop guard. The default is false. **true** - Specify that the port can be set to loop guard **false** - Specify that the port can not be set to loop guard change.
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** - Specify that the port can be set to flood the STP BPDU when the STP functionality is disabled. **disable** - Specify that the port can not be set to flood the STP BPDU when the STP

functionality is disabled.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure STP ports:

```
DGS-3000-28SC:admin#config stp ports 1 externalCost auto
Command: config stp ports 1 externalCost auto

Success.

DGS-3000-28SC:admin#
```

61-12 show stp ports

Description

This command is used to show the port information includes parameters setting and operational value.

Format

show stp ports {<portlist>}

Parameters

<portlist> - (Optional) Enter a list of ports to display parameters of the designated port numbers, to be distinguished from showing parameters of the bridge..

Restrictions

None.

Example

To show STP ports:

```
DGS-3000-28SC:admin#show stp ports
Command: show stp ports

MSTP instance id. Instance 0 represents the default instance : CIST.
The number of instances is defined by each project.

MSTP Port Information
Port Index        : 1     ,  Hello Time       : 2 /2 ,  Port STP : Enabled
External PathCost : Auto/200000   ,  Edge Port : No /No ,  P2P    : False/No
Port RestrictedRole : False,  Port RestrictedTCN : False
Forwarding BPDU   : Enabled,  Loop guard : False

Msti   Designated Bridge   Internal PathCost   Prio  Status      Role
-----  ------------------  -----------------  ----  ----------  ----------
0        N/A                   200000               128   Disabled    Disabled
2        N/A                   200000               128   Disabled    Disabled

CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

61-13 config stp priority

Description

This command is used to configure the instance priority.

Format

config stp priority <value 0-61440> instance_id <value 0-64>

Parameters

<value 0-61440> - Enter the bridge priority value here. This value must be divisible by 4096. This value must be between 0 and 61440.
instance_id - Identifier to distinguish different STP instances. **<value 0-64>** - Enter the STP instance ID here. This value must be between 0 and 64.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the STP instance ID:

```
DGS-3000-28SC:admin#config stp priority 61440 instance_id 0
Command: config stp priority 61440 instance_id 0

Success.

DGS-3000-28SC:admin#
```

61-14 config stp version

Description

This command is used to configure the STP version.

Format

config stp version [mstp | rstp | stp]

Parameters

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-3000-28SC:admin#config stp version mstp
Command: config stp version mstp

Success.

DGS-3000-28SC:admin#
```

To config STP version with the same value of old configuration:

```
DGS-3000-28SC:admin#config stp version mstp
Command: config stp version mstp

Configure value is the same with current value.
Success.

DGS-3000-28SC:admin#
```

61-15 config stp trap

Description

This command is used to enable or disable sending STP traps.

Format

config stp trap {topo_change [disable | enable] | new_root [enable | disable]}(1)

Parameters

topo_change - Specify to enable or disable topology change traps. Enable is default. **disable** - Enter disable to deactivate topology trap changes. **enable** - Enter enable to activate topology trap changes.
new_root - Specify to enable or disable new root traps. Enable is default. **enable** - Enter enable to activate the new root bridge trap. **disable** - Enter disable to deactivate the new root bridge trap.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To disable sending new root traps:

```
DGS-3000-28SC:admin# config stp trap new_root disable
Command: config stp trap new_root disable

Success.

DGS-3000-28SC:admin#
```

61-16 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 0-64>}

Parameters

<value 0-64> - (Optional) Enter the MSTP instance ID value here. This value must be between 0 and 64.

Restrictions

None.

Example

To show STP instance:

```
DGS-3000-28SC: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-3000-28SC:admin#
```

61-17 enable stp multiprocess_rstp

Description

This command is used to enable RSTP multi-process function globally. This is only supported in the RSTP version.

Format

enable stp multiprocess_rstp

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable the RSTP multi process function globally:

```
DGS-3000-28SC:admin#enable stp multiprocess_rstp
Command: enable stp multiprocess_rstp

Success.

DGS-3000-28SC:admin#
```

61-18 disable stp multiprocess_rstp

Description

This command is used to disable STP multi-process RSTP globally.

Format

disable stp multiprocess_rtsp

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To disable STP multi-process RSTP globally:

```
DGS-3000-28SC:admin#disable stp multiprocess_rstp
Command: disable stp multiprocess_rstp

Success.

DGS-3000-28SC:admin#
```

61-19 create stp multiprocess_rstp

Description

This command is used to create an RSTP ring when the RSTP multi-process function is enabled.

Format

create stp multiprocess_rstp <string>

Parameters

<string> - Enter the name of the RSTP string. Each RSTP ring runs the RSTP protocol. The ring name can consist of up to 32 characters.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To create an RSTP ring:

```
DGS-3000-28SC:admin#create stp multiprocess rstp Ring1
Command: create stp multiprocess rstp Ring1

Success.

DGS-3000-28SC:admin#
```

61-20 delete stp multiprocess_rstp

Description

This command is used to delete an RSTP ring when the RSTP multi-process function is enabled.

Format

delete stp multiprocess_rstp <string>

Parameters

<string> - Enter the name of the RSTP string. Each RSTP ring runs the RSTP protocol but will not affect other RSTP rings.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete an RSTP ring:

```
DGS-3000-28SC:admin#delete stp multiprocess rstp Ring1
Command: delete stp multiprocess rstp Ring1

Success.

DGS-3000-28SC:admin#
```

61-21 config stp multiprocess_rstp

Description

This command is used to add ports to an RSTP ring or to remove ports from an RSTP ring.

Format

config stp multiprocess_rstp <string> [add | delete] ports <portlist>

Parameters

<string> - Enter the name of the RSTP string. Each RSTP ring runs the RSTP protocol but will not affect other RSTP rings.
add - Specify to add an RSTP ring.
delete - Specify to delete an RSTP ring.
ports - Specify the RSTP port number. **<portlist>** - Enter the port.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To add ports to an RSTP ring:

```
DGS-3000-28SC:admin#config stp multiprocess_rstp add ports 1-3
Command: admin#config stp multiprocess_rstp add ports 1-3

Success.

DGS-3000-28SC:admin#
```

To remove ports to an RSTP ring:

```
DGS-3000-28SC:admin#config stp multiprocess_rstp delete ports 1-3
Command: admin#config stp multiprocess_rstp delete ports 1-3

Success.

DGS-3000-28SC:admin#
```

Chapter 62 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 1-4094>] <macaddr>
config nlb multicast_fdb [<vlan_name32> | vlanid <vlanid1-4094>] <macaddr> [add | delete] <portlist>
delete nlb multicast_fdb [<vlan_name32> | vlanid <vlanid1-4094>] <macaddr>
show nlb fdb

62-1 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> - Enter 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-3000-28SC:admin#create nlb unicast_fdb 02-bf-01-01-01-01
Command: create nlb unicast_fdb 02-BF-01-01-01-01

Success.

DGS-3000-28SC:admin#
```

62-2 config nlb unicast_fdb

Description

This command is used to add or delete the forwarding ports for the specified NLB unicast FDB entry.

Format

config nlb unicast_fdb <macaddr> [add | delete] <portlist>

Parameters

<macaddr> - Enter the MAC address of the NLB unicast FDB entry to be configured.
add - Specify to add the ports.
delete - Specify to delete the ports.
<portlist> - Enter a list of forwarding ports to be added or removed.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure NLB unicast FDB entry, for the product that support the VLAN information on the unicast forwarding:

```
DGS-3000-28SC: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-3000-28SC:admin#
```

62-3 delete nlb unicast_fdb

Description

This command is used to delete the NLB unicast FDB entry.

Format

delete nlb unicast_fdb <macaddr>

Parameters

<macaddr> - Enter the MAC address of the NLB unicast FDB entry to be deleted.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete the NLB unicast FDB entry, for the product that support the VLAN information on the unicast forwarding:

```
DGS-3000-28SC:admin#delete nlb unicast_fdb 02-bf-01-01-01-01
Command: delete nlb unicast_fdb 02-BF-01-01-01-01

Success.

DGS-3000-28SC:admin#
```

62-4 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 1-4094>] <macaddr>

Parameters

<vlan_name 32> - Enter the VLAN name of the NLB multicast FDB entry here. The VLAN name can be up to 32 characters long.
vlanid - Specify the VLAN by the VLAN ID. **<vlanid 1-4094>** - Enter the VLAN ID here.
<macaddr> - Enter the MAC address of the NLB multicast FDB entry to be created. Multicast MAC addresses with the prefix of 33-33-XX-XX-XX is used for address mapping with IP addresses. To avoid incorrect forwarding behaviors, 33-33-XX-XX-XX is not supported. Multicast MAC addresses with the prefix 01-80-C2-XX-XX is reserved MAC addresses and is also not supported.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To create a NLB multicast FDB entry:

```
DGS-3000-28SC: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-3000-28SC:admin#
```

62-5 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_name32> | vlanid <vlanid1-4094>] <macaddr> [add | delete] <portlist>

Parameters

<vlan_name 32> - Enter the VLAN of the NLB multicast FDB entry to be configured.
vlanid - Specify the VLAN by the VLAN ID. **<vlanid1-4094>** - Enter the VLAN ID here. Enter a value between 1 to 4094.
<macaddr> - Enter the Mac address of the NLB multicast FDB entry to be configured.
add - Specify a list of forwarding ports to be added.
delete - Specify 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-3000-28SC: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-3000-28SC:admin#
```

62-6 delete nlb multicast_fdb

Description

This command is used to delete the NLB multicast FDB entry.

Format

delete nlb multicast_fdb [<vlan_name32> | vlanid <vlanid1-4094>] <macaddr>

Parameters

<vlan_name 32> - Enter the VLAN of the NLB multicast FDB entry to be deleted.
vlanid - Specify the VLAN by VLAN ID. **<vlanid 1-4094>** - Enter the VLAN ID here. The value can be between 1 to 4094 characters.
<macaddr> - Enter the MAC address of the NLB multicast FDB entry to be deleted.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete NLB multicast FDB entry:

```
DGS-3000-28SC: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-3000-28SC:admin#
```

62-7 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-3000-28SC: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-3000-28SC:admin#
```

Chapter 63 Network Monitoring Command List

clear counters {ports <portlist>}
show error ports <portlist>
show packet ports <portlist>
show utilization [cpu | ports]
show utilization dram {unit <unit_id>}
show utilization flash {unit <unit_id>}

63-1 clear counters

Description

This command is used to clear the Switch's statistics counters.

Format

clear counters {ports <portlist>}

Parameters

ports - (Optional) Specify 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-3000-28SC:admin#clear counters ports 7-9
Command: clear counters ports 7-9

Success.

DGS-3000-28SC:admin#
```

63-2 show error ports

Description

This command is used to display the error statistics for a range of ports.

Format

show errors ports <portlist>

Parameters

<portlist> - Enter a range of ports to be displayed.

Restrictions

None.

Example

To display the errors of the port:

```
DGS-3000-28SC:admin#show error ports 3
Command: show error ports 3

Port Number : 1:3
                        RX Frames                           TX Frames
                        ---------                           ---------
 CRC Error              0             Excessive Deferral    0
 Undersize              0             CRC Error             0
 Oversize               0             Late Collision        0
 Fragment               0             Excessive Collision   0
 Jabber                 0             Single Collision      0
 Symbol Error           0             Collision             0
 Buffer Full Drop       0             STP Drop              0
 ACL Drop               0             HOL Drop              0
 Multicast Drop         0
 VLAN Ingress Drop      0
 Invalid IPv6           0
 STP Drop               0
 Storm and FDB Discard  0
 MTU Drop               0

CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

63-3 show packet ports

Description

This command is used to display statistics about the packets sent and received by the Switch.

Format

show packet ports <portlist>

Parameters

<portlist> - Enter a range of ports to be displayed.

Restrictions

None.

Example

To display the packets analysis for port 7:

```
DGS-3000-28SC:admin#show packet ports 7
Command: show packet ports 7

Port number : 1:7
 Frame Size/Type       Frame Counts                Frames/sec
 ---------------       ----------------------      -----------
 64                    0                           0
 65-127                0                           0
 128-255               0                           0
 256-511               0                           0
 512-1023              0                           0
 1024-1518             0                           0
 1519-1522             0                           0
 1519-2047             0                           0
 2048-4095             0                           0
 4096-9216             0                           0
 Unicast RX            0                           0
 Multicast RX          0                           0
 Broadcast RX          0                           0

CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

63-4 show utilization

Description

This command is used to display real-time CPU or port utilization statistics.

Format

show utilization [cpu | ports]

Parameters

cpu - Specify to display information regarding the CPU.
ports - Specify all ports to be displayed.

Restrictions

None.

Example

To display the ports utilization:

```
DGS-3000-28SC: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-3000-28SC:admin#
```

To display the CPU utilization:

```
DGS-3000-28SC: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
```

63-5 show utilization dram

Description

This command is used to show DRAM memory utilization.

Format

show utilization dram {unit <unit_id>}

Parameters

unit - (Optional) Specify the Switch unit ID to be displayed. **<unit_id>** - Enter the unit ID value. This value must be between 1 and 6.

Restrictions

None.

Example

To display DRAM utilization:

```
DGS-3000-28SC:admin#show utilization dram
Command: show utilization dram

DRAM Utilization :
        Total DRAM      : 131072    KB
        Used DRAM       : 128128    KB
        Utilization     : 97 %


CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

63-6 show utilization flash

Description

This command is used to display real-time FLASH memory utilization statistics.

Format

show utilization flash {unit <unit_id>}

Parameters

unit - (Optional) Specify the Switch unit ID to be displayed. **<unit_id>** - Enter the unit ID value. This value must be between 1 and 6.

Restrictions

None.

Example

To display FLASH utilization:

```
DGS-3000-28SC:admin#show utilization flash
Command: show utilization flash

Flash Memory Utilization :
        Total Flash     : 29937     KB
        Used Flash      : 18358      KB
        Utilization     : 61 %

CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

Chapter 64 OAM Command List

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]} | error_frame {threshold <range 0-4294967295> | window <millisecond 1000-60000> | notify_state [enable | disable]} | error_frame_seconds {threshold <range 1-900> | window <millisecond 10000-900000> | notify_state [enable | disable]} | error_frame_period {threshold <range 0-4294967295> | window <number 14881-892860000> | notify_state [enable | disable]}] | 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]

64-1 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. This command is used to configure the client to process or to ignore the received Ethernet OAM remote loopback command. In remote loopback mode, all user traffic will not be processed. Ignoring the received remote loopback command will prevent the port from entering remote loopback mode.

Format

config ethernet_oam ports [<portlist> | all] [mode [active | passive] | state [enable | disable] | link_monitor [error_symbol {threshold <range 0-4294967295> | window <millisecond 1000-60000> | notify_state [enable | disable]} | error_frame {threshold <range 0-4294967295> | window <millisecond 1000-60000> | notify_state [enable | disable]} | error_frame_seconds {threshold <range 1-900> | window <millisecond 10000-900000> | notify_state [enable |

disable]} | error_frame_period {threshold <range 0-4294967295> | window <number 14881-892860000> | notify_state [enable | disable]}] | critical_link_event [dying_gasp | critical_event] notify_state [enable | disable] | remote_loopback [start | stop] | received_remote_loopback [process | ignore]]

Parameters

<portlist> - Enter a range of ports to be configured.

all - Specify all ports to be configured.

mode - Specify the operation mode. The default mode is active.
- **active** - Specify to operate in active mode.
- **passive** - Specify to operate in passive mode.

state - Specify the OAM function status.
- **enable** - Specify to enable the OAM function.
- **disable** - Specify to disable the OAM function.

link_monitor - Specify to detect and indicate link faults under a variety of conditions.
- **error_symbol** - Specify to generate an error symbol period event to notify the remote OAM peer.
  - **threshold** - (Optional) Specify the number of symbol errors in the period that is required to be equal to or greater than in order for the event to be generated. The default value of threshold is 1 symbol error.
    - **<range 0-4294967295>** - Enter the range from 0 to 4294967295.
  - **window** - (Optional) The range is 1000 to 60000 ms. The default value is 1000ms.
    - **<millisecond 1000-60000>** - Enter a value in a range from 1000 to 60000 ms.
  - **notify_state** - (Optional) Specify the event notification status. The default state is enable.
    - **enable** - Specify to enable event notification.
    - **disable** - Specify to disable event notification.
- **error_frame** - Specify the error frame.
  - **threshold** - (Optional) Specify a threshold range.
    - **<range 0-4294967295>** - Enter a threshold range between 0 and 4294967295.
  - **window** - (Optional) The range is 1000 to 60000 ms. The default value is 1000ms.
    - **<millisecond 1000-60000>** - Enter a value within the range between 1000 to 60000 ms.
  - **notify_state** - (Optional) Specify the event notification status. The default state is enable.
    - **enable** - Specify to enable event notification.
    - **disable** - Specify to disable event notification.
- **error_frame_seconds** - Specify error fram time.
  - **threshold** - (Optional) Specify a threshold range between 1 and 900.
    - **<range 1-900>** - Enter a threshold range between 1 and 900.
  - **window** - (Optional) The range is 1000 to 900000 ms.
    - **<millisecond 10000-900000>** - Enter a value between the range 1000 to 900000 ms.
  - **notify_state** - (Optional) Specify the event notification status. The default state is enable.
    - **enable** - Specify to enable event notification.
    - **disable** - Specify to disable event notification.
- **error_frame_period** - Specify error frame period.
  - **threshold** - (Optional) Specify a threshold range between 0 and 4294967295.
    - **<range 0-4294967295>** - Enter a threshold range between 0 and 4294967295.
  - **window** - (Optional) The range is 148810 to 100000000 ms.
    - **<number 14881892860000>** - Enter a range between 1 to 14881892860000 ms.
  - **notify_state** - (Optional) Specify the event notification status. The default state is enable.
    - **enable** - Specify to enable event notification.
    - **disable** - Specify to disable event notification.

critical_link_event - Specify critical link event.
- **dying_gasp** - An unrecoverable local failure condition has occurred.
- **critical_event** - An unspecified critical event has occurred.
- **notify_state** - Specify the event notification status. The default state is enable.
  - **enable** - Specify to enable event notification.
  - **disable** - Specify to disable event notification.

remote_loopback - Specify 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 - Specify receive remote loop-back. **process** - Specify to process the received Ethernet OAM remote loopback command. **ignore** - Specify 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-3000-28SC:admin#config ethernet_oam ports 1-2 mode active
Command: config ethernet_oam ports 1-2 mode active

Success.

DGS-3000-28SC:admin#
```

To enable Ethernet OAM on port 1:

```
DGS-3000-28SC:admin#config ethernet_oam ports 1 state enable
Command: config ethernet_oam ports 1 state enable

Success.

DGS-3000-28SC:admin#
```

To configure the error symbol threshold to 2 and period to 1000ms for port 1:

```
DGS-3000-28SC: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-3000-28SC:admin#
```

To configure the error frame threshold to 2 and period to 1000 ms for port 1:

```
DGS-3000-28SC: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-3000-28SC:admin#
```

To configure the error frame seconds threshold to 2 and period to 10000 ms for port 1:

```
DGS-3000-28SC: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-3000-28SC:admin#
```

To configure the error frame threshold to10 and period to 1000000 ms for port 1:

```
DGS-3000-28SC: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-3000-28SC:admin#
```

To configure a dying gasp event for port 1:

```
DGS-3000-28SC: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-3000-28SC:admin#
```

To start remote loopback on port 1:

```
DGS-3000-28SC:admin#config ethernet_oam ports 1 remote_loopback start
Command: config ethernet_oam ports 1 remote_loopback start

Success.

DGS-3000-28SC:admin#
```

To configure the method of processing the received remote loopback command as “process” on port 1:

```
DGS-3000-28SC:admin#config ethernet_oam ports 1 received_remote_loopback
process
Command: config ethernet_oam ports 1 received_remote_loopback process

Success.

DGS-3000-28SC:admin#
```

64-2 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:

- OAM administration status: enabled or disabled.
- 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.
- OAM mode: passive or active.
- 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.
- 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.
- OAM mode change.
- OAM Functions Supported: The OAM functions supported on this port. These functions include:
    - Unidirectional: It indicates that the OAM entity supports the transmission of OAMPDUs on links that are operating in unidirectional mode (traffic flowing in one direction only).
    - Loopback: It indicates that the OAM entity can initiate and respond to loopback commands.
    - Link Monitoring: It indicates that the OAM entity can send and receive Event Notification OAMPDUs.
    - Variable: It indicates that the OAM entity can send and receive variable requests to monitor the attribute value as described in the IEEE 802.3 Clause 30 MIB.

The event log displays Ethernet OAM event log information. The switch can buffer 1000 event logs. The event log is different from sys-log as it provides more detailed information than sys-log. Each OAM event will be recorded in both OAM event log and syslog.

Format

show ethernet_oam ports {<portlist>} [status | configuration | statistics | event_log {index <value_list>}]

Parameters

<portlist> - (Optional) Enter the range of ports to display.
status - Specify to display the Ethernet OAM status.
configuration - Specify to display the Ethernet OAM configuration.
statistics - Specify to display Ethernet OAM statistics.
event_log - Specify to display the Ethernet OAM event log information. **index** - (Optional) Specify an index range to display. **<value_list>** - Enter an index range to display.

Restrictions

Only Administrators and Operators can issue this command.

Example

To display Ethernet OAM statistics information for port 1:

```
DGS-3000-28SC:admin#show ethernet_oam ports 1 statistics
Command: show ethernet_oam ports 1 statistics

Port 1
------------------------------------------------------------
Information OAMPDU TX                : 0
Information OAMPDU RX                : 0
Unique Event Notification OAMPDU TX   : 0
Unique Event Notification OAMPDU RX   : 0
Duplicate Event Notification OAMPDU TX: 0
Duplicate Event Notification OAMPDU RX: 0
Loopback Control OAMPDU TX            : 0
Loopback Control OAMPDU RX            : 0
Variable Request OAMPDU TX            : 0
Variable Request OAMPDU RX            : 0
Variable Response OAMPDU TX           : 0
Variable Response OAMPDU RX           : 0
Organization Specific OAMPDUs TX      : 0
Organization Specific OAMPDUs RX      : 0
Unsupported OAMPDU TX                 : 0
Unsupported OAMPDU RX                 : 0
Frames Lost Due To OAM                : 0

DGS-3000-28SC:admin#
```

64-3 clear ethernet_oam ports

Description

This command is used to clear Ethernet OAM information.

Format

clear ethernet_oam ports [<portlist> | all] [event_log | statistics]

Parameters

<portlist> - Enter a range of Ethernet OAM ports to be cleared.
all - Specify to clear all Ethernet OAM ports.
event_log - Specify to clear Ethernet OAM event log information.
statistics - Specify to clear Ethernet OAM statistics.

Restrictions

Only Administrators and Operators can issue this command.

Example

To clear port 1 OAM statistics:

```
DGS-3000-28SC:admin#clear ethernet_oam ports 1 statistics
Command: clear ethernet_oam ports 1 statistics

Success.

DGS-3000-28SC:admin#
```

To clear port 1 OAM events:

```
DGS-3000-28SC:admin#clear ethernet_oam ports 1 event_log
Command: clear ethernet_oam ports 1 event_log

Success.

DGS-3000-28SC:admin#
```

Chapter 65 Password Recovery Command List

enable password_recovery
disable password_recovery
show password_recovery

65-1 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-3000-28SC:admin#enable password_recovery
Command: enable password_recovery

Success.

DGS-3000-28SC:admin#
```

65-2 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-3000-28SC:admin#disable password_recovery
Command: disable password_recovery

Success.

DGS-3000-28SC:admin#
```

65-3 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-3000-28SC:admin#show password_recovery
Command: show password_recovery

 Running Configuration  : Enabled
 NV-RAM Configuration   : Enabled

DGS-3000-28SC:admin#
```

Chapter 66 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]
config fan trap state [enable | disable]
config power trap state [enable | disable]

66-1 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-3000-28SC:admin#show device_status
Command: show device_status

Unit   1:
    Internal Power: Active
    External Power: Fail
    Right Fan     : OK

DGS-3000-28SC:admin#
```

66-2 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-3000-28SC:admin#show environment
Command: show environment

Temperature Trap State     :  Enabled
Temperature Log State      :  Enabled
Fan Trap State             :  Enabled
Power Trap State           :  Enabled

High Warning Temperature Threshold(Celsius) :    79
Low Warning Temperature Threshold(Celsius)  :    11

Unit    1
Internal Power      : Active
External Power      : Fail
Right Fan 1         : Speed Low  (3000 RPM)
Right Fan 2         : Speed Low  (3000 RPM)
Current Temperature(Celsius) :   25
Fan High Temperature Threshold(Celsius)     :    41
Fan Low Temperature Threshold(Celsius)      :    36

DGS-3000-28SC:admin#
```

66-3 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) Specify to configure high threshold value. The high threshold must bigger than the low threshold. **<temperature -500-500>** - Enter the high threshold temperature.
low - (Optional) Specify 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-3000-28SC:admin#config temperature threshold high 80
Command: config temperature threshold high 80

Success.

DGS-3000-28SC:admin#
```

66-4 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 - Specify to enable or disable the trap state of the temperature warning event.
log - Specify to enable or disable the log state of the temperature warning event.
state - Specify to enable or disable the trap or log state of the temperature warning event. **enable** - Specify to enable the trap or log state of the temperature warning event. This is the default option. **disable** - Specify to disable the trap or log state of the temperature warning event.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the warning temperature trap state:

```
DGS-3000-28SC:admin#config temperature trap state enable
Command: config temperature trap state enable

Success.

DGS-3000-28SC:admin#
```

66-5 config fan trap state

Description

This command is used to configure the trap state for fan warning event.

Format

config fan trap state [enable | disable]

Parameters

enable - Specify to enable trap state for warning fan event.
disable - Specify to disable trap state for warning fan event.

Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

Example

To configure the warning fan traps state:

```
DGS-3000-28SC:admin#config fan trap state enable
Command: config fan trap state enable

Success.

DGS-3000-28SC:admin#
```

66-6 config power trap state

Description

This command is used to configure the trap state for power warning event.

Format

config power trap state [enable | disable]

Parameters

enable - Specify to enable trap state for warning power event.
disable - Specify to disable trap state for warning power event.

Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

Example

To configure the warning power traps state:

```
DGS-3000-28SC:admin# config power trap state enable
Command: config power trap state enable

Success.

DGS-3000-28SC:admin#
```

Chapter 67 Ping Command List

ping [<ipaddr> | <domain_name 255>] {times <value 1-255> | timeout <sec 1-99> | source_ip <ipaddr> | frequency <sec 0-86400>}
ping6 [<ipv6addr> | <domain_name 255>] {times <value 1-255> | size <value 1-6000>| timeout <sec 1-99> | source_ip <ipv6addr> | frequency <sec 0-86400>}
enable broadcast_ping_reply
disable broadcast_ping_reply
show broadcast_ping_reply

67-1 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> | source_ip <ipaddr> | frequency <sec 0-86400>}

Parameters

<ipaddr> - Enter the IP address of the host.
<domain_name 255> - Enter the domain name of the host.
times - (Optional) The number of individual ICMP echo messages to be sent. The maximum value is 255. 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.
source_ip - (Optional) Specify the IP source. **<ipaddr>** - Enter the IP address here.
frequency - (Optional) Specify the packet frequency. **<sec 0-86400>** - Enter a range between 0 to 86400 seconds.

Restrictions

None.

Example

To send an ICMP echo message to “10.51.17.1” 4 times:

```
DGS-3000-28SC: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-3000-28SC:admin#
```

67-2 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> | source_ip <ipv6addr> | frequency <sec 0-86400>}**

Parameters

<ipv6addr> - Enter the IPv6 address here.
<domain_name 255> - Enter the domain name of the host.
times - (Optional) The number of individual ICMPv6 echo messages to be sent. The maximum value is 255. 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.
source_ip - (Optional) Specify the IPv6 address. **<ipv6addr>** - Enter the IPv6 address here.
frequency - (Optional) Specify the IPv6 packet frequency. **<sec 0-86400>** - Enter a range between 0 to 86400 seconds.

Restrictions

None.

Example

To send ICMPv6 echo message to “3000::1” for 4 times:

```
DGS-3000-28SC: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-3000-28SC:admin#
```

67-3 enable broadcast_ping_reply

Description

This command is used to enable the broadcast ping reply state.

Format

enable broadcast_ping_reply

Parameters

None.

Restrictions

None.

Example

To enable the broadcast ping reply state:

```
DGS-3000-28SC:admin# enable broadcast_ping_reply
Command: enable broadcast_ping_reply

Success.

DGS-3000-28SC:admin#
```

67-4 disable broadcast_ping_reply

Description

This command is used to disable the broadcast ping reply state.

Format

disable broadcast_ping_reply

Parameters

None.

Restrictions

None.

Example

To disable the broadcast ping reply state:

```
DGS-3000-28SC:admin# disable broadcast_ping_reply
Command: disable broadcast_ping_reply

Success.

DGS-3000-28SC:admin#
```

67-5 show broadcast_ping_reply

Description

This command is used to show the broadcast ping reply state.

Format

show broadcast_ping_reply

Parameters

None.

Restrictions

None.

Example

To disable the broadcast ping reply state:

```
DGS-3000-28SC:admin# show broadcast_ping_reply
Command: show broadcast_ping_reply

Broadcast Ping Reply State:  Enabled

DGS-3000-28SC:admin#
```

Chapter 68 Port Security Command List

config port_security system max_learning_addr [<max_lock_no 1-3072> | no_limit]
config port_security ports [<portlist> | all] [{admin_state [enable | disable] | max_learning_addr <max_lock_no 0-3072> | action [drop | shutdown] | lock_address_mode [permanent | deleteontimeout | deleteonreset]}(1) | {vlan [<vlan_name32> | vlanid <vidlist>] max_learning_addr [<max_lock_no 0-3072> | no_limit]}(1)]
config port_security vlan [<vlan_name 32> | vlanid <vidlist>] max_learning_addr [<max_lock_no 0-3072> | 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>]}}
config port_security log state [enable | disable]
config port_security trap state [enable | disable]

68-1 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 1-3072> | no_limit]

Parameters

<max_lock_no 1-3328> - Enter 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-3000-28SC:admin#config port_security system max_learning_addr 256
Command: config port_security system max_learning_addr 256

Success.

DGS-3000-28SC:admin#
```

68-2 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 0-3072> | action [drop | shutdown] | lock_address_mode [permanent | deleteontimeout | deleteonreset]}(1) | {vlan [<vlan_name32> | vlanid <vidlist>] max_learning_addr [<max_lock_no 0-3072> | no_limit]}(1)]

Parameters

<portlist> - Enter the list of port used for this configuration here.
all - Specify that all ports will be configured.
admin_state - Specify the state of the port security function on the port. **enable** - Specify to enable the port security function on the port. **disable** - Specify to disable the port security function on the port. By default, the setting is disabled.
max_learning_addr - Specify 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 0-3072>** - Enter the maximum number of port security entries that can be learned here. This value must be between 0 and 3072.
action - Specify the action to be taken when the number of secure MAC address reaches the maximum learning on the port. **drop** - When the number of secure MAC address reaches the maximum learning on the port, new entry will be dropped. This is the default setting. **shutdown** - When the number of secure MAC address reaches the maximum learning on the port, the port will be shut down and enter error-disabled state immediately. The port state is recovered only by enabling the port manually.The shutdown action only applies to port level security setting.
lock_address_mode - 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 - Specify the VLAN name used here. **<vlan_name 32>** - Enter the VLAN name used here. This name can be up to 32 characters long.

vlanid - Specify the VLAN ID used here. **<vidlist>** - Enter the VLAN ID used here.
max_learning_addr - Specify the maximum learning address value. **<max_lock_no 0-3072>** - Enter the maximum learning address value here. This value must be between 0 and 3072. **no_limit** - Specify 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-3000-28SC: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-3000-28SC:admin#
```

68-3 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 0-3072> | no_limit]

Parameters

<vlan_name 32> - Enter the VLAN name here. This name can be up to 32 characters long.
vlanid - Specify a list of VLANs by VLAN ID. **<vidlist>** - Enter the VLAN ID list here.
max_learning_addr - Specify 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 0-3072>** - Enter the maximum number of port security entries that can be learned here. This value must be between 0 and 3072. **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-3000-28SC:admin#config port_security vlan vlanid 1 max_learning_addr 64
Command: config port_security vlan vlanid 1 max_learning_addr 64

Success.

DGS-3000-28SC:admin#
```

68-4 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 - Specify the VLAN by VLAN name. **<vlan_name 32>** - Enter the VLAN name here. This name can be up to 32 characters long.
vlanid - Specify the VLAN by VLAN ID. **<vlanid 1-4094>** - Enter the VLAN ID list here. This value must be between 1 and 4094.
mac_address - Specify 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-3000-28SC: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-3000-28SC:admin#
```

68-5 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) Specify the range of ports to be configured. **<portlist>** - Enter the port security entries learned on the specified port. **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) Specify 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-3000-28SC:admin#clear port_security_entry ports 6
Command: clear port_security_entry ports 6

Success.

DGS-3000-28SC:admin#
```

68-6 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 Specify 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) Specify the range of ports that will display the port security entries.

<portlist> - (Optional) Enter the list of port used for this configuration here. If no port is specified, information for all ports will be displayed.
vlan - (Optional) Specify 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) Specify 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-3000-28SC: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-3000-28SC:admin#
```

68-7 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) Specify the range of ports that will show their configuration. **<portlist>** - (Optional) Enter the list of port used for this configuration here. If no port is specified, information for all ports will be displayed.
vlan - (Optional) Specify 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) Specify 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-3000-28SC:admin#show port_security
Command: show port_security

Port Security Trap State      : Disabled
Port Security Log State       : Disabled
System Maximum Address        : 256

VLAN Configuration (Only VLANs with limitation are displayed)
VID   VLAN Name                         Max. Learning Addr.
 ----  --------------------------------  ------------------
 1     default                           64

DGS-3000-28SC:admin#
```

68-8 config port_security log state

Description

This command is used to enable or disable the port security log. When the port security log is enabled, if there is a new MAC that violates the pre-defined port security configuration, the MAC, port and other relevant information will be logged, otherwise, no log will be generated.

Format

config port_security log state [enable | disable]

Parameters

enable - Specify to enable port security log.
disable - Specify to disable port security log.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable the port security log:

```
DGS-3000-28SC:admin# config port_security log state enable
Command: config port_security log state enable

Success.

DGS-3000-28SC:admin#
```

68-9 config port_security trap state

Description

This command is used to enable or disable the sending of port security traps. When the port security trap is enabled, if there is a new MAC that violates the pre-defined port security configuration, a trap will be sent out with the information about the MAC address and port. If the port security trap is disabled, no trap will be sent out for a MAC address violation.

Format

config port_security trap state [enable | disable]

Parameters

enable - Specify to enable port security trap.
disable - Specify to disable port security trap.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable the sending of port security traps:

```
DGS-3000-28SC:admin# config port_security trap state enable
Command: config port_security trap state enable

Success.

DGS-3000-28SC:admin#
```

Chapter 69 Power Saving Command List

config power_saving mode {link_detection | led | port | hibernation} [enable | disable]
config power_saving hibernation [[add | delete] time_range <range_name 32> | clear_time_range]
config power_saving led [[add | delete] time_range <range_name 32> | clear_time_range]
config power_saving port [<portlist> | all] [[add | delete] time_range <range_name 32> | clear_time_range]
show power_saving {link_detection | led | port | hibernation}
config led state [enable | disable]
show led

69-1 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.

NOTE: Length detection is not supported in this project.

Format

config power_saving mode {link_detection | led | port | hibernation} [enable | disable]

Parameters

link_detection - (Optional) Specify the power saving link detection state. The default state is enabled.
led - (Optional) Specify to configure the power saving state of the LED port.
port - (Optional) Specify to configure the port power saving state.

hibernation - (Optional) Specify to configure the power saving state of system hibernation. The default state is disabled.
enable - Specify to enable power saving state.
disable - Specify 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-3000-28SC:admin#config power_saving mode port hibernation enable
Command: config power_saving mode port hibernation enable

Success.

DGS-3000-28SC:admin#
```

69-2 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 - Specify to add a time range.
delete - Specify to delete a time range.
time_range - Specify the name of the time range. **<range_name 32>** - Enter a name for maximum 32 characters.
clear_time_range - Specify 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-3000-28SC:admin#config power_saving hibernation add time_range range_1
Command: config power_saving hibernation add time_range range_1

Success.

DGS-3000-28SC:admin#
```

69-3 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 - Specify to add a time range.
delete - Specify to delete a time range.
time_range - Specify the name of the time range. **<range_name 32>** - Enter a name for maximum 32 characters.
clear_time_range - Specify 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-3000-28SC:admin#config power_saving led add time_range range_1
Command: config power_saving led add time_range range_1

Success.

DGS-3000-28SC:admin#
```

69-4 config power_saving port

Description

This command is used to add or delete the power saving schedule on the port. When any schedule is up, the specific port will be shut down (disabled).

NOTE: The port's admin state has high priority. If the port's admin state is disabled, the specific port will always be shut down (disabled). Currently only three time ranges are supported.

Format

config power_saving port [<portlist> | all] [[add | delete] time_range <range_name 32> | clear_time_range]

Parameters

<portlist> - Enter a range of ports.
all - Specify all ports.
add - Specify to add a time range.
delete - Specify to delete a time range.
time_range - Specify the name of the time range. **<range_name 32>** - Enter a name for maximum 32 characters.
clear_time_range - Specify 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-3000-28SC:admin#config power_saving port 1 add time_range range_1
Command: config power_saving port 1 add time_range range_1

Success.

DGS-3000-28SC:admin#
```

To delete a time range named "range_2" on port 1:

```
DGS-3000-28SC:admin#config power_saving port 1 delete time_range range_2
Command: config power_saving port 1 delete time_range range_2

Success.

DGS-3000-28SC:admin#
```

69-5 show power_saving

Description

This command is used to display the current state of power saving.

Format

show power_saving {link_detection | led | port | hibernation}

Parameters

link_detection - (Optional) Specify to display the link detection power saving configuration.
led - (Optional) Specify to display the power saving port LED configuration.
port - (Optional) Specify to display the port power saving configuration.
hibernation - (Optional) Specify to display the power saving system hibernation configuration.
If no parameter is specified, all configurations of power saving will be displayed.

Restrictions

None.

Example

To display the power saving function setting:

```
DGS-3000-28SC:admin# admin#show power_saving
Command: show power_saving

 Function Version: 3.00

 Link Detection State: Enabled
 Power Saving Configuration On System Hibernation
 ------------------------------------------------
 State: Enabled
 Time Range
 --------------------------------
 range_1

 Power Saving Configuration On Port LED
 ---------------------------------------
 State: Disabled

 Power Saving Configuration On Port
 ---------------------------------------
 State: Enabled
 Port       Time Range
 -------    --------------------------------
 1          range_1

DGS-3000-28SC:admin#
```

69-6 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 - Specify to enable the LED admin state of all ports.
disable - Specify 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-3000-28SC:admin#config led state disable
Command: config led state disable

Success.

DGS-3000-28SC:admin#
```

69-7 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-3000-28SC:admin#show led
Command: show led

 Port LED State: Disabled

DGS-3000-28SC:admin#
```

Chapter 70 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> | vendor3 <string 32>] | remote_id [default | vendor3 <string 32>]}(1)
show pppoe circuit_id_insertion
show pppoe circuit_id_insertion ports {<portlist>}

70-1 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 - Specify to enable the PPPoE circuit ID insertion on the Switch.
disable - Specify 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-3000-28SC:admin#config pppoe circuit_id_insertion state enable
Command: config pppoe circuit_id_insertion state enable

Success.

DGS-3000-28SC:admin#
```

70-2 config pppoe circuit_id_insertion ports

Description

This command is used to see then the port's state and the global state are enabled, the system will insert the Circuit ID and Remote ID TAG to the received PPPoE discovery initiation and request packet if the TAG is absent, and remove the Circuit ID and Remote 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> | vendor3 <string 32>] | remote_id [default | vendor3 <string 32>]}(1)

Parameters

<portlist> - Enter a list of ports to be configured.
state - Specify 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 - Specify 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. **vendor3** - Specify the user specified string for the circuit ID option. **<string 32>** - Enter the string value. The maximum length is 32.
remote_id - Specify the remote ID option. **default** - Specify default to leave the Remote ID option length empty. **vendor3** - Specify the user specified string for the circuit ID option. **<string 32>** - Enter the string value. The maximum length is 32.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable port 5 PPPoE circuit ID insertion function:

```
DGS-3000-28SC:admin#config pppoe circuit_id_insertion ports 5 state enable
Command: config pppoe circuit_id_insertion ports 5 state enable

Success.

DGS-3000-28SC:admin#
```

70-3 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-3000-28SC:admin#show pppoe circuit_id_insertion
Command: show pppoe circuit_id_insertion

Global PPPoE State: Enabled


DGS-3000-28SC:admin#
```

70-4 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) Enter a list of ports to be displayed.
If no port is specified, information for all ports will be displayed.

Restrictions

None.

Example

To display port 2-5 PPPoE circuit ID insertion configuration:

```
DGS-3000-28SC:admin# show pppoe circuit_id_insertion ports 2-5
Command: show pppoe circuit_id_insertion ports 2-5

Port State    PPPoE Tags
---- -------- ------------------------------------------------------
 2   Enabled  Circuit ID: Switch IP
              Remote ID : Default
 3   Enabled  Circuit ID: Switch IP
              Remote ID : Default
 4   Enabled  Circuit ID: Switch IP
              Remote ID : Default
 5   Enabled  Circuit ID: Switch IP
              Remote ID : Default

DGS-3000-28SC:admin#
```

Chapter 71 Protocol VLAN Command List

create dot1v_protocol_group group_id <int 1-16> {group_name <name 32>}
config dot1v_protocol_group [group_id <int 1-16> | group_name <name32>] [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 <int 1-16> | group_name <name 32> | all]
show dot1v_protocol_group {[group_id <int 1-16> | group_name <name 32>]}
config port dot1v ports [<portlist> | all] [add protocol_group [group_id <int 1-16> | group_name <name 32>] [vlan<vlan_name 32> | vlanid<id>] {priority <value0-7>} | deleteprotocol_group [group_id <int 1-16> | all]]
show port dot1v {ports <portlist>}

71-1 create dot1v_protocol_group group_id

Description

This command is used to create a protocol group for protocol VLAN function.

Format

create dot1v_protocol_group group_id < int 1-16> {group_name <name 32>}

Parameters

<int 1-16> - Enter the group ID for protocol VLAN. Enter a number between 1 and 16.
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-3000-28SC: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-3000-28SC:admin#
```

71-2 config dot1v_protocol_group

Description

This command is used to add a protocol to a protocol group. The selection of a protocol can be a pre-defined protocol type or a user defined protocol.

Format

config dot1v_protocol_group [group_id <int 1-16> | 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. **<int 1-16>** - Enter the group ID used here. This name can be up to 32 characters long.
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 - Specify that the protocol will be added to the specified group. **protocol** - The protocol value is used to identify a protocol of the frame type specified. **ethernet_2** - Specify that the Ethernet 2 protocol will be used. **ieee802.3_snap** - Specify that the IEEE 802.3 Snap protocol will be used. **ieee802.3_llc** - Specify that the IEEE 802.3 LLC protocol will be used. **<protocol_value>** - Enter the protocol value here.
delete - Specify 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. **ieee802.3_snap** - Specify that the IEEE 802.3 Snap protocol will be used. **ieee802.3_llc** - Specify 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-3000-28SC: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-3000-28SC:admin#
```

71-3 delete dot1v_protocol_group

Description

This command is used to delete a protocol group.

Format

delete dot1v_protocol_group [group_id <int 1-16> | group_name <name 32> | all]

Parameters

group_id - Specify the group ID to be deleted. **<int 1-16>** - Enter the group ID used here.
group_name - Specify 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 - Specify 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-3000-28SC:admin#delete dot1v_protocol_group group_id 100
Command: delete dot1v_protocol_group group_id 100

Success.

DGS-3000-28SC:admin#
```

71-4 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 <int 1-16> | group_name <name 32>]}

Parameters

group_id - (Optional) Specify the ID of the group to be displayed. **<int 1-16>** - Enter the group ID used here.
group_name - (Optional) Specify 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 100:

```
DGS-3000-28SC:admin#show dot1v_protocol_group group_id 100
Command: show dot1v_protocol_group group_id 100

Protocol Group ID Protocol Group Name              Frame Type     Protocol Value
----------------- -------------------------------- -------------- --------------
10                General_Group                    EthernetII     86dd

Total Entries: 1

DGS-3000-28SC:admin#
```

71-5 config port dot1v ports

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 prority 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 <int 1-16> | group_name <name 32>] [vlan <vlan_name 32> | vlanid <id>] {priority <value0-7>} | delete protocol_group [group_id <int 1-16> | all]]

Parameters

<portlist> - Enter a list of ports used for the configuration here.
all - Specify that all the ports will be used for this configuration.
add - Specify that the group specified will be added. **protocol_group** - Specify that parameters for the group will follow. **group_id** - Specify the group ID of the protocol group. **<int 1-16>** - Enter the group ID used here. **group_name** - Specify 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** - Specify the VLAN ID. **<id>** - Enter the VLAN ID used here. **priority** - (Optional) Specify 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 - Specify that the group specified will be deleted. **protocol_group** - Specify that parameters for the group will follow. **group_id** - Specify the group ID of the protocol group. **<int 1-16>** - Enter the group ID used here. **all** - Specify 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 untaged IPv6 packet ingress from port 3.

To configure the group ID 10 on port 3 to be associated with VLAN marketing-1:

```
DGS-3000-28SC: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-3000-28SC:admin#
```

71-6 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) Specify 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-3000-28SC: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-3000-28SC:admin#
```

Chapter 72 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 <hex0x1-0xffff> | use_inner_priority [enable | disable] | add_inner_tag [<hex0x1-0xffff> | disable] | [add | delete] vlan_translation_profile <profile_id>}(1)
config vlan_translation_profile <profile_id> add rule_id {<rule_id>} [add svid <vlanid 1-4094> {priority <priority 0-7>} classify {source_mac <macaddr> {sa_mask <macmask>} | destination_mac <macaddr> {da_mask <macmask>} | source_ipv4 <ipaddr> {sip_mask <netmask>} | destination_ipv4 <ipaddr> {dip_mask <netmask>} | outer_vid <vidlist> | 802.1p <priority 0-7> | ip_protocol <value 0-255> | l4_src_port <value 1-65535> | l4_dest_port <value 1-65535>} | replace svid <vlanid 1-4094> {priority <priority 0-7>} classify outer_vid <vlanid 1-4094> {source_mac <macaddr> {sa_mask <macmask>} | destination_mac <macaddr> {da_mask <macmask>} | source_ipv4 <ipaddr> {sip_mask <netmask>} | destination_ipv4 <ipaddr> {dip_mask <netmask>} | 802.1p <priority 0-7> | ip_protocol <value 0-255> | l4_src_port <value 1-65535> | l4_dest_port <value 1-65535>}]
create vlan_translation_profile <profile_id>
show qinq
show qinq inner_tpid
show qinq ports {<portlist>}
create vlan_translation ports [<portlist> | all] [add cvid <vidlist> | replace cvid <vlanid 1-4094>] svid <vlanid 1-4094> {priority <priority 0-7>}
delete vlan_translation ports [<portlist> | all] {cvid <vidlist>}
delete vlan_translation_profile [<profile_id> | all] { rule_id [<rule_id_list> | all]}
show vlan_translation {[ports <portlist> | cvid <vidlist>]}
show vlan_translation_profile {<profile_id_list>}

72-1 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-3000-28SC:admin#enable qinq
Command: enable qinq

Success.

DGS-3000-28SC:admin#
```

72-2 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-3000-28SC:admin#disable qinq
Command: disable qinq

Success.

DGS-3000-28SC:admin#
```

72-3 config qinq inner_tpid

Description

This command is used to configure the inner TPID of the system. The inner TPID is used to decide if the ingress packet is c-tagged. Inner tag TPID is per system configurable.

Format

config qinq inner_tpid <hex 0x1-0xffff>

Parameters

<hex 0x1-0xffff> - Enter the inner-TPID of the system here.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the inner TPID in the system to 0x9100:

```
DGS-3000-28SC:admin#config qinq inner_tpid 0x9100
Command: config qinq inner_tpid 0x9100

Success.

DGS-3000-28SC:admin#
```

72-4 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 <hex0x1-0xffff> | use_inner_priority [enable | disable] | add_inner_tag [<hex0x1-0xffff> | disable] | [add | delete] vlan_translation_profile <profile_id>}(1)

Parameters

<portlist> - Enter the list of ports to be configured here.
all - Specify that all the ports will be used for the configuration.
role - Specify the port role in QinQ mode. **nni** - Specify that the port is connecting to the service provider network. **uni** - Specify that the port is connecting to the customer network.
missdrop - Specify the state of the miss drop of ports option. **enable** - Specify that the miss drop of ports option will be enabled. **disable** - Specify that the miss drop of ports option will be disabled.
outer_tpid - Specify the outer-TPID of a port. **<hex 0x1 - 0xffff>** - Enter the outer-TPID value used here.
use_inner_priority – Specify the inner priority tag. **enable** - Specify the inner priority tag to be enabled. **disable** - Specify the inner priority tag to be disabled
add_inner_tag - Specify 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** - Specify that the add inner tag option will be disabled.
add - Specify to add a QinQ port parameter. **delete** - Specify to delete a QinQ port parameter. **vlan_translation_profile** - Specify the VLAN translation profile here. **<profile_id>** - Enter the profile ID for the VLAN translation profile here.

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-3000-28SC:admin#config qinq ports 1-4 role nni outer_tpid 0x88A8
Command: config qinq ports 1-4 role nni outer_tpid 0x88A8

Success.

DGS-3000-28SC:admin#
```

72-5 config vlan_translation_profile

Description

This command is used to configure a flow-based Q-in-Q translation rule. The S-VLAN assignment may be based on source MAC, destination MAC, 802.1p priority, source IP, destination IP, outer VID, etc. Flow-based VLAN translation rules indicate which S-VLAN will be assigned for matched packets and will indicate whether to add an S-Tag or replace the C-Tag by S-Tag. Each Q-in-Q rule has a priority. The rules of lower profile ID have higher priority, while in in the same profile, the rule which has the lower access ID has higher priority.

Format

config vlan_translation_profile <profile_id> add rule_id {<rule_id>} [add svid <vlanid 1-4094> {priority <priority 0-7>} classify {source_mac <macaddr> {sa_mask <macmask>} | destination_mac <macaddr> {da_mask <macmask>} | source_ipv4 <ipaddr> {sip_mask <netmask>} | destination_ipv4 <ipaddr> {dip_mask <netmask>} | outer_vid <vidlist> | 802.1p <priority 0-7> | ip_protocol <value 0-255> | l4_src_port <value 1-65535> | l4_dest_port <value 1-65535>} | replace svid <vlanid 1-4094> {priority <priority 0-7>} classify outer_vid <vlanid 1-4094> {source_mac <macaddr> {sa_mask <macmask>} | destination_mac <macaddr> {da_mask <macmask>} | source_ipv4 <ipaddr> {sip_mask <netmask>} | destination_ipv4 <ipaddr> {dip_mask <netmask>} | 802.1p <priority 0-7> | ip_protocol <value 0-255> | l4_src_port <value 1-65535> | l4_dest_port <value 1-65535>}]

Parameters

<profile_id> - Specify the profile ID number to be configured.
add rule_id - Specify the rule ID to be added to the profile. If the rule ID is not specified, it will be assigned automatically. **<rule_id>** - (Optional) Specify the rule ID to be added to the profile.
add svid - The action indicates to add a tag for the assigned S-VLAN before the Outer-VLAN tag. If there is an S-TAG in the packet, this rule will not take effect.

<vlanid 1-4094> - Specify the VLAN ID between 1 and 4094.
priority - (Optional) Specify a value for priority between 0 and 7.
<priority 0-7> - Specify a value for priority between 0 and 7.
classify - Specify to classify by key(this is a flexible way that can assign S-Tag based on source MAC address, destination MAC address, Outer-VID, 802.1P priority, source IP address, destination IP address, IP L4 source port number, and IP L4 destination port number).
source_mac - (Optional) Specify source MAC address for match.
<macaddr> - Specify the MAC address.
sa_mask - (Optional) Specify the source address mask.
<macmask> - Specify the source address mask.

destination_mac - Specify destination MAC address for match.
<macaddr> - Specify the MAC address.
da_mask - (Optional) Specify the destination mask.
<macmask> - Specify the destination mask.

source_ipv4 - Specify source IPv4 address or IPv4 subnet for match.
<ipaddr> - Specify source IPv4 address.
sip_mask - (Optional) Specify the SIP mask.
<netmask> - Specify the SIP mask.

destination_ipv4 - Specify destination IPv4 address or IPv4 subnet for match.
<ipaddr> - Specify destination IPv4 address.
dip_mask - (Optional) Specify the DIP mask.
<netmask> - Specify the DIP mask.

outer_vid - Specify packet's Outer-VID for match.
<vidlist> - Specify a range of VLAN IDs.

802.1p - Specify packet's 802.1p priority for match.
<priority 0-7> - Specify a value between 0 and 7.

ip_protocol - Specify the IP protocol.
<value 0-255> - Specify a value between 0 and 255.

l4_src_port - Specify the l4 source port ID for match.
<value 1-65535> - Specify a value between 1 and 65535.

l4_dest_port - Specify the l4 destination port ID for match.
<value 1-65535> - Specify a value between 1 and 65535.

replace svid - The action indicates to replace the Outer-VLAN ID in the tag by the SVID. If there is no TAG in the packet, this rule will not take effect.
<vlanid 1-4094> - Specify the VLAN ID between 1 and 4094.
priority - (Optional) Specify a value for priority between 0 and 7.
<priority 0-7> - Specify a value for priority between 0 and 7.
classify outer_vid - Specify to classify by Outer-VID.
<vlanid 1-4094> - Specify the VLAN ID between 1 and 4094.
source_mac - (Optional) Specify source MAC address for match.
<macaddr> - Specify the MAC address.
sa_mask - (Optional) Specify the source address mask.
<macmask> - Specify the source address mask.
destination_mac - (Optional) Specify destination MAC address for match.
<macaddr> - Specify the MAC address.
da_mask - (Optional) Specify the destination mask.
<macmask> - Specify the destination mask.
source_ipv4 - (Optional) Specify source IPv4 address or IPv4 subnet for match.
<ipaddr> - Specify source IPv4 address.
sip_mask - (Optional) Specify the SIP mask.
<netmask> - Specify the SIP mask.
destination_ipv4 - (Optional) Specify destination IPv4 address or IPv4 subnet for match.
<ipaddr> - Specify destination IPv4 address.
dip_mask - (Optional) Specify the DIP mask.
<netmask> - Specify the DIP mask.
802.1p - (Optional) Specify packet's 802.1p priority for match.
<priority 0-7> - Specify a value between 0 and 7.
ip_protocol - (Optional) Specify the IP protocol.
<value 0-255> - Specify a value between 0 and 255.

l4_src_port - (Optional) Specify the l4 source port ID for match.
<value 1-65535> - Specify a value between 1 and 65535.
l4_dest_port - (Optional) Specify the l4 destination port ID for match.
<value 1-65535> - Specify a value between 1 and 65535.

Restrictions

Only Administrators, and Operators can issue this command.

Example

To configure a flow-based Q-in-Q translation rule:

```
DGS-3000-28SC:admin# config vlan_translation_profile 2 add rule 3 add svid 100
classify outer_vid 1-1000
Command: config vlan_translation_profile 2 add rule 3 add svid 100 classify
outer_vid 1-1000

Success.

DGS-3000-28SC:admin#
```

To add an S-Tag in which the S-VID is 100 to the ingress packets of Port 3 if packet's C-VID is 10, MAC-SA is 00:00:00:11:22:33, Ether-type is 0x8000, SIP is 10.10.10.10, Priority is 2, and the port number of IPv4 is 1813:

Note: First create a VLAN translation profile named 3 before doing the configuration below and then add Q-in-Q port 3 to the profile.

```
DGS-3000-28SC:admin# config vlan_translation_profile 3 add rule_id 4 add svid
100 classify source_mac 00:00:00:11:22:33 source_ipv4 10.10.10.10 802.1p 2
ip_protcol 0x8000 l4_dest_port 1813 outer_vid 10
Command: config vlan_translation_profile 3 add rule_id 4 add svid 100 classify
source_mac 00:00:00:11:22:33 source_ipv4 10.10.10.10 802.1p 2 ip_protcol 0x8000
l4_dest_port 1813 outer_vid 10

Success.

DGS-3000-28SC:admin#
```

72-6 create vlan_translation_profile

Description

This command is used to create Q-in-Q flow- based VLAN translation profiles. Multiple flow-based VLAN translation rules can be specified for a profile.

Format

create vlan_translation_profile <profile_id>

Parameters

<profile_id> - Specify the ID number of the profile.

Restrictions

Only Administrators and Operators can issue this command.

Example

To create Q-in-Q profile 2:

```
DGS-3000-28SC:admin# create vlan_translation_profile 2
Command: create vlan_translation_profile 2

Success.

DGS-3000-28SC:admin#
```

72-7 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-3000-28SC:admin#show qinq
Command: show qinq

 QinQ Status : Enabled

DGS-3000-28SC:admin#
```

72-8 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-3000-28SC:admin#show qinq inner_tpid
Command: show qinq inner_tpid

 Inner TPID: 0x9100


DGS-3000-28SC:admin#
```

72-9 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-3000-28SC: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-3000-28SC:admin#
```

72-10 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 - Specify that all the ports will be used for the configuration.
add - Specify to add an S-Tag to the packet. **cvid** - Specify the customer VLAN ID used. **<vidlist>** - Enter the customer VLAN ID used here.
replace - Specify to replace the C-Tag with the S-Tag. **cvid** - Specify the customer VLAN ID used. **<vlanid 1-4094>** - Enter the customer VLAN ID used here.
svid - Specify the service provider VLAN ID used. **<vlanid 1-4094>** - Enter the service provider VLAN ID used here.
priority - (Optional) Specify 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-3000-28SC:admin#create vlan_translation ports 1 replace cvid 20 svid 200
Command: create vlan_translation ports 1 replace cvid 20 svid 200

Success.

DGS-3000-28SC: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-3000-28SC:admin#create vlan_translation ports 1 add cvid 30 svid 300
Command: create vlan_translation ports 1 add cvid 30 svid 300

Success.

DGS-3000-28SC:admin#
```

72-11 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 - Specify that all the ports will be used for the configuration.
cvid - (Optional) Specify 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-3000-28SC:admin#delete vlan_translation ports 1-4
Command: delete vlan_translation ports 1-4

Success.

DGS-3000-28SC:admin#
```

72-12 delete vlan_translation_profile

Description

This command is used to delete translation relationships between the C-VLAN and the S-VLAN.

Format

delete vlan_translation_profile [<profile_id> | all] {rule_id [<rule_id_list> | all]}

Parameters

<profile_id> - Enter the profile ID here.
all - Specify that all the ports will be used for the configuration.
rule_id - (Optional) Specify the rules for the specified CVIDs. If the CVID is not specified, all rules configured for the port will be deleted. **<rule_id_list>** - Enter the rule ID list value here. **all** - Specify to delete all the ports that will be used for the configuration.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete a VLAN translation profile on all ports:

```
DGS-3000-28SC:admin#delete vlan_translation_profile all
Command: delete vlan_translation_profile all

Success.

DGS-3000-28SC:admin#
```

72-13 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) Specify a list of ports to be displayed. **<portlist>** - Enter the list of ports to be displayed here.
cvid - (Optional) Specify 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-3000-28SC: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-3000-28SC:admin#
```

72-14 show vlan_translation_profile

Description

This command is used to display the VLAN translation profile.

Format

show vlan_translation_profile {<profile_id_list>}

Parameters

<profile_id_list> - (Optional) Enter the profile ID list here.

Restrictions

None.

Example

To show the VLAN translation profile:

```
DGS-3000-28SC:admin#show vlan_translation_profile
Command: show vlan_translation_profile

Port    CVID       SPVID      Action    Priority
-----   --------   --------   -------   ---------
1       20         200        Replace   -
1       30         300        Add       -

 Total Entries: 2

DGS-3000-28SC:admin#
```

Chapter 73 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>]}(1)
show bandwidth_control {<portlist>}
config per_queue bandwidth_control {ports [<portlist> | all]} <cos_id_list> {{min_rate [no_limit | <value 64-10240000>]} max_rate [no_limit | <value 64-10240000>]}(1)
show per_queue bandwidth_control {<portlist>}
config scheduling {ports [<portlist> | all]} <class_id 0-7> [strict | weight <value 1-127>]
config scheduling_mechanism {ports [<portlist> | all]} [strict | wrr]
show scheduling {<portlist>}
show scheduling_mechanism {<portlist>}
config 802.1p user_priority <priority 0-7> <class_id 0-7>
show 802.1p user_priority
config 802.1p default_priority [<portlist> | all] <priority 0-7>
show 802.1p default_priority {<portlist>}
enable hol_prevention
disable hol_prevention
show hol_prevention
config 802.1p map {[<portlist> | all]} 1p_color <priority_list> to [green | red | yellow]
show 802.1p map 1p_color {<portlist>}
config dscp trust [<portlist> | all] state [enable | disable]
show dscp trust {<portlist>}
config dscp map {[<portlist> | all]} [dscp_priority <dscp_list> to <priority 0-7> | dscp_dscp <dscp_list> to <dscp 0-63> | dscp_color <dscp_list> to [green | red | yellow]]
show dscp map {<portlist>} [dscp_priority | dscp_dscp | dscp_color] {dscp <dscp_list>}

73-1 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>]}(1)

Parameters

<portlist> - Enter a range of ports to be configured.
all - Specify that all the ports will be used for this configuration.
rx_rate - Specify 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 - Specify 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-3000-28SC:admin#config bandwidth_control 1-10 tx_rate 100
Command: config bandwidth_control 1-10 tx_rate 100

Granularity: RX: 64, TX: 64. Actual Rate: TX: 64.

Success

DGS-3000-28SC:admin#
```

73-2 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) Enter 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-3000-28SC:admin#show bandwidth_control 1-10
Command: show bandwidth_control 1-10

Bandwidth Control Table

 Port   RX Rate       TX Rate       Effective RX       Effective TX
        (Kbit/sec)    (Kbit/sec)    (Kbit/sec)         (Kbit/sec)
 -----  ----------    ----------    ----------------   ----------------
 1      No Limit      64                 -                  -
 2      No Limit      64                 -                  -
 3      No Limit      64                 -                  -
 4      No Limit      64                 -                  -
 5      No Limit      64                 -                  -
 6      No Limit      64                 -                  -
 7      No Limit      64                 -                  -
 8      No Limit      64                 -                  -
 9      No Limit      64                 -                  -
 10     No Limit      64                 -                  -

DGS-3000-28SC:admin#
```

73-3 config per_queue bandwidth_control

Description

This command is used to configure per port CoS bandwidth control.

Format

config per_queue bandwidth_control {ports [<portlist> | all]} <cos_id_list 0-7> {{min_rate [no_limit | <value 64-10240000>]} max_rate [no_limit | <value 64-10240000>]}(1)

Parameters

ports - (Optional) Specify 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.
<cos_id_list 0-7> - Enter a list of priority queues. The priority queue number is ranged from 0 to 7.
min_rate - (Optional) Specify 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** - Specify that there will be no limit on the rate of packets received by the above specified class. **<value 64-10240000>** - Enter 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 - Specify 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** - Specify that there will be no limit on the rate of packets received by the above specified class.

<value 64-10240000> - Enter 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-3000-28SC:admin#config per_queue bandwidth_control ports 1-10 1 min_rate
130 max_rate 1000
Command: config per_queue bandwidth_control ports 1-10 1 min_rate 130 max_rate
1000

 Granularity: TX: 64. Actual Rate: MIN: 128, MAX: 960.

Success.

DGS-3000-28SC:admin#
```

73-4 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) Enter 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-3000-28SC: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-3000-28SC:admin#
```

73-5 config scheduling

Description

This command is used to configure the traffic scheduling mechanism for each CoS queue.

Format

config scheduling {ports [<portlist> | all]} <class_id 0-7> [strict | weight <value 1-127>]

Parameters

ports – (Optional) Specify a range of ports to be configured. **<portlist>** - Enter the list of port used for this configuration here. **all** – Specify all the ports to be configured.
<class_id 0-7> - Enter 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 - Specify 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-3000-28SC:admin#config scheduling ports 10 1 weight 25
Command: config scheduling ports 10 1 weight 25

Success.

DGS-3000-28SC:admin#
```

73-6 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]

Parameters

ports - (Optional) Specify a range of ports to be configured. **<portlist>** - Enter the list of port used for this configuration here. **all** - Specify 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.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the traffic scheduling mechanism for each CoS queue:

```
DGS-3000-28SC:admin#config scheduling_mechanism strict
Command: config scheduling_mechanism strict

Success.

DGS-3000-28SC:admin#
```

To configure the traffic scheduling mechanism for CoS queue on port 1:

```
DGS-3000-28SC:admin#config scheduling_mechanism ports 1 strict
Command: config scheduling_mechanism ports 1 strict

Success.

DGS-3000-28SC:admin#
```

73-7 show scheduling

Description

This command is used to display the current traffic scheduling parameters.

Format

show scheduling {<portlist>}

Parameters

<portlist> - (Optional) Enter a range of ports to be displayed.
If no parameter is 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-3000-28SC: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-3000-28SC:admin#
```

73-8 show scheduling_mechanism

Description

This command is used to show the traffic scheduling mechanism.

Format

show scheduling_mechanism {<portlist>}

Parameters

<portlist> - (Optional) Enter a range of ports to be displayed.
If no parameter is specified, system will display all ports scheduling mechanism configurations.

Restrictions

None.

Example

To show scheduling mechanism:

```
DGS-3000-28SC: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-3000-28SC:admin#
```

73-9 config 802.1p user_priority

Description

This command is used to map the 802.1p user priority of an incoming packet to one of the eight hardware queues available on the Switch.

Format

config 802.1p user_priority <priority 0-7> <class_id 0-7>

Parameters

<priority 0-7> - Enter a priority class value to associate with.
<class_id 0-7> - Enter the Switch's class hardware priority queue ID. 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-3000-28SC:admin#config 802.1p user_priority 1 3
Command: config 802.1p user_priority 1 3

Success.

DGS-3000-28SC:admin#
```

73-10 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-3000-28SC: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-3000-28SC:admin#
```

73-11 config 802.1p default_priority

Description

This command is used to configure the 802.1p default priority settings on the Switch. If an untagged packet is received by the Switch, the priority configured with this command will be written to the packet's priority field.

Format

config 802.1p default_priority [<portlist> | all] <priority 0-7>

Parameters

<portlist> - Enter a range of ports for which the default priority is to be configured. That is, a range of ports for which all untagged packets received will be assigned the priority specified below. The port list is specified by listing the beginning port number on the Switch, separated by a colon. Then highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash.
all - Specify that the command apply to all ports on the Switch.
<priority 0-7> - Enter the priority value (0 to 7) assigned to untagged packets received by the Switch or a range of ports on the Switch.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the 802.1p default priority settings on the Switch:

```
DGS-3000-28SC:admin#config 802.1p default_priority all 5
Command: config 802.1p default_priority all 5

Success.

DGS-3000-28SC:admin#
```

73-12 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) Enter 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-3000-28SC: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-3000-28SC:admin#
```

73-13 enable hol_prevention

Description

This command is used to enable head of line prevention on the Switch.

Format

enable hol_prevention

Parameters

None.

Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

Example

To enable HOL prevention on the Switch:

```
DGS-3000-28SC:admin# enable hol_prevention
Command: enable hol_prevention

Success.

DGS-3000-28SC:admin#
```

73-14 disable hol_prevention

Description

This command is used to disable head of line prevention on the Switch.

Format

disable hol_prevention

Parameters

None.

Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

Example

To disable HOL prevention on the Switch:

```
DGS-3000-28SC:admin# disable hol_prevention
Command: disable hol_prevention

Success.

DGS-3000-28SC:admin#
```

73-15 show hol_prevention

Description

This command is used to display head of line prevention state on the Switch.

Format

show hol_prevention

Parameters

None.

Restrictions

None.

Example

To display HOL prevention state on the Switch.

```
DGS-3000-28SC:admin# show hol_prevention
Command: show hol_prevention

Device HOL Prevention State: Enabled

DGS-3000-28SC:admin#
```

73-16 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 - Specify that the command apply to all ports on the Switch.
state - Specify to enable or disable to trust DSCP. By default, DSCP trust is disabled. **enable** - Specify to enable the DSCP trust state. **disable** - Specify 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-3000-28SC:admin#config dscp trust 1-8 state enable
Command: config dscp trust 1-8 state enable

Success.

DGS-3000-28SC:admin#
```

73-17 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) Specify that the command apply to all ports on the Switch.
1p_color - The list of source priority for imcoming packets. **<priority_list>** - Enter the list of source priority for imcoming packets.
to - The mapped color for a packet.

green - Specify green as the mapped color. **red** - Specify red as the mapped color. **yellow** - Specify 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-3000-28SC: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-3000-28SC:admin#
```

73-18 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) Enter a list of ports.

Restrictions

None.

Example

To show the 802.1p color mapping on port 1:

```
DGS-3000-28SC:admin#show 802.1p map 1p_color 1
Command: show 802.1p map 1p_color 1

802.1p to Color Mapping:
-------------------------------------------------------------
Port 0      1      2      3      4      5      6      7
---- ------ ------ ------ ------ ------ ------ ------ ------
1    Green  Green  Green  Green  Green  Green  Green  Green

DGS-3000-28SC:admin#
```

73-19 show dscp trust

Description

This command is used to display DSCP trust state for the specified ports on the Switch.

Format

show dscp trust {<portlist>}

Parameters

<portlist> - (Optional) A range of ports to display.
If no port is specified, all ports for DSCP trust status on the Switch will be displayed.

Restrictions

None.

Example

Display DSCP trust status on ports 1-8.

```
DGS-3000-28SC: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-3000-28SC:admin#
```

73-20 config dscp map

Description

This command is used to configure DSCP mapping. The mapping of DSCP to priority will be used to determine the priority of the packet (which will be then used to determine the scheduling queue) when the port is in DSCP trust state.

The mapping of DSCP to color will be used to determine the initial color of the packet when the policing function of the packet is color aware and the packet is DSCP-trusted.

The DSCP-to-DSCP mapping is used in the swap of DSCP of the packet when the packet is ingresses to the port. The remaining processing of the packet will base on the new DSCP. By default, the DSCP is mapped to the same DSCP.

These DSCP mapping will take effect at the same time when IP packet ingress from a DSCP-trusted port.

Format

config dscp map {[<portlist> | all]} [dscp_priority <dscp_list> to <priority 0-7> | dscp_dscp <dscp_list> to <dscp 0-63> | dscp_color <dscp_list> to [green | red | yellow]]

Parameters

<portlist> - (Optional) Enter the list of port used for this configuration here.
all – (Optional) Specify that all the ports will be included in this configuration.
dscp_priority - Specify a list of DSCP value to be mapped to a specific priority. **<dscp_list>** - Enter the DSCP priority list here. **to** - Specify that the above or following parameter will be mapped to the previously mentioned parameter. **<priority 0-7>** - Enter the result priority of mapping.
dscp_dscp - Specify a list of DSCP value to be mapped to a specific DSCP. **<dscp_list>** - Enter the DSCP to DSCP list here. **to** - Specify that the above or following parameter will be mapped to the previously mentioned parameter. **<dscp 0-63>** - Enter the result DSCP of mapping.
dscp_color - Specify a list of DSCP value to be mapped to a specific color. **<dscp_list>** - Enter the DSCP to color list here. **to** - Specify that the above or following parameter will be mapped to the previously mentioned parameter. **green** - Specify the result color of mapping to be green. **red** - Specify the result color of mapping to be red. **yellow** - Specify 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-3000-28SC:admin#config dscp map 1-8 dscp_priority 1 to 1
Command: config dscp map 1-8 dscp_priority 1 to 1

Success.

DGS-3000-28SC:admin#
```

To configure the global mapping of the DSCP priority to priority 1:

```
DGS-3000-28SC:admin#config dscp map dscp_priority 1 to 1
Command: config dscp map dscp_priority 1 to 1

Success.

DGS-3000-28SC:admin#
```

73-21 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) Enter a range of ports to show. If no port is specified, all ports' DSCP mapping will be displayed.
dscp_priotity - Specify a list of DSCP value to be mapped to a specific priority.
dscp_dscp - Specify a list of DSCP value to be mapped to a specific DSCP.
dscp_color - Specify a list of DSCP value to be mapped to a specific color.
dscp - (Optional) This Specify 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-3000-28SC: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-3000-28SC:admin#
```

Chapter 74 RADIUS Client Command List

config radius add <server_index 1-3> [<server_ip> | <ipv6addr>] [key <password 32> | encryption_key <password 56>] [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> | encryption_key <password 56>] | 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

74-1 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> | encryption_key <password 56>] [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.
encryption_key - Specify the key pre-negotiated between the switch and the RADIUS server. It is used to encrypt the user's authentication data before being transmitted over the Internet. **<password 56>** - Enter the enryption key.
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 - Specify 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 - Specify 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-3000-28SC: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-3000-28SC:admin#
```

74-2 config radius delete

Description

This command is used to delete a RADIUS server.

Format

config radius delete <server_index 1-3>

Parameters

<server_index 1-3> - Enter 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-3000-28SC:admin#config radius delete 1
Command: config radius delete 1

Success.

DGS-3000-28SC:admin#
```

74-3 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> | encryption_key <password 56>] | auth_port [<udp_port_number 1-65535> | default] | acct_port [<udp_port_number 1-65535> | default] | timeout [<sec 1-255> | default] | retransmit [<int 1-20> | default]}(1)

Parameters

<server_index 1-3> - Enter the RADIUS server index here. This value must be between 1 and 3.
ipaddress - 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.
encryption_key - Specify the key pre-negotiated between the switch and the RADIUS server. It is used to encrypt the user's authentication data before being transmitted over the Internet. **<password 56>** - Enter the enryption key.
auth_port - Specify 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** - Specify that the default port number will be used.
acct_port - Specify 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** - Specify 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** - Specify 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** - Specify 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-3000-28SC:admin#config radius 1 auth_port 60
Command: config radius 1 auth_port 60

Success.

DGS-3000-28SC:admin#
```

74-4 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-3000-28SC:admin#show radius
Command: show radius

Index  IP Address      Auth-Port Acct-Port Timeout Retransmit Key
                                           (sec)
-----  --------------- --------- --------- ------- ---------- ----------------
1      10.48.74.121    60        1813      5       2          dlink


Total Entries : 1

DGS-3000-28SC:admin#
```

74-5 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-3000-28SC: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-3000-28SC:admin#
```

74-6 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-3000-28SC: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-3000-28SC:admin#
```

Chapter 75 Remote Copy Protocol (RCP) Command List

download firmware_fromRCP [{username <username>} {<ipaddr>} src_file <path_filename 64> |rcp: <string 128>] {[unit <unit_id 1-6> | all]} {dest_file <pathname>} {boot_up}
upload firmware_toRCP [{username <username>} {<ipaddr>} dest_file <path_filename 64> | rcp: <string 128>] {unit <unit_id 1-6>} {src_file <pathname>}
download cfg_fromRCP [{ username <username>} {<ipaddr>} src_file <path_filename 64> | rcp: <string 128>] {[unit <unit_id 1-6> | all]} {dest_file <pathname>}
upload cfg_toRCP [{username <username>} {<ipaddr>} dest_file <path_filename 64> | rcp: <string 128>] {unit <unit_id 1-6>} {src_file <pathname>} {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}} {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}} {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}}}}}
upload log_toRCP [{username <username>} {<ipaddr>} dest_file <path_filename 64> | rcp: <string128>]
upload attack_log_toRCP [{username <username>} {<ipaddr>} dest_file <path_filename 64> | rcp: <string 128>] {unit <unit_id 1-6>}
config rcp server {ipaddress <ipaddr> | username <username>}(1)
config rcp server clear [ipaddr | username | both]
show rcp server

75-1 download firmware_fromRCP

Description

This command is used to download a firmware file from a Remote Copy Protocol (RCP) server.

Format

download firmware_fromRCP [{username <username>} {<ipaddr>} src_file <path_filename 64> | rcp: <string 128>] {[unit <unit_id 1-6> | all]} {dest_file <pathname>} {boot_up}

Parameters

username - (Optional) Specify the remote user name on the RCP server. **<username>** - Enter the remote user name on the RCP server.
<ipaddr> - (Optional) Enter the IP address of the RCP server.
src_file - Specify the path name on the RCP server or local. **<path_filename 64>** - Enter the path name on the RCP server or local.
rcp: - Specify the path and the login credentials on the RCP server that will be used for the download. **<string 128 >** - Enter the path and the login credentials on the RCP server that will be used for the download. No spaces are allowed.
unit - (Optional) Specify the unit ID used. **<unit_id>** - Enter the unit ID here.
all - (Optional) Specify all unit ID's.
dest_file - (Optional) Specify the path and file name of the destination file on the device. **<pathname>** - Enter the path and file name of the destination file.
boot_up - Specify it as a boot-up file.

Restrictions

Only Administrators can issue this command.

Example

To download firmware from an RCP server:

```
DGS-3000-28SC:admin#download firmware_fromRCP username rcp_user 10.90.90.90
src_file /home/
Command: download firmware_fromRCP username rcp_user 10.90.90.90 src_file
/home/

Connecting to server.................. Done.
Download firmware..................... Done.   Do not power off !!
Please wait, programming flash......... Done.

DGS-3000-28SC:admin#
```

75-2 upload firmware_toRCP

Description

This command is used to upload firmware from this Switch to a Remote Copy Protocol (RCP) server.

Format

upload firmware_toRCP [{username <username>} {<ipaddr>} dest_file <path_filename 64> | rcp: <string128>] {unit <unit id1-6>} {src_file <pathname>}

Parameters

username - (Optional) Specify the remote user name on the RCP server. **<username>** - Enter the remote user name on the RCP server.
<ipaddr> - (Optional) Enter the IP address of the RCP server.
dest_file - Specify the path name on the RCP server. **<path_filename 64>** - Enter the path name on the RCP server.
rcp: - Specify the path and the login credentials on the RCP server that will be used for the upload. **<string128>** - Enter the path and the login credentials on the RCP server that will be used for the upload.
unit - (Optional) Specify the unit size. **<unit id1-6>** - Enter the unit ID number here. Choose option 1-6.
src_file - (Optional) Specify the path name of the source file. If not specified, the boot-up image on the device will be uploaded. **<pathname>** - Enter the path name of the source file.

Restrictions

Only Administrators can issue this command.

Example

To upload firmware image to an RCP server:

```
DGS-3000-28SC:admin#upload firmware_toRCP rcp:
rcp_user@172.18.212.106/firmware.had src_file 1.12.had
Command: upload firmware_toRCP rcp: rcp_user@172.18.212.106/firmware.had
src_file 1.12.had


Connecting to server.............. Done.
Upload firmware.................. Done.


DGS-3000-28SC:admin#
```

75-3 download cfg_fromRCP

Description

This command is used to download a configuration file from an RCP server.

Format

download cfg_fromRCP [{username <username>} {<ipaddr>} src_file <path_filename 64> | rcp: <string 128>] {[unit <unit_id 1-6> | all]} {dest_file <pathname>}

Parameters

username - (Optional) Specify the remote user name on the RCP server. **<username>** - Enter the remote user name on the RCP server.
<ipaddr> - (Optional) Enter the IP address of the RCP server.
src_file - Specify the path name on the RCP server or local. **<path_filename 64>** - Enter the path name on the RCP server or local.
rcp: - Specify the path and the login credentials on the RCP server that will be used for the download. **<string 128 >** - Enter the path and the login credentials on the RCP server that will be used for the download. No spaces are allowed.
unit - (Optional) Specify the unit ID used. **<unit_id 1-6>** - Enter the unit ID here.
all - (Optional) Specify all unit ID's.
dest_file - (Optional) Specify the path and file name of the destination file on the device. **<pathname >** - Enter the path and file name of the destination file.

Restrictions

Only Administrators can issue this command.

Example

To download a configuration file from an RCP server:

```
DGS-3000-28SC:admin# download cfg_fromRCP username rcp_user  172.18.212.106
src_file /home/DGS-3000-28SC.cfg
Command: download cfg_fromRCP username rcp_user  172.18.212.106 src_file
/home/DGS-3000-28SC.cfg

Connecting to server.................…. Done.
Download configuration................. Done.

DGS-3000-28SC:admin#
```

To download a configuration using an RCP string:

```
DGS-3000-28SC:admin# download cfg_fromRCP rcp:
rcp_user@172.18.212.106/home/DGS-3000-28SC.cfg config_id 1
Command: download cfg_fromRCP rcp: rcp_user@172.18.212.106/home/DGS-3000-
28SC.cfg config_id 1

Connecting to server.................. Done.
Download configuration................. Done.

DGS-3000-28SC:admin#
```

75-4 upload cfg_toRCP

Description

This command is used to upload a configuration file from the device to an RCP server. If the remote filename is not specified, the default file name will be modelname-image-id.

Format

upload cfg_toRCP [{username <username>} {<ipaddr>} dest_file <path_filename 64> | rcp: <string 128>] {unit <unit_id 1-6>} {src_file <pathname>} {[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

username - (Optional) Specify the remote user name on the RCP server. **<username>** - Enter the remote user name on the RCP server.
<ipaddr> - (Optional) Enter the IP address of the RCP server.
dest_file - Specify the path name on the RCP server. **<path_filename 64>** - Enter the path name on the RCP server or local RCP client.
rcp: - Specify the path and the login credentials of the configuration file located on the RCP server that will be used for the upload. **<string 128>** - Enter the path and the login credentials of the firmware file located on the RCP server that will be used for the upload. No spaces are allowed.
unit - (Optional) Specify which unit on the stacking system. If it is not specified, it refers to the master unit. **<unit_id 1-6>** - Enter the unit ID value. This value must be between 1 and 6.
src_file - (Optional) Specify the path name of the source file. **<pathname 64>** - Enter the path name of the source file. Note that if no path name is Specify, only the current device configuration will be uploaded.

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> - Enter a filter string enclosed by the quotation mark symbol. Thus, the filter string itself cannot contain the quotation mark character. The filter string is case sensitive.
<filter_string 80> - (Optional) Enter a filter string enclosed by the quotation mark symbol.
<filter_string 80> - (Optional) Enter a filter string enclosed by the quotation mark symbol.

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> - Enter a filter string enclosed by the quotation mark symbol. Thus, the filter string itself cannot contain the quotation mark character. The filter string is case sensitive.
<filter_string 80> - (Optional) Enter a filter string enclosed by the quotation mark symbol.
<filter_string 80> - (Optional) Enter a filter string enclosed by the quotation mark symbol.

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> - Enter a filter string enclosed by the quotation mark symbol. Thus, the filter string itself cannot contain the quotation mark character. The filter string is case sensitive.
<filter_string 80> - (Optional) Enter a filter string enclosed by the quotation mark symbol.
<filter_string 80> - (Optional) Enter a filter string enclosed by the quotation mark symbol.

Restrictions

Only Administrators can issue this command.

Example

To upload the current configuration from the device to an RCP server:

```
DGS-3000-28SC:admin# upload cfg_toRCP username rcp_user  172.18.212.104
dest_file /home/config.cfg
Command: upload cfg_toRCP username rcp_user  172.18.212.104 dest_file
/home/config.cfg

Connecting to server... Done.
Upload configuration... Done.

DGS-3000-28SC:admin#
```

To upload the configuration from a file system supported device to an RCP Server:

```
DGS-3000-28SC:admin# upload cfg_toRCP username rcp_user  172.18.212.104
dest_file /home/rcp_user/bone_switch.cfg src_file c:\config.cfg
Command: upload cfg_toRCP username rcp_user  172.18.212.104 dest_file
/home/rcp_user/bone_switch.cfg src_file c:\config.cfg

Connecting to server... Done.
Upload configuration... Done.

DGS-3000-28SC:admin#
```

75-5 upload log_toRCP

Description

This command is used to upload a log file from the device to a Remote Copy Protocol (RCP) server.

Format

upload log_toRCP [{username <username>} {<ipaddr>} dest_file <path_filename 64> | rcp: <string 128>]

Parameters

username - (Optional) Specify the remote user name on the RCP server. **<username>** - Enter the remote user name on the RCP server.
<ipaddr> - (Optional) Enter the IP address of the RCP server.
dest_file - Specify the path name of the RCP server. **<path_filename 64>** - Enter the path name of the RCP server.
rcp - Specify the path name on the RCP server. **<string 128>** - Enter the path name on the RCP server.

Restrictions

Only Administrators can issue this command.

Example

To upload the log from the device to an RCP server:

```
DGS-3000-28SC:admin#upload log_toRCP rcp_user 172.18.212.104 dest_file
/home/system-log.log
Command: upload log_toRCP rcp_user 172.18.212.104 dest_file /home/system-
log.log

Connecting to server... Done.
Upload log.............. Done.

DGS-3000-28SC:admin#
```

To upload log from the device to an RCP server using an RCP string:

```
DGS-3000-28SC:admin#upload log_toRCP rcp: rcp_user 172.18.212.104/home/system-
log.log
Command: upload log_toRCP rcp: rcp_user 172.18.212.104/home/system-log.log

Connecting to server... Done.
Upload log.............. Done.

DGS-3000-28SC:admin#
```

75-6 upload attack_log_toRCP

Description

This command is used to upload the attack log file from the device to an RCP server.

NOTE: If a user Specify the relative file path, the path search strategy will depend on the server system. For some systems, it will search the current user working directory first, and then search the environment paths.

Format

upload attack_log_toRCP [{username <username>} {<ipaddr>} dest_file <path_filename 64> | rcp: <string 128>] {unit <unit_id 1-6>}

Parameters

username - (Optional) Specify the remote user name on the RCP Server. **<username>** - Enter the remote username used here. This name can be up to 15 characters long.
<ipaddr> - (Optional) Enter the IP address used for the configuration here.
dest_file - Specify the destination file used. **<path_filename 64>** - Enter the pathname on the RCP server or local device.
rcp: - Specify the path of the log configuration file located on the RCP server that will be used for the upload. **<string 128>** - Enter the path and the login credentials of the firmware file located on the RCP server that will be used for the upload. No spaces are allowed. For example, user_name@10.1.1.1/home/user_name/firmware.had.
unit - (Optional) Specify which unit on the stacking system. If it is not specified, it refers to the master unit. **<unit_id 1-6>** - Enter the unit ID value. This value must be between 1 and 6.

Restrictions

Only Administrators can issue this command.

Example

To upload the attack log from the device to an RCP server:

```
DGS-3000-28SC:admin#  upload attack_log_toRCP username rcp_user 172.18.212.104
/home/attack-log.log
Command: upload attack_log_toRCP username rcp_user 172.18.212.104 /home/attack-
log.log


Connecting to server.......... Done.
Upload attack log.............. Done.


DGS-3000-28SC:admin#
```

75-7 config rcp server

Description

This command is used to configure Remote Copy Protocol (RCP) global server information. This global RCP server setting can be used when the server or remote user name is not specified. Only one RCP server can be configured for each system. If a user does not specify the RCP server in the CLI command, and the global RCP server was not configured, the switch will ask the user to input the server IP address or remote user name while executing the RCP commands.

Format

config rcp server {ipaddress <ipaddr> | username <username>}(1)

Parameters

ipaddress - Specify the IP address of the global RCP server. By default, the server is unspecified. **<ipaddr>** - Enter the IP address of the RCP server.
username - Specify the remote user name on the RCP server. **<username>** - Enter the remote user name on the RCP server.

Restrictions

Only Administrators can issue this command.

Example

To configure RCP global server information for the username “travel”:

```
DGS-3000-28SC:admin#config rcp server username travel
Command: config rcp server username travel

Success.

DGS-3000-28SC:admin#
```

75-8 config rcp server clear

Description

This command is used to clear Remote Copy Protocol (RCP) global server information.

Format

config rcp server clear [ipaddr | username | both]

Parameters

ipaddr - Clear the IP address of the RCP server.
username - Clear the username of the RCP server.
both - Clear both the IP address and the username of the RCP server.

Restrictions

Only Administrators can issue this command.

Example

To clear the current username of the RCP global server:

```
DGS-3000-28SC:admin#config rcp server clear username
Command: config rcp server clear username

Success.

DGS-3000-28SC:admin#
```

75-9 show rcp server

Description

This command is used to display Remote Copy Protocol (RCP) global server information.

Format

show rcp server

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To display RCP global server information:

```
DGS-3000-28SC:admin#show rcp server
Command: show rcp server

RCP Server Address        :
RCP Server Username       : travel

DGS-3000-28SC:admin#
```

Chapter 76 Route Command List

show ipfdb {[ip_address <ipaddr> | interface <ipif_name 12> | port <port>]}
create iproute [default | <network_address>] [<ipaddr> {<metric1-65535>} {[primary | backup]}
delete iproute [default | <network_address>] [<ipaddr>]
show iproute {<network_address> | <ipaddr>} {static | hardware}

76-1 show ipfdb

Description

This command is used to display the current network address forwarding database.

Format

show ipfdb {[ip_address <ipaddr> | interface <ipif_name 12> | port <port>]}

Parameters

ip_address - (Optional) Displays the specified host IP address. **<ipaddr>** - Enter the IP address used here.
interface - (Optional) Specify a IP interface. **<ipif_name 12>** - Enter the IP interface name here. This name can be up to 12 characters long.
port - (Optional) Specify a port. **<port>** - Enter the port number here.

Restrictions

None.

Example

To display network address forwarding table:

```
DGS-3000-28SC:admin# show ipfdb
Command: show ipfdb

Interface     IP Address       Port    Learned
------------  ---------------  ------  ---------
System        10.1.1.101       1:3    Dynamic
System        10.1.40.22       1:3    Dynamic
System        10.2.27.250      1:3    Dynamic

Total Entries: 3

DGS-3000-28SC:admin#
```

76-2 create iproute

Description

This command is used to create an IP route entry in the Switch's IP routing table. "Primary" and "backup" are mutually exclusive. Users can select only one when creating one new route. If a user sets neither of these, the system will try to set the new route first by primary and second by backup.

Format

create iproute [default | <network_address>] <ipaddr> {<metric 1-65535>} {[primary | backup]}

Parameters

default - Specify to create an IP default route (0.0.0.0/0).
network_address - Specify the IP address and net mask of the destination route. The address and the mask can be set using the traditional format (for example, 10.1.2.3/255.0.0.0) or in CIDR format (for example,10.1.2.3/16).
<ipaddr> - Enter the IP address for the IP route.
<metric 1-65535> - (Optional) Enter the routing protocol metric entry representing the number of routers between the Switch and the IP address above. The default setting is 1.
primary - (Optional) Specify the route as the primary route to the destination
backup - (Optional) Specify the route as the backup route to the destination.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To add an IP default route:

```
DGS-3000-28SC:admin# create iproute 10.48.74.121/255.0.0.0 10.1.1.254 primary
Command: create iproute 10.48.74.121/8 10.1.1.254 primary


DGS-3000-28SC:admin# create iproute 11.53.73.131/8 10.1.2.11
Command: Command: create iproute 11.53.73.131/8 10.1.2.11

Success.

DGS-3000-28SC:admin#
```

76-3 delete iproute

Description

This command is used to delete an IP route entry from the Switch's IP routing table.

Format

delete iproute [default | <network_address>] [<ipaddr>]

Parameters

default - Deletes an IP default route (0.0.0.0/0).
<network_address> - Enter the destination IP address and net mask route. The address and the mask can be set by the traditional format (for example, 10.1.2.3/255.0.0.0 or in CIDR format, 10.1.2.3/16).
<ipaddr> - Enter the next hop IP address route that needs to be deleted

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete an IP default route:

```
DGS-3000-28SC:admin# delete iproute 10.48.74.121/255.0.0.0 10.1.1.254
Command: delete iproute 10.48.74.121/8 10.1.1.254

Success.

DGS-3000-28SC:admin#
```

76-4 show iproute

Description

This command is used to display the switch's IP routing table.

Format

show iproute {<network_address> | <ipaddr>} {static | hardware}

Parameters

<network_address> - (Optional) Enter the destination network address of the route to be displayed.
<ipaddr> - (Optional) Enter the destination IP address of the route to be displayed. The longest prefix matched route will be displayed
static - (Optional) Specify to display only static routes. One static route may be active or inactive.
hardware - (Optional) Specify to display only the routes that have been written into the chip.

Restrictions

None.

Example

To display the contents of the IP routing table:

```
DGS-3000-28SC: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-3000-28SC:admin#show iproute static
Command: show iproute static


Routing Table

IP Address/Netmask  Gateway        Cost   Protocol  Backup    Status
------------------  -------------  -----  --------  --------  ------
0.0.0.0/0           10.1.1.11      1      Default   Primary   Active
100.1.1.0/24        10.1.1.11      1      Static    Primary   Active
101.1.1.0/24        10.1.1.12      1      Static    Primary   Inactive
102.1.1.0/24        tn1            1      Static    Primary   Inactive
103.1.1.0/24        tn2            1      Static    Primary   Active

Total Entries : 5

DGS-3000-28SC:admin#
```

Chapter 77 RPC PortMapper Command List

config filter rpc_portmapper [<portlist> | all] state [enable | disable]
show filter rpc_portmapper

77-1 config filter rpc_portmapper

Description

This command is used to configure the Switch to deny TCP/UDP packets with port number 135 on the network.

Format

config filter rpc_portmapper [<portlist> | all] state [enable | disable]

Parameters

<portlist> - Specify a list of ports to be configured for the RPC portmapper filter state.
all - Specify all ports to be configured for the RPC portmapper filter state.
state - Specify the RPC portmapper filter state. **enable** - Enable the RPC portmapper filter on specified ports. **disable** - Disable the RPC portmapper filter on specified ports.

Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

Example

To enable RPC portmapper filter on unit 1 port 1 to port 10:

```
DGS-3000-28SC:admin#config filter rpc_portmapper 1:1-1:10 state enable
Command: config filter rpc_portmapper 1:1-1:10 state enable

Success.

DGS-3000-28SC:admin#
```

77-2 show filter rpc_portmapper

Description

This command is used to display the RPC portmapper filter state on the Switch.

Format

show filter rpc_portmapper

Parameters

None.

Restrictions

None.

Example

To display the RPC portmapper state:

```
DGS-3000-28SC:admin#show filter rpc_portmapper
Command: show filter rpc_portmapper

 Enabled Ports: 1:1-1:10


DGS-3000-28SC:admin#
```

Chapter 78 RSPAN Command List

enable rspan
disable rspan
create rspan vlan [vlan_name <vlan_name> | vlan_id <vlanid 1-4094>]
delete rspan vlan [vlan_name <vlan_name> | vlan_id <vlanid 1-4094>]
config rspan vlan [vlan_name <vlan_name> | vlan_id <vlanid 1-4094>] [redirect [add | delete] ports <portlist> | source {[mirror_group_id <value 1-4> | [add | delete] ports<portlist> [rx | tx | both]]}]
show rspan {[vlan_name <vlan_name> | vlan_id <vlanid 1-4094>]}

78-1 enable rspan

Description

This command is used to enable all previously entered RSPAN configurations.

Format

enable rspan

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable all previously entered RSPAN configurations:

```
DGS-3000-28SC:admin#enable rspan
Command: enable rspan

Success.

DGS-3000-28SC:admin#
```

78-2 disable rspan

Description

This command is used to disable all previously entered RSPAN configurations.

Format

disable rspan

Parameters

None.

Restrictions

Only Administrators and Operators can issue this command.

Example

To disable all previously entered RSPAN configurations:

```
DGS-3000-28SC:admin#disable rspan
Command: disable rspan

Success.

DGS-3000-28SC:admin#
```

78-3 create rspan vlan

Description

This command is used to create an RSPAN VLAN. Up to 16 RSPAN VLANs can be created.

Format

create rspan vlan [vlan_name <vlan_name> | vlan_id <vlanid 1-4094>]

Parameters

vlan_name - Create the RSPAN VLAN by VLAN name. **<vlan_name>** - Enter the VLAN name.
vlan_id - Create the RSPAN VLAN by VLAN ID. **<vlanid 1-4094>** - Enter the VLAN ID between 1 and 4094.

Restrictions

Only Administrators and Operators can issue this command.

Example

To create an RSPAN VLAN entry by VLAN name “v2”:

```
DGS-3000-28SC:admin#create rspan vlan vlan_name v2
Command: create rspan vlan vlan_name v2

Success.

DGS-3000-28SC:admin#
```

To create an RSPAN VLAN entry by VLAN ID “3”:

```
DGS-3000-28SC:admin#create rspan vlan vlan_id 3
Command: create rspan vlan vlan_id 3

Success.

DGS-3000-28SC:admin#
```

78-4 delete rspan vlan

Description

This command is used to delete RSPAN VLANs.

Format

delete rspan vlan [vlan_name <vlan_name> | vlan_id <vlanid 1-4094>]

Parameters

vlan_name - Specify the RSPAN VLAN by VLAN name. **<vlan_name>** - Enter the VLAN name.
vlan_id - Specify the RSPAN VLAN by VLAN ID. **<vlanid 1-4094>** - Enter the VLAN ID between 1 and 4094.

Restrictions

Only Administrators and Operators can issue this command.

Example

To delete an RSPAN VLAN entry by VLAN name “v2”:

```
DGS-3000-28SC:admin#delete rspan vlan vlan_name v2
Command: delete rspan vlan vlan_name v2

Success.

DGS-3000-28SC:admin#
```

To delete an RSPAN VLAN entry by VLAN ID “3”:

```
DGS-3000-28SC:admin#delete rspan vlan vlan_id 3
Command: delete rspan vlan vlan_id 3

Success.

DGS-3000-28SC:admin#
```

78-5 config rspan vlan

Description

This command with source parameter is used by the source switch to configure the source setting for the RSPAN VLAN. While the command with redirect parameter is used by the intermediate or last switch to configure the output port of the RSPAN VLAN packets, and makes sure that the RSPAN VLAN packets can egress to the redirect ports. In addition, the VLAN setting must be correctly configured to make the RSPAN VLAN work correctly. That is, for the intermediate switch, the redirect port must be a tagged member port of the RSPAN VLAN. For the last switch, the redirect port must be either a tagged member port or an untagged member port of the RSPAN VLAN based on the users' requirements. If untagged membership is specified, the RSPAN VLAN tag will be removed. The redirect function will only work when RSPAN is enabled. Multiple RSPAN VLANs can be configured with the redirect setting at the same time.

A RSPAN VLAN can be configured with the source setting and the redirect setting at the same time.

Format

config rspan vlan [vlan_name <vlan_name> | vlan_id <vlanid 1-4094>] [redirect [add | delete] ports <portlist> | source {[mirror_group_id <value 1-4> | [add | delete] ports<portlist> [rx | tx | both]]}]

Parameters

vlan_name - Specify the RSPAN VLAN by VLAN name.
- **<vlan_name>** - Enter the VLAN name.

vlan_id - Specify the RSPAN VLAN by VLAN ID.
- **<vlanid 1-4094>** - Enter the VLAN ID between 1 and 4094.

redirect - Specify output port list for the RSPAN VLAN packets. If the redirect port is a Link Aggregation port, the Link Aggregation behavior will apply to the RSPAN packets.
- **add** - Specify to add the redirect port.
- **delete** - Specify to delete the redirect port.
  - **ports** - Specify the output port list to add to or delete from the RSPAN packets.
    - **<portlist>** - Enter a range of ports to be configured.

source - If the ports are not specified by this command, the source of RSPAN will come from the source specified by the mirror command or the flow-based source specified by an ACL. If no parameter is specified for source, it deletes the configured source parameters.
- **mirror_group_id** - (Optional) Specify which mirror session is used for RSPAN source function. When the mirror group isn't specified, mirror group 1 will be the default group.
  - **<value 1-4>** - Enter the mirror group ID here.
- **add** - (Optional) Specify to add source ports.
- **delete** - (Optional) Specify to delete source ports.
  - **ports** - Specify source port list to add to or delete from the RSPAN source.
    - **<portlist>** - Enter a range of ports to be configured.
  - **rx** - Specify to only monitor ingress packets.
  - **tx** - Specify to only monitor egress packets.
  - **both** - Specify to monitor both ingress and egress packets.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure an RSPAN source entry without source target port:

```
DGS-3000-28SC:admin#config rspan vlan vlan_name vlan2 source add ports 1:2-1:5
rx
Command: config rspan vlan vlan_name vlan2 source add ports 1:2-1:5 rx

Success.

DGS-3000-28SC:admin#
```

To configure an RSPAN source entry for per flow RSPAN, without any source ports:

```
DGS-3000-28SC:admin#config rspan vlan vlan_id 2 source
Command: config rspan vlan vlan_id 2 source

Success.

DGS-3000-28SC:admin#
```

To configure RSPAN redirect for “VLAN 2” to ports 18 and 19:

```
DGS-3000-28SC:admin#config rspan vlan vlan_name vlan2 redirect add ports 1:18-
1:19
Command: config rspan vlan vlan_name vlan2 redirect add ports 1:18-1:19

Success.

DGS-3000-28SC:admin#
```

78-6 show rspan

Description

This command is used to display RSPAN configuration.

Format

show rspan {[vlan_name <vlan_name> | vlan_id <vlanid 1-4094>]}

Parameters

vlan_name - (Optional)Specify the RSPAN VLAN by VLAN name. **<vlan_name>** - Enter the VLAN name.
vlan_id - (Optional)Specify the RSPAN VLAN by VLAN ID. **<vlanid 1-4094>** - Enter the VLAN ID between 1 and 4094.

Restrictions

None.

Example

To display specific RSPAN VLAN settings:

```
DGS-3000-28SC:admin# show rspan vlan_id 1
Command: show rspan vlan_id 1

RSPAN   : Enabled

RSPAN VLAN ID  : 1
--------------------
  Mirror Group ID  : 1
  Target Port      : 1:1
  Source Ports
      RX           : 1:2-1:5
      TX           : 1:2-1:5

DGS-3000-28SC:admin#
```

To display all RSPAN VLAN settings:

```
DGS-3000-28SC:admin# show rspan
Command: show rspan

RSPAN   : Enabled

RSPAN VLAN ID  : 1
--------------------
  Mirror Group ID  : 1
  Target Port      : 1:1
  Source Ports
      RX           : 1:2-1:5
      TX           : 1:2-1:5

RSPAN VLAN ID  : 2
--------------------
  Redirect Ports   : 1:6-1:10

RSPAN VLAN ID  : 3
--------------------


Total RSPAN VLAN :3

DGS-3000-28SC:admin#
```

Chapter 79 Safeguard Engine Command List

config safeguard_engine {state [enable | disable] | utilization {rising <20-100> | falling <20-100>}(1) | trap_log [enable | disable] | mode [strict | fuzzy]}(1)
show safeguard_engine

79-1 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>}(1) | trap_log [enable | disable] | mode [strict | fuzzy]}(1)

Parameters

state - Specify to configure CPU protection state to enable or disable. **enable** - Specify that CPU protection will be enabled. **disable** - Specify that CPU protection will be enabled.
utilization - Specify to configure the CPU protection threshold. **rising** - Specify 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** - Specify 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 - Specify to enable or disable the trap and log mechanism. **enable** - Specify that the trap and log mechanism will be enabled. **disable** - Specify that the trap and log mechanism will be disabled.
mode - Specify 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-3000-28SC: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-3000-28SC:admin#
```

79-2 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-3000-28SC: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-3000-28SC:admin#
```

NOTE: Safeguard engine current status has two modes: exhausted and normal mode.

Chapter 80 Secure File Transfer Protocol (SFTP) Command List

config sftp server {timeout <sec 30-600>}
enable sftp server
disable sftp server
show sftp server

80-1 config sftp server

Description

This command is used to configure parameters for SFTP server.

Format

config sftp server {timeout <sec 30-600>}

Parameters

timeout - (Optional) Specify the idle timer for SFTP server. If the SFTP server detects no operation after this duration for a specific SFTP session, it will close this SFTP session. The default value is 120 seconds.
<sec 30-600> - Enter the SFTP server timeout value here. This value must be between 30 and 600 seconds.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure idle timer to 600 seconds:

```
DGS-3000-28SC:admin# config sftp server timeout 600
Command: config sftp server timeout 600

Success.

DGS-3000-28SC:admin#
```

80-2 enable sftp server

Description

This command is used to enable the SFTP function globally. SFTP over SSH2 is a remotely secure file transfer protocol providing security on all file operations. SFTP server runs as a subsystem of SSH server. SSH server is required to be enabled before enabling SFTP server.

Format

enable sftp server

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable SFTP server globally:

```
DGS-3000-28SC:admin# enable sftp server
Command: enable sftp server

Success.

DGS-3000-28SC:admin#
```

80-3 disable sftp server

Description

This command is used to disable the SFTP server function globally. All active SFTP sessions will be disturbed after executing this command. SFTP server runs as a subsystem of the SSH server. Disabling SSH server will also disturb all SFTP session.

Format

disable sftp server

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To disable SFTP server globally:

```
DGS-3000-28SC:admin# disable sftp server
Command: disable sftp server

Success.

DGS-3000-28SC:admin#
```

80-4 show sftp server

Description

This command is used to show the parameters of the SFTP server.

Format

show sftp server

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To show the parameters of the SFTP server:

```
DGS-3000-28SC:admin# show sftp server
Command: show sftp server

 The SFTP Server Configuration
 Protocol Version              : 3
 State                         : Enabled
 Session Idle Timeout          : 600 sec

DGS-3000-28SC:admin#
```

Chapter 81 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 30-600> | authfail <int 2-20> | rekey [10min | 30min | 60min | never] | port <tcp_port_number 1-65535>}
enable ssh
disable ssh
show ssh server
config ssh client_pubkey_owner key_id <int 1-8> [add | remove] user <username 15>
config ssh publickey bypass_login_screen state [enable | disable]
download ssh client_pub_key [<ipaddr> | <ipv6addr> | <domain_name 255>] src_file <path_filename 64>
show ssh client_pub_key
upload ssh client_public_key [<ipaddr> | <ipv6addr> | <domain_name 255>] dest_file <path_filename 64>

81-1 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.
AES128 - Specify that the AES, 128-bit encryption method will be used.
AES192 - Specify that the AES, 192-bit encryption method will be used.
AES256 - Specify that the AES, 256-bit encryption method will be used.
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.
twofish128 - Specify that the Twofish, 128-bit encryption method will be used.
twofish192 - Specify that the Twofish, 192-bit encryption method will be used.

twofish256 - Specify that the Twofish, 256-bit encryption method will be used.
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-3000-28SC:admin#config ssh algorithm DSA enable
Command: config ssh algorithm DSA enable

Success.

DGS-3000-28SC:admin#
```

81-2 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-3000-28SC: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-3000-28SC:admin#
```

81-3 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 - Specify the user authentication method using password.
publickey - Specify the user authentication method using public key.
hostbased - Specify 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-3000-28SC:admin#config ssh authmode publickey enable
Command: config ssh authmode publickey enable

Success.

DGS-3000-28SC:admin#
```

81-4 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-3000-28SC:admin#show ssh authmode
Command: show ssh authmode

The SSH Authentication Method:
Password    : Enabled
Public Key  : Enabled
Host-based  : Enabled


DGS-3000-28SC:admin#
```

81-5 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 - Specify the authentication method.
hostbased - Specify user authentication method.
hostname - Specify host domain name.
<domain_name 32> - Enter the domain name here. This name can be up to 32 characters long.
hostname_IP - Specify host domain name and IP address.
<domain_name 32> - Enter host name if configuring Host-based method.
<ipaddr> - Enter host IP address if configuring Host-based method.
<ipv6addr> - Enter host IPv6 address if configuring Host-based method.
password - Specify user authentication method.
publickey - Specify user authentication method.

Restrictions

Only Administrators can issue this command.

Example

To update user “test” authentication method:

```
DGS-3000-28SC:admin#config ssh user test authmode publickey
Command: config ssh user test authmode publickey

Success.

DGS-3000-28SC:admin#
```

81-6 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-3000-28SC: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-3000-28SC:admin#
```

81-7 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 30-600> | authfail <int 2-20> | rekey [10min | 30min | 60min | never] | port <tcp_port_number 1-65535>}

Parameters

maxsession - (Optional) Specify 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) Specify SSH server connection time-out, in the unit of second.
<sec 30-600> - Enter the connection time-out value here. This value must be between 30 and 600 seconds.

authfail - (Optional) Specify 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) Specify 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 - Specify that the re-generate session key time will be 10 minutes.
30min - Specify that the re-generate session key time will be 30 minutes.
60min - Specify that the re-generate session key time will be 60 minutes.
never - Specify that the re-generate session key time will be set to never.

port - (Optional) Specify 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-3000-28SC:admin#config ssh server maxsession 3
Command: config ssh server maxsession 3

Success.

DGS-3000-28SC:admin#
```

81-8 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-3000-28SC:admin#enable ssh
Command: enable ssh

Success.

DGS-3000-28SC:admin#
```

81-9 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-3000-28SC:admin#disable ssh
Command: disable ssh

Success.

DGS-3000-28SC:admin#
```

81-10 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-3000-28SC: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-3000-28SC:admin#
```

81-11 config ssh client_pubkey_owner key_id

Description

This command is used to manage the public keys ownership. Once the authorized public keys file (each line of the file contains one key) is downloaded to the switch, each key will be automatically assigned an index which starts from one. The administrator can associate the public key with a user account based on the index.

NOTE: Each time the authorized public keys file is downloaded to the switch, the previous configuration about the relationship between user account and public key will be reset. The administrator must re-configure if a public key is intended for a special user account.

Format

config ssh client_pubkey_owner key_id <int 1-8> [add | remove] user <username 15>

Parameters

<int 1-8> - Enter the key ID that will be associated with the user account. This value must be between 1 and 8.
add - Specify to add an association between the key and the user account. When a public key is associated with a user account, the public key can only be used by that user account. A public key may be associated with more than one user account, and a user account may associate with more than one public keys. A public key which has not been associated with any user account can be used by all users.
remove - Specify to remove the association between the key and the user account.
user - Specify the user account that will be used for this configuration. **<username 15>** - Enter the user account's user name here. This name can be up to 15 characters long.

Restrictions

Only Administrator level can issue this command.

Example

To associate a public key with the index of 1 to the user account named “User1”:

```
DGS-3000-28SC:admin# config ssh client_pubkey_owner key_id 1 add user User1
Command: config ssh client_pubkey_owner key_id 1 add user User1

Success.

DGS-3000-28SC:admin#
```

81-12 config ssh publickey bypass_login_screen state

Description

This command is used to enable or disable bypassing login screen which is used to avoid a secondary username/password authentication for users using SSH public key authentication.

Format

config ssh publickey bypass_login_screen state [enable | disable]

Parameters

enable - Specify to bypass the username/password login screen to avoid a secondary authentication after using SSH public key authentication. If this method is specified, the login user using SSH public key authentication can execute command directly with the initial privilege level of the login user.
disable - Specify to need a secondary username/password authentication after using SSH public key authentication. If this method is specified, the login user using SSH public key authentication must pass username/password authentication before execution shell is obtained. The initial privilege level depends on the secondary username/password authentication.

Restrictions

Only Administrator level can issue this command.

Example

To disable the secondary username/password authentication for users using SSH public key authentication:

```
DGS-3000-28SC:admin# config ssh publickey bypass_login_screen state disable
Command: config ssh publickey bypass_login_screen state disable

Success.

DGS-3000-28SC:admin#
```

81-13 download ssh client_pub_key

Description

This command is used to download the SSH public key file on client computer to the switch through TFTP protocol.

Format

download ssh client_pub_key [<ipaddr> | <ipv6addr> | <domain_name 255>] src_file <path_filename 64>

Parameters

<ipaddr> - Specify the IPv4 address of the TFTP server.
<ipv6addr> - Specify the IPv6 address of the TFTP server.
<domain_name 255> - Enter the domain name of the TFTP server.
src_file - Specify the path name and file name of the TFTP server. It can be a relative path name or an absolute path name. If path name is not specified, it refers to the TFTP server path. **<path_filename 64>** - Enter the source file path. This can be up to 64 characters long.

Restrictions

Only Administrator-level users can issue this command.

Example

To download a SSH public key file named id_rsa_keys from TFTP server 169.168.10.100 to the switch:

```
DGS-3000-28SC:admin#download ssh client_pub_key 169.168.10.100 src_file
id_rsa_keys
Command: download ssh client_pub_key 169.168.10.100 src_file id_rsa_keys

  Connecting to server.................. Done.
  Download SSH public key.................Done.

DGS-3000-28SC:admin#
```

81-14 show ssh client_pub_key

Description

This command is used to display the client SSH public key.

Format

show ssh client_pub_key

Parameters

None.

Restrictions

None.

Example

To show how to display SSH public keys:

```
DGS-3000-28SC:admin# show ssh client_pub_key
Command: show ssh client_pub_key

Key ID    : 1
User Name :
Key       :
ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEA2ubZ/h5yrP8vEmYeDcpZP/TA8SR7q0tZcywKcTujES0Ue/muoyy
tJhTZuI2B2Z4A4ufJ1yCR9NTWrL4mhJNJOspGLssBeHbf6HtGwyInYm5MJBqeoht0RrS8NIa2VWsvQc
xQQSoNeS7J5ROvfSpgTdYBsTosJUHzBvNsGy4w1S0= rsa-key-20110603

Key ID    : 2
User Name : User1
Key       :
ssh-rsa
AAAAB3NzaC1yc2EAAAABJQAAAIBJv3BYQ7DeO0mDatPa//wG3j/5yhBZw9mY+xw1ovskDE6/os7swVj
w3wK+Tt40GJVdVVF7w195prYA+tYcBFy5iJpnwykwwxD09BMVwHhvZs9/U4LaAek2USarYfQU7ZoNof
OC3F86EPtsUJ2s98rMAa6DYqRS+JyH/IpA8T1x5w== rsa-key-20110603

DGS-3000-28SC:admin#
```

81-15 upload ssh client_public_key

Description

This command is used to display the client SSH public key.

Format

upload ssh client_public_key [<ipaddr> | <ipv6addr> | <domain_name 255>] dest_file <path_filename 64>

Parameters

<ipaddr> - Specify the IPv4 address of the TFTP server.
<ipv6addr> - Specify the IPv6 address of the TFTP server.
<domain_name 255> - Enter the domain name of the TFTP server.
dest_file - Specify the path name and file name of the TFTP server. It can be a relative path name or an absolute path name. If path name is not specified, it refers to the TFTP server path. **<path_filename 64>** - Enter the source file path. This can be up to 64 characters long.

Restrictions

Only Administrator level can issue this command.

Example

To upload a SSH public key file named id_rsa_keys to TFTP server 169.168.10.100 to the switch:

```
DGS-3000-28SC:admin# upload ssh client_public_key 169.168.10.100 dest_file
id_rsa_keys
Command: upload ssh client_public_key 169.168.10.100 dest_file id_rsa_keys

  Connecting to server.................. Done.
  Upload SSH public key.................Done.

DGS-3000-28SC:admin#
```

Chapter 82 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 {[chain | <path_filename 64>]}}
show ssl cachetimeout
config ssl cachetimeout <value 60-86400>
config ssl certificate chain [default | <cert_list>]
delete ssl certificate <path_filename 64>

82-1 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) Specify 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) Specify 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-3000-28SC: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-3000-28SC:admin#
```

82-2 enable ssl

Description

This command is used to enable SSL status and it's 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) Specify the cipher suite combination used for this configuration.
- **RSA_with_RC4_128_MD5** - (Optional) Indicates RSA key exchange with RC4 128 bits encryption and MD5 hash.
- **RSA_with_3DES_EDE_CBC_SHA** - (Optional) Indicates RSA key exchange with 3DES_EDE_CBC encryption and SHA hash.
- **DHE_DSS_with_3DES_EDE_CBC_SHA** - (Optional) Indicates DH key exchange with 3DES_EDE_CBC encryption and SHA hash.
- **RSA_EXPORT_with_RC4_40_MD5** - (Optional) 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-3000-28SC:admin#enable ssl
Command: enable ssl

Note: Web will be disabled if SSL is enabled.
Success.

DGS-3000-28SC:admin#
```

To enable SSL:

```
DGS-3000-28SC:admin#enable ssl
Command: enable ssl

Success.

DGS-3000-28SC:admin#
```

NOTE: Web will be disabled when SSL is enabled.

82-3 disable ssl

Description

This command is used to disable SSL feature and supported ciphercuites. 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) Specify the cipher suite combination used for this configuration.
- **RSA_with_RC4_128_MD5** - (Optional) Indicates RSA key exchange with RC4 128 bits encryption and MD5 hash.
- **RSA_with_3DES_EDE_CBC_SHA** - (Optional) Indicates RSA key exchange with 3DES_EDE_CBC encryption and SHA hash.
- **DHE_DSS_with_3DES_EDE_CBC_SHA** - (Optional) Indicates DH key exchange with 3DES_EDE_CBC encryption and SHA hash.
- **RSA_EXPORT_with_RC4_40_MD5** - (Optional) 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-3000-28SC:admin#disable ssl ciphersuite RSA_with_RC4_128_MD5
Command: disable ssl ciphersuite RSA_with_RC4_128_MD5

Success.

DGS-3000-28SC:admin#
```

To disable SSL:

```
DGS-3000-28SC:admin#disable ssl
Command: disable ssl

Success.

DGS-3000-28SC:admin#
```

82-4 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 {[chain | <path_filename 64>]}}

Parameters

certificate - (Optional) Specify that the SSL certificate will be displayed. **chain** - (Optional) Specify the chain of certifications on the Switch to be displayed. **<path_filename 64>** - (Optional) Specify the certification file name on the Switch.

Restrictions

None.

Example

To show SSL:

```
DGS-3000-28SC: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-3000-28SC:admin#
```

To show certificate:

```
DGS-3000-28SC:admin#show ssl certificate
Command: show ssl certificate

Loaded with RSA Certificate!

DGS-3000-28SC:admin#
```

82-5 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-3000-28SC:admin#show ssl cachetimeout
Commands: show ssl cachetimeout

Cache timeout is 600 second(s)

DGS-3000-28SC:admin#
```

82-6 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

<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-3000-28SC:admin#config ssl cachetimeout 60
Commands: config ssl cachetimeout 60

Success.

DGS-3000-28SC:admin#
```

82-7 config ssl certificate chain

Description

This command is used to specify chain of certifications on the Switch.

Format

config ssl certificate chain [default | <cert_list>]

Parameters

default - Specify to use all certificates to constitute the SSL certificate chain.
<cert_list> - Specify chain of certifications on the Switch.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure SSL chain of certifications:

```
DGS-3000-28SC:admin# config ssl certificate chain web_ca2.cer,server.crt
Command: config ssl certificate chain web_ca2.cer,server.crt

Success.

DGS-3000-28SC:admin#
```

82-8 delete ssl certificate

Description

This command is used to delete a certification on the Switch.

Format

delete ssl certificate <path_filename 64>

Parameters

<path_filename 64> - Specify the certification file name on the Switch.

Restrictions

Only Administrator-level users can issue this command.

Example

To delete a certificate:

```
DGS-3000-28SC:admin# delete ssl certificate web_ca2.cer
Command: delete ssl certificate web_ca2.cer

Success.

DGS-3000-28SC:admin#
```

Chapter 83 sFlow Command List

config sflow analyzer_server <value 1-4> {timeout [<sec 1-2000000> | infinite] | collectoraddress [<ipaddr> | <ipv6addr>] | collectorport <udp_port_number 1-65535> | maxdatagramsize <value 300-1400>}(1)
config sflow counter_poller ports [<portlist> | all] interval [disable | <sec 20-120>]
config sflow flow_sampler ports [<portlist> | all] {rate <value 0-65535> | tx_rate <value 0-65535> | maxheadersize <value 18-256>}(1)
create sflow analyzer_server <value 1-4> owner <name 16> {timeout [<sec 1-2000000> | infinite] | collectoraddress [<ipaddr> | <ipv6addr>] | collectorport <udp_port_number 1-65535> | maxdatagramsize <value 300-1400>}
create sflow counter_poller ports [<portlist> | all] analyzer_server_id <value 1-4> {interval [disable | <sec 20-120>]}
create sflow flow_sampler ports [<portlist> | all] analyzer_server_id <value 1-4> { rate <value 0-65535> | tx_rate <value 0-65535> | maxheadersize <value 18-256>}
delete sflow analyzer_server <value 1-4>
delete sflow counter_poller ports [<portlist> | all]
delete sflow flow_sampler ports [<portlist> | all]
enable sflow
disable sflow
show sflow
show sflow analyzer_server
show sflow counter_poller
show sflow flow_sampler

83-1 config sflow analyzer_server

Description

This command is used to configure the receiver information. You can specify more than one collector with the same IP address if the UDP port numbers are unique.

Format

config sflow analyzer_server <value 1-4> {timeout [<sec 1-2000000> | infinite] | collectoraddress [<ipaddr> | <ipv6addr>] | collectorport <udp_port_number 1-65535> | maxdatagramsize < value 300-1400>}(1)

Parameters

<value 1-4> - Enter the analyzer server ID here. This value must be between 1 and 4.
timeout - The time (in seconds) remaining before the sample is released and stops sampling. When the analyzer_server times out, all of the flow_samplers and counter_pollers associated with this analyzer_server will be deleted. **<sec 1-2000000>** - Enter the time-out value here. This value must be between 1 and 2000000 seconds. **infinite** - Indicates the analyzer server never timeout
collectoraddress - The IP address of the server. If not specified or set a 0 address, sFlow packets will not be sent to this server. **<ipaddr>** - Enter the IP address used for the configuration here. **<ipv6addr>** - Enter the IPv6 address used for the configuration here.

collectorport - The destination UDP port for sending the sFlow datagram. If not specified, the default value is 6364 **<udp_port_number 1-65535>** - Enter the destination port number here. This value must be between 1 and 65535.
maxdatagramsize - The maximum number of data bytes that can be packed in a single sample datagram. If not specified, the default value is 1400 bytes. **<value 300-1400>** - Enter the maximum datagram size here. This value must be between 300 and 1400.

Restrictions

Only Administrators and Operators can issue this command.

Example

Configure the host 10.90.90.90 to be the sFlow analyzer server with the ID 1:

```
DGS-3000-28SC:admin# config sflow analyzer_server 1 collectoraddress
10.90.90.90
Command: config sflow analyzer_server 1 collectoraddress 10.90.90.90

Success.

DGS-3000-28SC:admin#
```

83-2 config sflow counter_poller ports

Description

This command is used to configure the sFlow counter poller parameters. If the user wants the change the analyzer_server_id, he needs to delete the counter_poller and creates a new one.

Format

config sflow counter_poller ports [<portlist> | all] interval [disable | <sec 20-120>]

Parameters

<portlist> - Enter the list of ports that will be used for this configuration here.
all - Specify all ports on the Switch.
interval - The maximum number of seconds between successive samples of the counters. **disable** - Stop exporting counter. **<sec 20-120>** - Enter the maximum number of seconds between successive samples of the counters here. This value must be between 20 and 120.

Restrictions

Only Administrators and Operators can issue this command.

Example

Configure the interval of sFlow counter poller port 1 to be 0:

```
DGS-3000-28SC:admin#config sflow counter_poller ports 1:1 interval disable
Command: config sflow counter_poller ports 1:1 interval disable

Success.

DGS-3000-28SC:admin#
```

83-3 config sflow flow_sampler ports

Description

This command is used to configure the sFlow flow sampler parameters. In order to change the analyzer_server_id, delete the flow_sampler first and create a new one.

Format

config sflow flow_sampler ports [<portlist> | all] {rate <value 0-65535> | tx_rate <value 0-65535> | maxheadersize <value 18-256>}(1)

Parameters

<portlist> - Enter the list of ports that will be used for this configuration here.
all - Specify all ports on the Switch.
rate - The sampling rate for packet Rx sampling. If set to 0, the sampler is disabled. If the rate is not specified, its default value is 0. **<value 0-65535>** - Enter the sampling rate value here. This value must be between 0 and 65535.
tx_rate - Specify the sampling rate for packet transmitting sampling. If set to 0, the sampler is disabled. If the rate is not specified, its default value is 0. **<value 0-65535>** - Enter the product dependent variables between 0 to 65535 here.
maxheadersize - The maximum number of leading bytes in the packet which has been sampled that will be encapsulated and forwarded to the server. The default value is 128. **<value 18-256>** - Enter the maximum header size value here. This value must be between 18 and 256.

Restrictions

Only Administrators and Operators can issue this command.

Example

Configure the sFlow sampler the rate of port 1 to be 0:

```
DGS-3000-28SC:admin# config sflow flow_sampler ports 1:1 rate 0 maxheadersize
18
Command: config sflow flow_sampler ports 1:1 rate 0 maxheadersize 18

Success.

DGS-3000-28SC:admin#
```

83-4 create sflow analyzer_server

Description

This command is used to create the analyzer server. You can specify more than one analyzer_server with the same IP address but with different UDP port numbers. You can have up to four unique combinations of IP address and UDP port number.

Format

create sflow analyzer_server <value 1-4> owner <name 16> {timeout [<sec 1-2000000> | infinite] | collectoraddress [<ipaddr> | <ipv6addr>] | collectorport <udp_port_number 1-65535> | maxdatagramsize <value 300-1400>}

Parameters

<value 1-4> - Enter the analyzer server ID here.
owner - The entity making use of this sFlow analyzer_server. When owner is set or modified, the timeout value will become 400 automatically. **<name 16>** - Enter the owner name here. This name can be up to 16 characters long.
timeout - (Optional) The seconds to wait before the server is timed out. When the analyzer server times out, all of the flow_samplers and counter_pollers associated with this analyzer server will be deleted. The default value is 400 seconds. **<sec 1-2000000>** - Enter the time-out value here. This value must be between 1 and 2000000 seconds. **infinite** - Indicates the analyzer server never timeout.
collectoraddress - (Optional) The IP address of the analyzer server. If this is set to 0 or not specified, the IP address is 0 and the entry is not active. **<ipaddr>** - Enter the IP address used for the configuration here. **<ipv6addr>** - Enter the IPv6 address used for the configuration here.
collectorport - (Optional) The destination UDP port for sending the sFlow datagram. If not specified, the default value is 6364. The specified UDP port number can not conflict with other applications. **<udp_port_number 1-65535>** - Enter the destination UDP port number here. This value must be between 1 and 65535.
maxdatagramsize - (Optional) The maximum number of data bytes that can be packed in a single sample datagram. If not specified, the default value is 1400 bytes. **<value 300-1400>** - Enter the maximum datagram size here. This value must be between 300 and 1400.

Restrictions

Only Administrators and Operators can issue this command.

Example

To create the analyzer server:

```
DGS-3000-28SC:admin# create sflow analyzer_server 2 owner monitor timeout
infinite collectoraddress 10.0.0.1 collectorport 65524 maxdatagramsize 300
Command: create sflow analyzer_server 2 owner monitor timeout infinite
collectoraddress 10.0.0.1 collectorport 65524 maxdatagramsize 300

Success.

DGS-3000-28SC:admin#
```

83-5 create sflow counter_poller ports

Description

This command is used to create the sFlow counter poller. The poller function instructs the Switch to forward statistics counter information with respect to a port.

Format

create sflow counter_poller ports [<portlist> | all] analyzer_server_id <value 1-4> {interval [disable | <sec 20-120>]}

Parameters

<portlist> - Enter the list of ports that will be used for this configuration here.
all - Specify all ports on the Switch.
analyzer_server_id - Specify the analyzer server ID. **<value 1-4>** - Enter the analyzer server here. This value must be between 1 and 4.
interval - (Optional) The maximum number of seconds between successive statistics counters information. **disable** - This new sFlow counter will not export counter until the interval to be set a appropriate value. If interval is not specified, its default value is disabled. **<sec 20-120>** - Enter the maximum number of seconds between successive statistics counters information here. This value must be between 20 and 120 seconds.

Restrictions

Only Administrators and Operators can issue this command.

Example

Create sFlow counter poller, which sample port 1 to analyzer server 1:

```
DGS-3000-28SC:admin# create sflow counter_poller ports 1:1 analyzer_server_id 1
Command: create sflow counter_poller ports 1:1 analyzer_server_id 1

Success.

DGS-3000-28SC:admin#
```

83-6 create sflow flow_sampler ports

Description

This command is used to create the sFlow flow sampler. By configuring the sampling function for a port, a sample packet received by this port will be encapsulated and forwarded to analyzer server at the specified interval.

Format

create sflow flow_sampler ports [<portlist> | all] analyzer_server_id <value 1-4> {rate <value 0-65535> | tx_rate <value 0-65535> | maxheadersize <value 18-256>}

Parameters

<portlist> - Enter the list of ports that will be used for this configuration here.
all - Specify all ports on the Switch.
analyzer_server_id - Specify the ID of a server analyzer where the packet will be forwarded. **<value 1-4>** - Enter the analyzer server ID here. This value must be between 1 and 4.
rate - (Optional) The sampling rate for packet Rx sampling. The configured rate value multiplied by x is the actual rate, where the x is project dependent with the default value 256. If set to 0, the sampler is disabled. If the rate is not specified, its default value is 0. **<value 0-65535>** - Enter the sampling rate value here. This value must be between 0 and 65535.
tx_rate - (Optional) Specify the sampling rate for packet transmitting sampling. The configured rate value multiplied by x is the actual rate, where the x is project dependent with the default value 256. If set to 0, the sampler is disabled. If the rate is not specified, its default value is 0. **<value 0-65535>** - Enter the product dependent variables between 0 to 65535 here.
maxheadersize - (Optional) The maximum number of leading bytes in the packet which has been sampled that will be encapsulated and forwarded to the server. If not specified, the default value is 128. **<value 18-256>** - Enter the maximum header size here. This value must be between 18 and 256.

Restrictions

Only Administrators and Operators can issue this command.

Example

Create sFlow flow sampler:

```
DGS-3000-28SC:admin# create sflow flow_sampler ports 1 analyzer_server_id 1
rate 1 maxheadersize 18
Command: create sflow flow_sampler ports 1 analyzer_server_id 1 rate 1
maxheadersize 18


Success.


DGS-3000-28SC:admin#
```

83-7 delete sflow_analyzer_server

Description

This command is used to delete a specified analyzer server.

Format

delete sflow analyzer_server <value 1-4>

Parameters

<value 1-4> - Enter the analyzer server ID value here. This value must be between 1 and 4.

Restrictions

Only Administrators and Operators can issue this command.

Example

To delete an analyzer server:

```
DGS-3000-28SC:admin# delete sflow analyzer_server 1
Command: delete sflow analyzer_server 1

Success.

DGS-3000-28SC:admin#
```

83-8 delete sflow counter_poller

Description

This command is used to delete the sFlow counter poller from the specified port

Format

delete sflow counter_poller ports [<portlist> | all]

Parameters

<portlist> - Enter the list of ports to be deleted.
all - Specify all ports on the Switch.

Restrictions

Only Administrators and Operators can issue this command.

Example

To delete an sFlow counter poller on port 1:

```
DGS-3000-28SC:admin# delete sflow counter_poller ports 1:1
Command: delete sflow counter_poller ports 1:1

Success.

DGS-3000-28SC:admin#
```

83-9 delete sflow flow_sampler ports

Description

This command is used to delete the sFlow flow sampler.

Format

delete sflow flow_sampler ports [<portlist> | all]

Parameters

<portlist> - Enter the list of ports to be deleted.
all - Specify all ports on the Switch.

Restrictions

Only Administrators and Operators can issue this command.

Example

To delete the sFlow sampler port 1:

```
DGS-3000-28SC:admin# delete sflow flow_sampler ports 1:1
Command: delete sflow flow_sampler ports 1:1

Success.

DGS-3000-28SC:admin#
```

83-10 enable sflow

Description

This command is used to enable the sFlow function on the Switch.

Format

enable sflow

Parameters

None.

Restrictions

Only Administrator and Operator-level users can issue this command.

Example

To enable the sFlow function globally:

```
DGS-3000-28SC:admin# enable sflow
Command: enable sflow

Success.

DGS-3000-28SC:admin#
```

83-11 disable sflow

Description

This command is used to disable the sFlow function on the Switch.

Format

disable sflow

Parameters

None.

Restrictions

Only Administrator and Operator-level users can issue this command.

Example

Disable the sFlow globally:

```
DGS-3000-28SC:admin# disable sflow
Command: disable sflow

Success.

DGS-3000-28SC:admin#
```

83-12 show sflow

Description

This command is used to show the sFlow information.

Format

show sflow

Parameters

None.

Restrictions

None.

Example

To show the sFlow information:

```
DGS-3000-28SC:admin#show sflow
Command: show sflow

 sFlow Version  : V5
 sFlow Address  : 10.90.90.90
 sFlow State    : Disabled

DGS-3000-28SC:admin#
```

83-13 show sflow analyzer_server

Description

This command is used to show the sFlow analyzer server information. The Timeout field specifies the time configured by user. The Current Countdown Time is the current time remaining before the server timeout.

Format

show sflow analyzer_server

Parameters

None.

Restrictions

None.

Example

To show the sFlow flow sampler information of ports which have been created:

```
DGS-3000-28SC:admin#show sflow analyzer_server
Command: show sflow analyzer_server

 sFlow Analyzer_server Information
 ------------------------------
 Server ID             : 1
 Owner                 : sflow
 Timeout               : 400
 Current Countdown Time: 400
 Collector Address     : 10.90.90.90
 Collector Port        : 6343
 Max Datagram Size     : 1400

 Server ID             : 2
 Owner                 : monitor
 Timeout               : Infinite
 Current Countdown Time: Infinite
 Collector Address     : 10.0.0.1
 Collector Port        : 65524
 Max Datagram Size     : 300

Total Entries: 2

DGS-3000-28SC:admin#
```

83-14 show sflow counter_poller

Description

This command is used to display the sFlow counter pollers which have been configured for port.

Format

show sflow counter_poller

Parameters

None.

Restrictions

None.

Example

To show the sFlow counter poller information of ports which have been created:

```
DGS-3000-28SC:admin#show sflow counter_poller
Command: show sflow counter_poller

 Port   Analyzer Server ID   Polling Interval (sec)
 ----   ------------------   ----------------------
 1:1    1                    Disable

Total Entries: 1

DGS-3000-28SC:admin#
```

83-15 show sflow flow_sampler

Description

This command is used to show the sFlow flow sampler configured for ports. The actual value rate is 256 times the displayed rate value. There are two types of rates. The Configured Rate is configured by the user. In order to limit the number of packets sent to the CPU when the rate of traffic to the CPU is high, the sampling rate will be decreased. This is specified as the active rate.

Format

show sflow flow_sampler

Parameters

None.

Restrictions

None.

Example

To show the sFlow flow sampler information of ports which have been created:

```
DGS-3000-28SC:admin#DGS-3000-28SC:admin#show sflow flow_sampler
Command: show sflow flow_sampler

 Port    Analyzer   Configured  Configured  Active   Active   Max Header
         Server ID  Rx Rate     Tx Rate     Rx Rate  Tx Rate  Size
 ------  ---------  ----------  ----------  -------  -------  -----------
 1:1     1          0           0           0        0        128

Total Entries: 1

DGS-3000-28SC:admin#
```

Chapter 84 Simple Network Management Protocol (SNMP) Command List

enable community_encryption
disable community_encryption
show community encryption
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 community_masking view <view_name 32> [read_only | read_write]
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
config snmp trap_port [<portlist> | all] state [enable | disable]
show snmp trap_port [<portlist> | all]
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

84-1 enable community_encryption

Description

This command is used to enable the encryption state on the SNMP community string.

Format

enable community_encryption

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To enable the encryption state on an SNMP community string:

```
DGS-3000-28SC:admin# enable community_encryption
Command: enable community_encryption

Success.

DGS-3000-28SC:admin#
```

84-2 disable community_encryption

Description

This command is used to disable the encryption state on the SNMP community string.

Format

disable community_encryption

Parameters

None.

Restrictions

Only Administrators can issue this command.

Example

To disable the encryption state on the SNMP community string:

```
DGS-3000-28SC:admin# disable community_encryption
Command: disable community_encryption

Success.

DGS-3000-28SC:admin#
```

84-3 show community_encryption

Description

This command is used to display the encryption state on the SNMP community string.

Format

show community_encryption

Parameters

None.

Restrictions

None.

Example

To show the encryption state on the SNMP community string:

```
DGS-3000-28SC:admin# show community_encryption
Command: show community_encryption

SNMP Community Encryption State : Enabled

DGS-3000-28SC:admin#
```

84-4 create snmp community

Description

This command is used to create an SNMP community string.

Use an SNMP community string to define the relationship between the SNMP manager and the agent. The community string acts like a password to permit access to the agent on the Switch. You can specify one or more of the following characteristics associated with the string:

An access list of IP addresses of the SNMP managers that are permitted to use the community string to gain access to the agent.

A MIB view, which defines the subset of all MIB objects accessible to the given community.

Read and write or read-only permission for the MIB objects accessible to the community.

Format

create snmp community <community_string 32> view <view_name 32> [read_only | read_write]

Parameters

<community_string 32> - Enter the community string value here. This string can be up to 32 characters long.
view_name - Specify the view name of the MIB. **<view_name 32>** - Enter the MIB view name here. This name can be up to 32 characters long.
read_only - 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.
read_write - 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-3000-28SC:admin#create snmp community System view CommunityView read_only
Command: create snmp community System view CommunityView read_only

Success.

DGS-3000-28SC:admin#
```

84-5 delete snmp community

Description

This command is used to delete an SNMP community string.

Format

delete snmp community <community_string 32>

Parameters

<community_string 32> - Enter the community string value 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-3000-28SC:admin#delete snmp community System
Command: delete snmp community System

Success.

DGS-3000-28SC:admin#
```

84-6 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) Enter the Community string.
If no parameter is specified, all community string information will be displayed.

Restrictions

None.

Example

To display SNMP community:

```
DGS-3000-28SC: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-3000-28SC:admin#
```

84-7 create snmp community_masking view

Description

This command is used to choose a security method for creating an SNMP community string, but the community string encrypted or not depends on the SNMP community encryption state.

If users use this command to create an SNMP community string, the community string that the user inputs will be displayed as "*", and the user will have to double input (confirm) the SNMP community string when creating an SNMP community.

Format

create snmp community_masking view <view_name 32> [read_only | read_write]

Parameters

<view_name 32> - Enter the MIB view name used here. This name can be up to 32 characters long.
read_only - Specify that the user, using the community string, will have read only access to the switch's SNMP agent.
read_write - Specify that the user, using the community string, will have read/write access to the switch's SNMP agent.

Restrictions

Only Administrators can issue this command.

Example

To create an SNMP community string called "community123" with the "read_only" security method:

```
DGS-3000-28SC:admin# create snmp community_masking view CommunityView read_only
Command: create snmp community_masking view CommunityView read_only

Enter a case-sensitive community:************
Enter the community again for confirmation:************

Success.

DGS-3000-28SC:admin#
```

84-8 create snmp user

Description

This command is used to create a new user to an SNMP group originated by this command.

Format

create snmp user <user_name 32> <groupname 32> {encrypted [by_password auth [md5 <auth_password 8-16> | sha <auth_password 8-20>] priv [none | des <priv_password 8-16>] | by_key auth [md5 <auth_key 32-32> | sha <auth_key 40-40>] priv [none | des <priv_key 32-32>]]}

Parameters

<user_name 32> - Enter the name of the user on the host that connects to the agent. The name can be up to 32 characters long.

<groupname 32> - Enter the name of the group to which the user is associated. The name can be up to 32 characters long.

encrypted - (Optional) Specify whether the password appears in encrypted format.
- **by_password** - 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** - A privacy key used by DES. It is hex string type.
    - **none** - Specify that no encryption will be used for the privacy key.
    - **des** - Specify 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** - 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** - A privacy key used by DES, it is hex string type.
    - **none** - Specify that no encryption will be used for the privacy key.
    - **des** - Specify 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-3000-28SC: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-3000-28SC:admin#
```

84-9 delete snmp user

Description

This command is used to remove a user from an SNMP group and delete the associated group in SNMP group.

Format

delete snmp user <username 32>

Parameters

<username 32> - Enter the name of the user on the host that connects to the agent. The name can be up to 32 characters long.

Restrictions

Only Administrators can issue this command.

Example

To delete a SNMP user “user123”:

```
DGS-3000-28SC:admin#delete snmp user user123
Command: delete snmp user user123

Success.

DGS-3000-28SC:admin#
```

84-10 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-3000-28SC: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-3000-28SC:admin#
```

84-11 create snmp group

Description

This command is used to create a new SNMP group, or a table that maps SNMP users to SNMP views.

Format

create snmp group <groupname 32> [v1 | v2c | v3 [noauth_nopriv | auth_nopriv | auth_priv]] {read_view <view_name 32> | write_view <view_name 32> | notify_view <view_name 32>}

Parameters

<groupname 32> - Enter the group name here. This name can be up to 32 characters long.
v1 - 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) Specify 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) Specify that the view name would be write. **<view_name 32>** - Enter the wite view name here. This name can be up to 32 characters long.
notify_view - (Optional) Specify 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-3000-28SC: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-3000-28SC:admin#
```

84-12 delete snmp group

Description

This command is used to remove a SNMP group.

Format

delete snmp group <groupname 32>

Parameters

<groupname 32> - Enter the group name to be deleted.

Restrictions

Only Administrators can issue this command.

Example

To delete SNMP group “group123”:

```
DGS-3000-28SC:admin#delete snmp group group123
Command: delete snmp group group123

Success.

DGS-3000-28SC:admin#
```

84-13 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-3000-28SC:admin#show snmp groups
Command: show snmp groups

Vacm Access Table Settings

Group    Name      : public
ReadView Name     : CommunityView
WriteView Name    :
Notify View Name : CommunityView
Securiy Model     : SNMPv1
Securiy Level     : NoAuthNoPriv

Group    Name      : public
ReadView Name     : CommunityView
WriteView Name    :
Notify View Name : CommunityView
Securiy Model     : SNMPv2
Securiy Level     : NoAuthNoPriv

Group    Name      : initial
ReadView Name     : restricted
WriteView Name    :
Notify View Name : restricted
Securiy Model     : SNMPv3
Securiy Level     : NoAuthNoPriv

Group    Name      : WriteGroup
ReadView Name     : CommunityView
WriteView Name    : CommunityView
Notify View Name : CommunityView
Securiy Model     : SNMPv2
Securiy Level     : NoAuthNoPriv

Total Entries: 10

DGS-3000-28SC:admin#
```

84-14 create snmp view

Description

This command is used to assign views to community strings to limit which MIB objects an SNMP manager can access.

Format

create snmp view <view_name 32> <oid> view_type [included | excluded]

Parameters

<view_name 32> - Enter the view name here. The name can be up to 32 characters long.
<oid> - Enter the object-Identified tree, or MIB tree.
view_type - Specify 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-3000-28SC:admin#create snmp view view123 1.3.6 view_type included
Command: create snmp view view123 1.3.6 view_type included

Success.

DGS-3000-28SC:admin#
```

84-15 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 - Specify that all view records will be removed.
<oid> - Enter the Object-Identified tree, or MIB tree.

Restrictions

Only Administrators can issue this command.

Example

To delete SNMP view “view123”:

```
DGS-3000-28SC:admin#delete snmp view view123 all
Command: delete snmp view view123 all

Success.

DGS-3000-28SC:admin#
```

84-16 show snmp view

Description

This command is used to display the SNMP view record.

Format

show snmp view {<view_name 32>}

Parameters

<view_name 32> - (Optional) Enter the view name to be displayed. The name can be up to 32 characters long.

Restrictions

None.

Example

To show SNMP view:

```
DGS-3000-28SC: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-3000-28SC:admin#
```

84-17 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 - Specify the recipient for which the traps are targeted. **<ipaddr>** - Enter the IP address of the recipient for which the traps are targeted.
v6host - Specify the IPv6 host address to which the trap packet will be sent. **<ipv6addr>** - Enter the IPv6 address of the recipient for which the traps are targeted.
v1 - Specify that SNMPv1 will be used. The is the least secure of the possible security models.
v2c - Specify that SNMPv2c will be used. This is the second least secure of the possible security models.
v3 - Specify that SNMPv3 will be used. This is the most secure of the possible security models. **noauth_nopriv** - Neither supports packet authentication nor encryption. **auth_nopriv** - Supports packet authentication. **auth_priv** - Supports packet authentication and encryption.
<auth_string 32> - Enter the authentication string. If the v1 or v2 is specified, the auth_string presents the community string, and it must be one of the entries in the community table. If the v3 is specified, the auth_string presents the user name, and it must be one of the entries in the user table.

Restrictions

Only Administrators can issue this command.

Example

To create SNMP host “10.0.0.1” with community string “public”:

```
DGS-3000-28SC:admin#create snmp host 10.0.0.1 v1 public
Command: create snmp host 10.0.0.1 v1 public

Success.

DGS-3000-28SC:admin#
```

84-18 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-3000-28SC:admin#delete snmp host 10.0.0.1
Command: delete snmp host 10.0.0.1

Success.

DGS-3000-28SC:admin#
```

84-19 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 is specified, all SNMP hosts will be displayed.

Restrictions

None.

Example

To show SNMP host:

```
DGS-3000-28SC: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-3000-28SC:
```

84-20 show snmp v6host

Description

This command is used to display the SNMP version 6 hosts.

Format

show snmp v6host {<ipv6addr>}

Parameters

<ipv6addr> - (Optional) Enter the IPv6 host address used for the configuration here. If no parameter is specified, SNMP version 6 hosts will be displayed.

Restrictions

None.

Example

To show SNMP v6 host:

```
DGS-3000-28SC: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-3000-28SC:admin#
```

84-21 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-3000-28SC:admin#config snmp engineID 1023457890
Command: config snmp engineID 1023457890

Success.

DGS-3000-28SC:admin#
```

84-22 show snmp engineID

Description

This command is used to display the identification of the SNMP engine on the Switch. The default value is suggested in RFC2271. The very first bit is 1, and the first four octets are set to the binary equivalent of the agent’s SNMP management private enterprise number as assigned by IANA, D_Link is 171. The fifth octet is 03 to indicates the rest is the MAC address of this device. The 6th –11th octets is MAC address.

Format

show snmp engineID

Parameters

None.

Restrictions

None.

Example

To show SNMP engine ID:

```
DGS-3000-28SC:admin#show snmp engineID
Command: show snmp engineID

SNMP Engine ID : 1023457890

DGS-3000-28SC:admin#
```

84-23 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-3000-28SC:admin#enable snmp
Command: enable snmp

Success.

DGS-3000-28SC:admin#
```

84-24 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-3000-28SC:admin#disable snmp
Command: disable snmp

Success.

DGS-3000-28SC:admin#
```

84-25 config snmp trap_port

Description

This command is used to configure the per port's SNMP trap state. The default port trap state is enabled for each port.

Format

config snmp trap_port [<portlist> | all] state [enable | disable]

Parameters

<portlist> - Enter to config the SNMP trap port.
all - Specify all the SNMP trap ports.
state - Specify each SNMP trap state port, the default port trap state is enable for each port. **enable** - Specify to enable the SNMP trap port state. **disable** - Specify to disable the SNMP trap port state.

Restrictions

Only Administrators can issue this command.

Example

To configure the SNMP trap port state:

```
DGS-3000-28SC:admin# config snmp trap_port all state enable
Command: config snmp trap_port all state enable

Success.

DGS-3000-28SC:admin#
```

84-26 show snmp trap_port

Description

This command is used to display the SNMP trap_port state.

Format

show snmp trap_port [<portlist> | all]

Parameters

<portlist> - Enter to config the SNMP trap port.
all - Specify all the SNMP trap ports.

Restrictions

Only Administrators can issue this command.

Example

To show the port state of SNMP trap:

```
DGS-3000-28SC:admin# admin#show snmp trap_port all
Command: show snmp trap_port all

 Port                    Trap State
-----                   -------------
  1                      Enabled
  2                      Enabled
  3                      Enabled
  4                      Enabled
  5                      Enabled
  6                      Enabled
  7                      Enabled
  8                      Enabled
  9                      Enabled
  10                     Enabled

CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

84-27 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-3000-28SC”:

```
DGS-3000-28SC:admin#config snmp system_name DGS-3000-28SC
Command: config snmp system_name DGS-3000-28SC

Success.

DGS-3000-28SC:admin#
```

84-28 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-3000-28SC:admin#config snmp system_location HQ 5F
Command: config snmp system_location HQ 5F

Success.

DGS-3000-28SC:admin#
```

84-29 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-3000-28SC:admin#config snmp system_contact "MIS Department II"
Command: config snmp system_contact "MIS Department II"

Success.

DGS-3000-28SC:admin#
```

84-30 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-3000-28SC:admin#enable snmp traps
Command: enable snmp traps

Success.

DGS-3000-28SC:admin#
```

84-31 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-3000-28SC:admin#disable snmp traps
Command: disable snmp traps

Success.

DGS-3000-28SC:admin#
```

84-32 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-3000-28SC:admin#enable snmp authenticate_traps
Command: enable snmp authenticate_traps

Success.

DGS-3000-28SC:admin#
```

84-33 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-3000-28SC:admin#disable snmp authenticate_traps
Command: disable snmp authenticate_traps

Success.

DGS-3000-28SC:admin#
```

84-34 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-3000-28SC:admin#enable snmp linkchange_traps
Command: enable snmp linkchange_traps

Success.

DGS-3000-28SC:admin#
```

84-35 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-3000-28SC:admin#disable snmp linkchange_traps
Command: disable snmp linkchange_traps

Success.

DGS-3000-28SC:admin#
```

84-36 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 - Specify that all ports will be used.
<portlist> - Enter the range of ports used.
enable - Specify to enable the sending of the link change trap for this port.
disable - Specify to disable 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-3000-28SC:admin#config snmp linkchange_traps ports 1-4 enable
Command: config snmp linkchange_traps ports 1-4 enable

Success.

DGS-3000-28SC:admin#
```

84-37 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 - Specify to enable the trap of the coldstart event. The default state is enabled.
disable - Specify to disable the trap of the coldstart event.

Restrictions

Only Administrators can issue this command.

Example

To configure the trap for coldstart event:

```
DGS-3000-28SC:admin#config snmp coldstart_traps enable
Command: config snmp coldstart_traps enable

Success.

DGS-3000-28SC:admin#
```

84-38 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 - Specify to enable the trap of the warmstart event. The default state is enabled.
disable - Specify to disable the trap of the warmstart event.

Restrictions

Only Administrators can issue this command.

Example

To configure the trap state for warmstart event:

```
DGS-3000-28SC:admin#config snmp warmstart_traps enable
Command: config snmp warmstart_traps enable

Success.

DGS-3000-28SC:admin#
```

84-39 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) Specify that the SNMP trap sending status will be displayed.

ports - (Optional) Specify the ports for the display. **<portlist>** - Enter the list of ports used for the display here.

Restrictions

None.

Example

```
DGS-3000-28SC:admin#show snmp traps
Command: show snmp traps

SNMP Traps         : Enabled
Authenticate Trap  : Enabled
Linkchange Traps   : Enabled
Coldstart Traps    : Enabled
Warmstart Traps    : Enabled

DGS-3000-28SC:admin#
```

84-40 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 - Specify the trap state for rising alarm. The default state is enabled. **enable** - Specify that the rising alarm function will be enabled. **disable** - Specify that the rising alarm function will be disabled.
falling_alarm - Specify the trap state for falling alarm. The default state is enabled. **enable** - Specify that the falling alarm function will be enabled. **disable** - Specify 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-3000-28SC:admin#config rmon trap rising_alarm disable
Command: config rmon trap rising_alarm disable

Success.

DGS-3000-28SC:admin#
```

84-41 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-3000-28SC:admin#show rmon
Command: show rmon

RMON Rising Alarm Trap      : Enabled
RMON Falling Alarm Trap     : Enabled

DGS-3000-28SC:admin#
```

Chapter 85 Simple RED Command List

enable sred
disable sred
config sred [<portlist> | all] [<class_id 0-7> | all] {threshold {low <value 0-100> | high <value 0-100>} | drop_rate {low <value 1-8> | high <value 1-8>} | drop_green [enable | disable]}
show sred {<portlist> {<class_id 0-7>}}
show sred drop_counter {<portlist>}

85-1 enable sred

Description

This command is used to enable the sRED function. By default, sRED is disabled.

Format

enable sred

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable sRED:

```
DGS-3000-28SC:admin#enable sred
Command: enable sred

Success.

DGS-3000-28SC:admin#
```

85-2 disable sred

Description

This command is used to disable the sRED function.

Format

disable sred

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To disable sRED:

```
DGS-3000-28SC:admin#disable sred
Command: disable sred

Success.

DGS-3000-28SC:admin#
```

85-3 config sred

Description

This command is used to configure the sRED port's queue settings.

Format

config sred [<portlist> | all] [<class_id 0-7> | all] {threshold {low <value 0-100> | high <value 0-100>} | drop_rate {low <value 1-8> | high <value 1-8>} | drop_green [enable | disable]}

Parameters

<portlist> - Enter the list of ports, used for this configuration, here.
all - Specify that all the ports will be used.
<class_id 0-7> - Enter the CoS Class ID used here. This value must be between 0 and 7.
all - Specify that all the CoS Class ID will be used.
threshold - (Optional) Specify the threshold of the percent of space utilized. **low** - (Optional) Specify the low threshold value used. **<value 0-100>** - Enter the low threshold value used here. This value must be between 0 and 100. **high** - (Optional) Specify the high threshold value used. **<value 0-100>** - Enter the high threshold value used here. This value must be between 0 and 100.
drop_rate - (Optional) Specify the drop rate value used. **low** - (Optional) Specify the low drop rate value used. **<value 1-8>** - Enter the low drop rate value used here. This value must be between 1 and 8. **high** - (Optional) Specify the high drop rate value used. **<value 1-8>** - Enter the high drop rate value used here. This value must be between 1 and 8. (Note: There are 8 drop rates: 1=100%; 2=6.25%; 3=3.125%; 4= 1.5625%; 5= 0.78125%; 6=0.390625%; 7= 0.1953125%; 8= 0.09765625%)
drop_green - (Optional) Specify the drop green parameters. **enable** - Probabilistic drop yellow and red colored packets if the queue depth is above the low threshold, and probabilistic drop green colored packets if the queue depth is above the high threshold.

disable - Probabilistic drop red colored packets if the queue depth is above the low threshold, and probabilistic drop yellow colored packets if the queue depth is above the high threshold.

Restrictions

Only Administrators, Operators and Power users can issue this command.

Example

To configure threshold low 40 percentage of congestion limit and threshold high 70 percentage of congestion limit of all port's queue.:

```
DGS-3000-28SC:admin# config sred all all threshold low 40 high 70

Command: config sred all all threshold low 40 high 70

Success.

DGS-3000-28SC:admin#
```

85-4 show sred

Description

This command is used to display the current thresholds (per port and per queue) parameters in use on the Switch

Format

show sred {<portlist> {<class_id 0-7>}}

Parameters

<portlist> - (Optional) Enter the list of port used for the display.
<class_id 0-7> - (Optional) Enter which of the hardware CoS queues to display.
If no parameter is specified, then all information will be displayed.

Restrictions

None.

Example

To display the configuration of port 1:

```
DGS-3000-28SC:admin# sred 1
Command: show sred 1

Simple RED Globale Status: Enabled

Port Class Drop Green Threshold Drop Rate
                            Low   High Low  High
---- -----  --------- ----  ---- ---- ---- ----
1     0       Disabled   40     70    1     1
1     1       Disabled   40     70    1     1
1     2       Disabled   40     70    1     1
1     3       Disabled   40     70    1     1
1     4       Disabled   40     70    1     1
1     5       Disabled   40     70    1     1
1     6       Disabled   40     70    1     1
1     7       Disabled   40     70    1     1
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

85-5 show sred drop_counter

Description

This command is used to display the drop count of threshold low and high per port basis. No parameter input will display all ports.

Format

show sred drop_counter {<portlist>}

Parameters

<portlist> - (Optional) Enter the list of port used for the display.
If no parameter is specified, then all information will be displayed.

Restrictions

None.

Example

To display the dropped packet count of egress ports:

```
DGS-3000-28SC:admin#show sred drop_counter 1-5
Command: show sred drop_counter 1-5

Port  Yellow          Red
----  --------------  ---------------
1     0               0
2     0               0
3     0               0
4     0               0
5     0               0
6     0               0
7     0               0
8     0               0
9     0               0
10    0               0
11    0               0
12    0               0

DGS-3000-28SC:admin#
```

Chapter 86 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]

86-1 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-3000-28SC:admin#enable sim
Command: enable sim

Success.

DGS-3000-28SC:admin#
```

86-2 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-3000-28SC:admin#disable sim
Command: disable sim

Success.

DGS-3000-28SC:admin#
```

86-3 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) Specify the candidate devices. **<candidate_id 1-100>** - (Optional) Enter the candidate device ID here. This value must be between 1 and 100.
members - (Optional) Specify the member devices. **<member_id 1-32>** - (Optional) Enter the member device ID here. This value must be between 1 and 32.
group - (Optional) Specify other group devices. **commander_mac** - (Optional) Specify the commander MAC address used. **<macaddr>** - Enter the commander MAC address used here.
neighbor - (Optional) Specify other neighbor devices.

Restrictions

None.

Example

To show the self information in detail:

```
DGS-3000-28SC:admin#show sim
Command: show sim

SIM Version        : VER-1.61
Firmware Version   : 5.00.020
Device Name        :
MAC Address        : 00-01-02-03-04-00
Capabilities       : L2
Platform           : DGS-3000-28SC L2 Switch
SIM State          : Disabled
Role State         : Candidate
Discovery Interval : 30 sec
Hold Time          : 100 sec

DGS-3000-28SC:admin#
```

To show the candidate information in summary, if user specify candidate id, it would show information in detail:

```
DGS-3000-28SC:admin#show sim candidates
Command: show sim candidates

ID  MAC Address       Platform /              Hold  Firmware  Device Name
                      Capability              Time  Version
--- ----------------- ----------------------- ----- --------- ----------------
1  00-01-02-03-04-00 DGS-3000-28SC L2 Switch  40    5.00.020  Device
2  00-55-55-00-55-00 DGS-3000-28SC L2 Switch  140   5.00.020  Device2

Total Entries: 2

DGS-3000-28SC:admin#
```

To show the member information in summary, if user specify member id, it will show information in detail:

```
DGS-3000-28SC:admin#show sim members
Command: show sim members

ID  MAC Address       Platform /               Hold  Firmware  Device Name
                      Capability               Time  Version
--- ----------------- ------------------------ ----- --------- ----------------
1  00-01-02-03-04-00 DGS-3000-28SC L2 Switch   40    5.00.020  Device
2  00-55-55-00-55-00 DGS-3000-28SC L2 Switch   140   5.00.020  Device2

Total Entries: 2

DGS-3000-28SC:admin#
```

To show other groups information in summary, if user specify group name, it will show information in detail:

```
DGS-3000-28SC:admin#show sim group
Command: show sim group

SIM Group Name : default

ID  MAC Address         Platform /            Hold  Firmware Device Name
                        Capability            Time  Version
--- ----------------- ------------------------ ----- --------- ----------------
*1  00-01-02-03-04-00 DGS-3000-28SC L2 Switch  40    5.00.020  Device
 2  00-55-55-00-55-00

SIM Group Name : SIM2

ID  MAC Address          Platform /           Hold  Firmware Device Name
                         Capability           Time  Version
--- ----------------- ------------------------ ----- --------- ----------------
*1 00-01-02-03-04-00  DGS-3000-28SC L2 Switch  40    5.00.020  Device
 2 00-55-55-00-55-00
 3 00-55-55-00-55-11

Total Entries: 2

DGS-3000-28SC:admin#
```

To show neighbor table of SIM:

```
DGS-3000-28SC:admin#show sim neighbor
Command: show sim neighbor

Neighbor Info Table

Port    MAC Address         Role
------  ------------------  ---------
23      00-35-26-00-11-99   Commander
23      00-35-26-00-11-91   Member
24      00-35-26-00-11-90   Candidate

Total Entries: 3

DGS-3000-28SC:admin#
```

86-4 reconfig

Description

This command is used to re-Telnet to member.

Format

reconfig {member_id <value 1-32> | exit}

Parameters

member_id - (Optional) Specify the serial number of the member. **<value 1-32>** - Enter the serial number of the member here.
exit - (Optional) Specify to exit from the Telnet session.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To re-Telnet to member:

```
DGS-3000-28SC:admin#reconfig member_id 1
Command: reconfig member_id 1

DGS-3000-28SC:admin#

                    DGS-3000-28SC Gigabit Ethernet Switch
                           Command Line Interface

                          Firmware: Build 5.00.020
          Copyright(C) 2014 D-Link Corporation. All rights reserved.
UserName:
PassWord:
```

86-5 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 - Specify 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 - Specify 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-3000-28SC:admin#config sim_group add 2
Command: config sim_group add 2

Please wait for ACK !!!
SIM Configure Success !!!

Success.

DGS-3000-28SC:admin#
```

To delete a member:

```
DGS-3000-28SC:admin#config sim_group delete 1
Command: config sim_group delete 1

Please wait for ACK !!!
SIM Configure Success !!!

Success.

DGS-3000-28SC:admin#
```

86-6 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 - Specify to transfer the role to the commander. **group_name** - (Optional) Specify 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 - Specify to transfer the role to the candidate.
dp_interval - 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 - 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-3000-28SC:admin#config sim commander
Command: config sim commander

Success.

DGS-3000-28SC:admin#
```

To transfer to candidate:

```
DGS-3000-28SC:admin#config sim candidate
Command: config sim candidate

Success.

DGS-3000-28SC:admin#
```

To update name of group:

```
DGS-3000-28SC:admin#config sim commander group_name mygroup
Command: config sim commander group_name mygroup

Success.

DGS-3000-28SC:admin#
```

To change the time interval of discovery protocol:

```
DGS-3000-28SC:admin#config sim dp_interval 30
Command: config sim dp_interval 30

Success.

DGS-3000-28SC:admin#
```

To change the hold time of discovery protocol:

```
DGS-3000-28SC:admin#config sim hold_time 200
Command: config sim hold_time 200

Success.

DGS-3000-28SC:admin#
```

86-7 download sim_ms

Description

This command is used to download firmware or configuration from TFTP server to indicated devices.

Format

download sim_ms [firmware_from_tftp | configuration_from_tftp] <ipaddr> <path_filename> {[members <mslist 1-32> | all]}

Parameters

firmware_from_tftp - Specify to download firmware from a TFTP server.

configuration_from_tftp - Specify to download configuration from a TFTP server.
<ipaddr> - Enter the IP address of the TFTP server.
<path_filename> - Enter the file path of firmware or configuration in the TFTP server.
members - (Optional) Specify a range of members which download this firmware or configuration. **<mslist 1-32>** - Enter a range of members which download this firmware or configuration.
all - (Optional) Specify all members which download this firmware or configuration.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To download firmware:

```
DGS-3000-28SC:admin# download sim_ms firmware_from_tftp 10.55.47.1
D:\firmware.had members 1
Commands: download sim_ms firmware_from_tftp 10.55.47.1 D:\firmware.had 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
2   00-07-06-05-04-03  Transfer Fail

DGS-3000-28SC:admin#
```

To download configuration:

```
DGS-3000-28SC:admin# download sim_ms configuratin_from_tftp 10.55.47.1
D:\config.cfg
Commands: download sim_ms configuration_from_tftp 10.55.47.1 D:\config.cfg

This device is updating configuration.  Please wait several minutes...

Download Status :

ID   MAC Address        Result
---  -----------------  ----------------
1   00-01-02-03-04-00  Success
2   00-07-06-05-04-03  Transfer Fail
3   00-07-06-05-04-03  Transfer Fail

DGS-3000-28SC:admin#
```

86-8 upload sim_ms

Description

This command is used to upload configuration or logs from indicated devices to the TFTP server.

Format

upload sim_ms [configuration_to_tftp | log_to_tftp] <ipaddr> <path_filename> {[members <mslist> | all]}

Parameters

configuration_to_tftp - Specify to upload configuration to a TFTP server.
log_to_tftp - Specify to upload a log to a TFTP server.
<ipaddr> - Enter the IPv4 address of TFTP server.
<path_filename> - Enter the file path to store configuration in TFTP server.
members - (Optional) Specifiy the members which upload its configuration. **<mslist>** - Enter the members which upload its configuration.The value is from 1 to 32.
all - (Optional) Specify all members which upload its configuration.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To upload configuration:

```
DGS-3000-28SC:admin#upload sim_ms configuration_to_tftp 10.55.47.1 D:\config.cfg
members 1
Command: upload sim_ms configuration_to_tftp 10.55.47.1 D:\config.cfg members 1

This device is uploading configuration. Please wait several minutes ...

Upload Status :
ID   MAC Address          Result
---  ----------------- ----------------
1    00-01-02-03-04-00    Success

DGS-3000-28SC:admin#
```

86-9 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 - Specify to enable the trap state.
disable - Specify to disable the trap state.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable SIM trap:

```
DGS-3000-28SC:admin#config sim trap enable
Command: config sim trap enable

Success.

DGS-3000-28SC:admin#
```

Chapter 87 Stacking Command List

config box_priority current_box_id <value 1-6> priority <value 1-63>
config box_id current_box_id <value 1-6> new_box_id [auto | <value 1-6>]
config stacking force_master_role state [enable | disable]
config stacking log state [enable | disable]
config stacking trap state [enable | disable]
config stacking_mode [disable | enable]
show stack_device
show stack_information
show stacking_mode

87-1 config box_priority current_box_id

Description

This command is used to configure the priority of switch, which will determines which box becomes master. A lower number means a higher priority. The new priority will take effect after the Switch was rebooted or when the topology changed.

Format

config box_priority current_box_id <value 1-6> priority <value 1-63>

Parameters

<value 1-6> - Enter the current box ID of the Switch here. This value must be between 1 and 6.
priority - Specify the priority assigned to the box, with lower number meaning higher priority. The range is 1-63. **<value 1-63>** - Enter the higher priority value here. This value must be between 1 and 63.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure box priority:

```
DGS-3000-28SC:admin# config box_priority current_box_id 1 priority 1
Command: config box_priority current_box_id 1 priority 1

Success.

DGS-3000-28SC:admin#
```

87-2 config box_id current_box_id

Description

This command is used to configure the box ID. By default, the box ID is automatically assigned by the system based topology election results. Administrators can assign box IDs statically. The new box ID will take effect after unit reboot. Each unit in the Switch stack must have a unique box IDs. If the IDs duplicate, the stack system cannot stack normally.

Format

config box_id current_box_id <value 1-6> new_box_id [auto | <value 1-6>]

Parameters

<value 1-6> - Enter the current box ID of the Switch here. This value must be between 1 and 6.
new_box_id - Specify the new ID assigned to the box. **auto** - Allows the box ID to be assigned automatically by the stack system. The new box ID will take effect after the next boot. **<value 1-6>** - Enter the new box ID here. This value must be between 1 and 6.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable SIM:

```
DGS-3000-28SC:admin# config box_id current_box_id 1 new_box_id auto
Command: config box_id current_box_id 1 new_box_id auto

Success.

DGS-3000-28SC:admin#
```

87-3 config stacking force_master_role state

Description

This command is used to configure the stacking force master role state. If the state is enabled, when device is in election state, it still uses old priority setting and MAC to compare device priority. After stacking is stable, master's priority will become zero. If stacking topology change again, Master will use priority zero and MAC address to determine who new primary master is.

Format

config stacking force_master_role state [enable | disable]

Parameters

enable - Specify that switch's stacking force master role will be enabled.
disable - Specify that switch's stacking force master role will be disabled.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable stacking force master role state:

```
DGS-3000-28SC:admin# config stacking force_master_role state enable
Command: config stacking force_master_role state enable

Success.

DGS-3000-28SC:admin#
```

87-4 config stacking log state

Description

This command is used to configure log state for stacking.

Format

config stacking log state [enable | disable]

Parameters

enable - Specify to enable the Switch's stacking log.
disable - Specify to disable the Switch's stacking log.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable the stacking log state:

```
DGS-3000-28SC:admin# config stacking log state enable
Command: config stacking log state enable

Success.

DGS-3000-28SC:admin#
```

87-5 config stacking trap state

Description

This command is used to configure trap state for stacking.

Format

config stacking trap state [enable | disable]

Parameters

enable - Specify to enable the Switch's stacking trap.
disable - Specify to disable the Switch's stacking trap.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable the stacking trap state:

```
DGS-3000-28SC:admin# config stacking trap state enable
Command: config stacking trap state enable

Success.

DGS-3000-28SC:admin#
```

87-6 config stacking_mode

Description

This command is used to configure the stacking mode.

Format

config stacking_mode **[disable | enable]**

Parameters

enable - Specify to enable the Switch's stacking mode.
disable - Specify to disable the Switch's stacking mode.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable stacking mode:

```
DGS-3000-28SC:admin# config stacking_mode enable
Command: config stacking_mode enable

Changing the stacking mode may cause the device to restart. Do you still want
to continue?(y/n)  y
Please wait, the switch is rebooting...

DGS-3000-28SC:admin#
```

87-7 show stack_device

Description

This command is used to display the information for devices in the stack.

Format

show stack_device

Parameters

None.

Restrictions

None.

Example

To display the stack information:

```
DGS-3000-28SC:admin# show stack_device
Command: show stack_device

Box ID  Box Type           H/W Version  Serial Number
------  ----------------   -----------  --------------------
1       DGS-3000-28SC      A1           PVT93CB000001

DGS-3000-28SC:admin#
```

87-8 show stack_information

Description

This command is used to display stacking information.

There are five messages defined for stack topology status displayed by show stack_information, beside the basic information of stack devices.

Message 1:

Stack Topology Status: Topology will change from Chain to Ring after n seconds.

When this message is shown, it means the topology change is detected; the topology change process will take place after the count down timer reaches 0. If topology change is detected again before the count down timer reaches 0, the count down timer will be restarted.

Message 2:

Stack Topology Status: New device is detected; hot insert may happen after n seconds.

When this message is shown, it means hot insert of new device is detected. The stack system will do the hot insert action after the timer reaches 0. If topology change is detected again before the count down timer reaches 0, the count down timer will be reset. It is suggested for the user not to do any command regarding read /write of flash, for example:”download firmware”,”save”,”show config in flash”,”upload”,”copy”,”show slave’s dangerous log”.

Message 3:

Stack Topology Status: Configuring the new device.

When this message is shown, it means stacking has started to do the hot insert action. Now the system is configuring the new device, and the user can not execute any command except “show stack_ information”.

Message 4: Stack Topology Status: Topology will change from Ring to Chain after n seconds.

when this message is shown, it means the topology change is detected; and the topology change process will be took place after the count down timer reaches 0. If topology change is detected again before the count down timer reaches 0, the count down timer will be restart.

Message 5: Stack Topology Status:Hot remove happen.

When this message is shown, it means stacking has detected one or more switches hot removed.

If no message shown means the topology is stable and the system operation is normally.

Format

show stack_information

Parameters

None.

Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

Example

To display the stack information:

```
DGS-3000-28SC:admin# show stack_information
Command: show stack_information


Topology            : Duplex_Chain
My Box ID           : 1
Master ID           : 1
Box Count           : 1

Force Master Role   : Disabled
Trap State          : Enabled
Log State           : Enabled

Box User                         Prio-                 Prom     Runtime  H/W
ID  Set     Type           Exist rity        MAC       version  version
version
--- ---- ---------------- ----- --- ----------------- -------- --------- -----
1   Auto DGS-3000-28SC     Exist 32  00-01-02-03-04-00 5.00.003 5.00.020 A1
2   -    NOT_EXIST         No
3   -    NOT_EXIST         No
4   -    NOT_EXIST         No
5   -    NOT_EXIST         No
6   -    NOT_EXIST         No

DGS-3000-28SC:admin#
```

87-9 show stacking_mode

Description

This command is used to display the current stacking mode.

Format

show stacking_mode

Parameters

None.

Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

Example

To display stacking mode:

```
DGS-3000-28SC:admin# show stacking_mode
Command: show stacking_mode

Stacking mode  : Enabled

DGS-3000-28SC:admin#
```

Chapter 88 Surveillance VLAN Command List

enable surveillance_vlan [<vlan_name 32> | vlanid <vlanid 1-4094>]
disable surveillance_vlan
config surveillance_vlan aging_time <min 1-65535>
config surveillance_vlan log state [enable | disable]
config surveillance_vlan oui [add | delete] <macaddr> <macmask> {component_type [vms | vms_client | video_encoder | network_storage | other] description <desc 32>}
config surveillance_vlan ports [<portlist> | all] state [enable | disable]
config surveillance_vlan priority <int 0-7>
show surveillance_vlan {[oui | ports {<portlist>} | device {ports <portlist>}]}

88-1 enable surveillance_vlan

Description

This command is used to enable surveillance VLAN globally. To enable the surveillance VLAN, a name must be assigned to the sureveillance VLAN, and there must be an existing static 802.1Q VLAN. To change the surveillance VLAN ID, the surveillance VLAN function has to be disabled and then re-issue the enable command.

Format

enable surveillance_vlan [<vlan_name 32> | vlanid <vlanid 1-4094>]

Parameters

<vlan_name 32> - Specify the name of surveillance VLAN.
vlanid - Specify the ID of surveillance VLAN. **<vlanid 1-4094>** - Enter the ID of surveillance VLAN.

Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

Example

To enable a surveillance VLAN with the name “v2”:

```
DGS-3000-28SC:admin#enable surveillance_vlan v2
Command: enable surveillance_vlan v2

Success.

DGS-3000-28SC:admin#
```

88-2 disable surveillance_vlan

Description

This command is used to disable surveillance VLAN globally.

Format

disable surveillance_vlan

Parameters

None.

Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

Example

To disable the surveillance VLAN:

```
DGS-3000-28SC:admin#disable surveillance_vlan
Command: disable surveillance_vlan

Success.

DGS-3000-28SC:admin#
```

88-3 config surveillance_vlan aging_time

Description

This command is used to set the aging time of the surveillance VLAN. The aging time is used to remove a port from the surveillance VLAN if the port is an automatic surveillance VLAN member. When the last surveillance device stops sending traffic and the MAC address of this surveillance device is aged out, the surveillance VLAN aging timer will be started. The port will be removed from the surveillance VLAN after expiration of surveillance VLAN aging timer. If the surveillance traffic resumes during the aging time, the aging timer will be reset and stopped.

Format

config surveillance_vlan aging_time <min 1-65535>

Parameters

<min 1-65535> - Specify the aging time. The range is from 1 to 65535 minutes. The default value is 720.

Restrictions

Only Administrators and Operators can issue this command.

Example

To set the aging time of the surveillance VLAN to 60 minutes:

```
DGS-3000-28SC:admin# config surveillance_vlan aging_time 60
Command: config surveillance_vlan aging_time 60

Success.

DGS-3000-28SC:admin#
```

88-4 config surveillance_vlan log state

Description

This command is used to configure the log state of the surveillance VLAN.

Format

config surveillance_vlan log state [enable | disable]

Parameters

enable - Specify to enable the log state of the surveillance VLAN.
disable - Specify to disable the log state of the surveillance VLAN.

Restrictions

Only Administrators and Operators can issue this command.

Example

To enable the log state of the surveillance VLAN:

```
DGS-3000-28SC:admin# config surveillance_vlan log state enable
Command: config surveillance_vlan log state enable

Success.

DGS-3000-28SC:admin#
```

88-5 config surveillance_vlan oui

Description

This command is used to configure the user-defined surveillance traffic OUI. OUI is used by the Switch to identify the surveillance traffic packets. Apart from the pre-defined OUIs, the user can further create user-defined OUI if needed. A user-defined OUI cannot be the same as any of the pre-defined OUI.

Format

config surveillance_vlan oui [add | delete] <macaddr> <macmask> {component_type [vms | vms_client | video_encoder | network_storage | other] description <desc 32>}

Parameters

add - Specify to add a user-defined OUI of a surveillance device vendor.
delete - Specify to remove a user-defined OUI of a surveillance device vendor.
<macaddr> - The user-defined OUI MAC address.
<macmask> - The user-defined OUI MAC address mask.
component_type - (Optional) Specify the surveillance components that could be auto-detected by surveillance VLAN. **vms** - Specify the Video Manage Server (VMS) to be auto-detected by surveillance VLAN. **vms_client** - Specify the VMS client to be auto-detected by surveillance VLAN. **video_encoder** - Specify the video encoder to be auto-detected by surveillance VLAN. **network_storage** - Specify the network storage to be auto-detected by surveillance VLAN. **other** - Specify other surveillance devices to be auto-detected by surveillance VLAN. **description** - Specify the description for the user-defined OUI. **<desc 32>** - Enter the description.

Restrictions

Only Administrators and Operators can issue this command.

Example

To add a user-defined OUI of a surveillance device:

```
DGS-3000-28SC:admin# config surveillance_vlan oui add AA-BB-CC-DD-EF-FF FF-FF-FF-00-00-00 component_type other description abc
Command: config surveillance_vlan oui add AA-BB-CC-DD-EF-FF FF-FF-FF-00-00-00 component_type other description abc

Success.

DGS-3000-28SC:admin#
```

88-6 config surveillance_vlan ports

Description

This command is used to configure the surveillance VLAN state on the specific ports.

Format

config surveillance_vlan ports [<portlist> | all] state [enable | disable]

Parameters

<portlist> - Enter a list of ports to be configured.
all - Specify all ports to be configured.
state - The state of the surveillance VLAN function on the specified ports. **enable** - Specify to enable surveillance VLAN function on the specified ports.

disable - Specify to disable surveillance VLAN function on the specified ports.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure Surveillance VLAN to the enabled state on ports 4-6 of unit 1:

```
DGS-3000-28SC:admin# config surveillance_vlan ports 1:4-1:6 state enable
Command: config surveillance_vlan ports 1:4-1:6 state enable

Success.

DGS-3000-28SC:admin#
```

88-7 config surveillance_vlan priority

Description

This command is used to configure the surveillance VLAN priority which is associated with the surveillance VLAN traffic to distinguish the QoS of the surveillance traffic from the data traffic.

Format

config surveillance_vlan priority <int 0-7>

Parameters

<int 0-7> - Enter the priority of the surveillance VLAN. The range is from 0 to 7. The default priority is 5.

Restrictions

Only Administrators and Operators can issue this command.

Example

To set the priority of the surveillance VLAN to be 6:

```
DGS-3000-28SC:admin# config surveillance_vlan priority 6
Command: config surveillance_vlan priority 6

Success.

DGS-3000-28SC:admin#
```

88-8 show surveillance_vlan

Description

This command is used to display the surveillance VLAN information.

Format

show surveillance_vlan {[oui | ports {<portlist>} | device {ports <portlist>}]}

Parameters

oui - (Optional) The OUI information of the surveillance VLAN.
ports - (Optional) Specify a range of ports to be displayed. **<portlist>** - (Optional) Enter a range of ports to be displayed.
device - (Optional) The Surveillance devices that are learned through their OUI. **ports** - (Optional) Specify a range of ports to be displayed. **<portlist>** - Enter a range of ports to be displayed.

Restrictions

None.

Example

To display the surveillance VLAN global information when surveillance VLAN is enabled:

```
DGS-3000-28SC:admin# show surveillance_vlan
Command: show surveillance_vlan

Surveillance VLAN State : Enabled
VLAN ID                 : 2
VLAN Name               : v2
Priority                : 6
Aging Time              : 60 minutes
Log State               : Enabled
Member Ports            :
Dynamic Member Ports    :

DGS-3000-28SC:admin#
```

Chapter 89 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

89-1 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 - Specify to clear the configured source IP interface.

Restrictions

Only Administrators and Operators can issue this command.

Example

Configure syslog source IP interface:

```
DGS-3000-28SC:admin#config syslog source_ipif ipif3 14.0.0.5
Command: config syslog source_ipif ipif3 14.0.0.5

Success

DGS-3000-28SC:admin#
```

To clear the configured source IP interface for syslog:

```
DGS-3000-28SC:admin#config syslog source_ipif none
Command: config syslog source_ipif none

Success

DGS-3000-28SC:admin#
```

89-2 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-3000-28SC: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-3000-28SC:admin#
```

89-3 config trap source_ipif

Description

This command is used to configure trap source IP interface.

Format

config trap source_ipif [<ipif_name 12> {<ipaddr> | <ipv6addr>} | none]

Parameters

<ipif_name 12> - Enter the IP interface name here. This name can be up to 12 characters long. **<ipaddr>** - (Optional) Enter the IP address used for the configuration here. **<ipv6addr>** - (Optional) Enter the IPv6 address used for the configuration here.
none - Specify to clear the configured source IP interface.

Restrictions

Only Administrators and Operators can issue this command.

Example

Configure trap source IP interface:

```
DGS-3000-28SC:admin#config trap source_ipif System
Command: config trap source_ipif System

Success

DGS-3000-28SC:admin#
```

To clear the configured trap source IP interface:

```
DGS-3000-28SC:admin#config trap source_ipif none
Command: config trap source_ipif none

Success

DGS-3000-28SC:admin#
```

89-4 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-3000-28SC: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-3000-28SC:admin#
```

Chapter 90 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 1-4> | 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 {unit <unit_id 1-6} {index <value_list>}
clear attack_log {[unit <unit_id 1-6> | all]}
config system_severity [trap | log | all] [emergency | alert| critical | error | warning | notice | information | debug | <level 0-7>]
show system_severity

90-1 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-3000-28SC:admin#clear log
Command: clear log

Success.

DGS-3000-28SC:admin#
```

90-2 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) Specify 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) Specify the severity level used. **module** - (Optional) Specify 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>** - (Optional) Enter 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) Specify 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-3000-28SC: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-3000-28SC:admin#
```

90-3 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-3000-28SC:admin# DGS-3000-28SC:admin#show log_software_module
Command: show log_software_module

CFM_EXT             DHCPv6_CLIENT       DHCPv6_RELAY        ERPS
ERROR_LOG           MSTP

DGS-3000-28SC:admin#
```

90-4 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-3000-28SC:admin#enable syslog
Command: enable syslog

Success.

DGS-3000-28SC:admin#
```

90-5 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-3000-28SC:admin#disable syslog
Command: disable syslog

Success.

DGS-3000-28SC:admin#
```

90-6 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-3000-28SC:admin#show syslog
Command: show syslog

Syslog Global State: Enabled

DGS-3000-28SC:admin#
```

90-7 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 - Specify the IP address for the host. **<ipaddr>** - Enter the IP address for the host. **<ipv6addr>** - Enter the IPv6 address for the host.
severity - (Optional) Specify 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** - Specify that the user-defined facility will be set to local 0. **local1** - Specify that the user-defined facility will be set to local 1. **local2** - Specify that the user-defined facility will be set to local 2. **local3** - Specify that the user-defined facility will be set to local 3. **local4** - Specify that the user-defined facility will be set to local 4. **local5** - Specify that the user-defined facility will be set to local 5. **local6** - Specify that the user-defined facility will be set to local 6. **local7** - Specify that the user-defined facility will be set to local 7.	
udp_port - (Optional) Specify 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** - Specify that the host to receive such messages will be enabled. **disable** - Specify 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-3000-28SC: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-3000-28SC:admin#
```

90-8 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 1-4> | 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 1-4> - Enter the host index value here. This value must be between 0 and 4.
all - Specify that all the host indexes will be used.
severity - Specify 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** - Specify that the user-defined facility will be set to local 0. **local1** - Specify that the user-defined facility will be set to local 1. **local2** - Specify that the user-defined facility will be set to local 2. **local3** - Specify that the user-defined facility will be set to local 3. **local4** - Specify that the user-defined facility will be set to local 4. **local5** - Specify that the user-defined facility will be set to local 5. **local6** - Specify that the user-defined facility will be set to local 6. **local7** - Specify that the user-defined facility will be set to local 7.
udp_port - Specify the UDP port number. **<udp_port_number>** - Enter the UDP port number used here.
ipaddress - Specify 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** - Specify that the host to receive such messages will be enabled. **disable** - Specify 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-3000-28SC:admin#config syslog host all severity debug facility local0
Command: config syslog host all severity debug facility local0

Success.

DGS-3000-28SC:admin#
```

90-9 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 - Specify 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-3000-28SC:admin#delete syslog host 4
Command: delete syslog host 4

Success.

DGS-3000-28SC:admin#
```

90-10 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-3000-28SC: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-3000-28SC:admin#
```

90-11 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 - Specify 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 - Specify 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 - Specify 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-3000-28SC:admin#config log_save_timing on_demand
Command: config log_save_timing on_demand

Success.

DGS-3000-28SC:admin#
```

90-12 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-3000-28SC:admin#show log_save_timing
Command: show log_save_timing

Saving Log Method: On_demand

DGS-3000-28SC:admin#
```

90-13 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 {unit <unit_id 1-6} {index <value_list>}

Parameters

unit - (Optional) The attack log messages on the specified unit will be displayed. If unit ID is not specified, then it will be referred to as the master unit. **<unit_id 1-6>** - Enter the unit ID value. This value must be between 1 and 6.
index - (Optional) The list of index numbers of the entries that need to be displayed. For example, show attack_log index 1-5 will display the attack log messages from 1 to 5. **<value_list>** - Enter the index numbers of the entries that needs to be displayed here.
If no parameter is specified, all entries in the attack log will be displayed.

Restrictions

None.

Example

To show dangerous messages on the master:

```
DGS-3000-28SC:admin#show attack_log index 1
Command: show attack_log index 1

Index   Date       Time      Level     Log Text
----- ---------- -------- -------- ------------------------------------------
1      2014-05-17 15:00:14 CRIT(2)   Possible spoofing attack from IP: , MAC:
                                     0A-00-00-5A-00-01, port: 3

DGS-3000-28SC:admin#
```

90-14 clear attack_log

Description

This command is used to clear the attack log.

Format

clear attack_log {[unit <unit_id 1-6> | all]}

Parameters

unit - (Optional) The attack log messages on the specified unit will be cleared. **<unit_id 1-6>** - Enter the unit ID value. This value must be between 1 and 6.
all - (Optional) Specify that all the unit ID's information will be used.
If no parameter is specified, the master unit will be applied.

Restrictions

Only Administrators and Operators can issue this command.

Example

To clear the master's attack log:

```
DGS-3000-28SC:admin# clear attack_log
Command: clear attack_log

Success.

DGS-3000-28SC:admin#
```

90-15 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 - Specify the severity level control for traps.
log - Specify the severity level control for the log.
all - Specify 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-3000-28SC:admin#config system_severity trap warning
Command: config system_severity trap warning

Success.

DGS-3000-28SC:admin#
```

90-16 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-3000-28SC:admin#show system_severity
Command: show system_severity

System Severity Trap : warning(4)
System Severity Log : information(6)

DGS-3000-28SC:admin#
```

Chapter 91 Technical Support Command List

show tech_support
upload tech_support_toTFTP <ipaddr> <path_filename 64>

91-1 show tech_support

Description

This command is used to show technical support information.

Format

show tech_support

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To show technical support information:

```
DGS-3000-28SC:admin# show tech_support
Command: show tech_support

#------------------------------------------------------------------------------
-
#                       DGS-3000-28SC Gigabit Ethernet Switch
#                         Technical Support Information
#
#                            Firmware: Build 5.00.0020
#          Copyright(C) 2014  D-Link Corporation. All rights reserved.
#------------------------------------------------------------------------------


********************   Basic System Information   ********************

[SYS 2014-1-4 20:31:02]

Boot Time           : 4 Jan 2014  20:20:18
RTC Time            : 2014/01/04 20:31:02
Boot PROM Version   : Build 5.00.003
Firmware Version    : Build 5.00.020
Hardware Version    : A1
Serial number       : 123456
MAC Address         : 00-01-02-03-04-00
MAC Address Number  : 65535

********************   System Log   ********************

[SYS_LOG 2014-1-4 20:31:02]

Index Date       Time     Level   Log Text
----- ---------- -------- ------- --------------------------------------------
3     2014-01-04 20:30:51 INFO(6) Successful login through Console (Username:
An
                                  onymous)
2     2014-01-04 20:20:49 CRIT(2) System started up
1      2014-01-04 20:20:49 CRIT(2) System cold start

********************   Running Configuration   ********************

[DUAL_CONFIG 2014-1-4 20:31:02]

#------------------------------------------------------------------------------
#                    DGS-3000-28SC Gigabit Ethernet Switch
#                                 Configuration
#
#                            Firmware: Build 5.00.020
#           Copyright(C) 2014 D-Link Corporation. All rights reserved.
#------------------------------------------------------------------------------
DGS-3000-28SC:admin:

# STACK
```

```
config stacking force_master_role state disable

# DEVICE

config temperature threshold high 79
config temperature threshold low 11
config temperature trap state enable
config temperature log state enable
config fan trap state enable
config power trap state enable

# BASIC

# ACCOUNT LIST
# ACCOUNT END
# PASSWORD ENCRYPTION
disable password encryption
config serial_port auto_logout 10_minutes
enable web 80
enable clipaging
config terminal width 80
disable command logging
enable password_recovery
config configuration trap save disable
config configuration trap upload disable
config configuration trap download disable

# DEBUG

debug config state enable
debug config error_reboot enable

# GM

disable sim
config sim candidate
config sim dp_interval 30
config sim hold_time 100
......
#------------------------------------------------------------------
#             End of configuration file for DGS-3000-28SC
#------------------------------------------------------------------
********************   Layer One Information   ********************

[PORT 2009-9-8 09:18:22]


Logical port = 1

 MAC Base information : dev_num = 0, phy port = 8, medium = fiber
 ====================================
State                    :Enable
```

```
Speed                   :1000
Auto negotiation        :Enable
Duplex                  :FULL Duplex
Mdix                    :cross
Flow control            :Disable
 ====================================
 Dump normal register vale:
 register : 0x0 --->value : 0x1840
 register : 0x1 --->value : 0x79c9
 register : 0x2 --->value : 0x600d
 register : 0x3 --->value : 0x8453
 register : 0x4 --->value : 0xa1
 register : 0x5 --->value : 0x0
 register : 0x6 --->value : 0x64
 register : 0x7 --->value : 0x2001
......
[MIRROR 2009-9-8 09:18:22]


 ****************** Mirror ******************
Mirror SW table:
       State: Disable


********************   Layer Two Information   ********************

[VLAN 2014-1-4 20:31:24]

[MSTP 2014-1-4 20:31:24]

 Instance Type          : CIST
 Instance Status        : Disabled
 Instance Priority      : 32768(Bridge Priority : 32768, SYS ID Ext : 0 )


 Port Index     : 1      , Hello Time: 2 /2 , Port STP : Enabled  ,
 External PathCost : Auto/200000   , Edge Port : False/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   Disabled    Disabled
......

********************   Layer Three Information   ********************

[IP_INTERFACE 2014-1-4 20:31:39]

IP Interface               : System
VLAN Name                  : default
Interface Admin state      : Enabled
Link Status                : LinkDown
```

```
IPv4 Address                : 10.90.90.90/8 (Manual)  Primary
Proxy ARP                   : Disabled   (Local : Disabled)
IP MTU                      : 1500

 Total Entries   : 1
[ARP 2014-1-4 20:31:39]


 ARP Aging Time : 20

Interface      IP Address       MAC Address        Type    Box  Port
-------------  ---------------  -----------------  ---------------

Total Entries: 0

********************   Application   ********************


********************   OS Status   ********************

[OS 2014-1-4 20:31:52]
TID      TaskName    StkBott    StkPt   StkKb  CpuTic    Pri  Status
01F09DE4 HISR0      04367CA0 04367C10   1/  4       0   0/  0 Pend
01F0A0A0 HISR1      04368F80 04368EF0   1/  4     165   1/  1 Pend
......

********************   Management   ********************

[SNMP 2014-1-4 20:31:57]

SNMP : Enabled
---------------------------------------
SNMP Engine ID : 800000ab03000102030400
SNMP Engine Boots : 2
SNMP Engine Time : 0 day 00:11:07
......

******************** Reboot Schedule ********************

 Reboot Schedule Settings
 ---------------------------
 No reboot schedule.

[LBD 2014-1-4 20:32:00]

 LBD is disable
[TRAFFIC_SEG 2014-1-4 20:32:00]


#------------------------------------------------------------------
#        End of Technical Support Information for <DGS-3000-28SC>
#------------------------------------------------------------------
```

```
DGS-3000-28SC:admin
```

91-2 upload tech_support_toTFTP

Description

This command is used to upload the technical support information of the switch to TFTP server.

Format

upload tech_support_toTFTP <ipaddr> <path_filename 64>

Parameters

<ipaddr> - Enter the IP address of the tech support TFTP server.
<path_filename 64> - Enter the path filename of the TFTP server.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

Telnet to a Switch by specifying the IP address:

```
DGS-3000-28SC:admin#upload tech_support_toTFTP 10.90.90.90 c:/support
Command: upload tech_support_toTFTP

Connecting to server……
TFTP Establish session success

Success

DGS-3000-28SC:admin
```

Chapter 92 Telnet Client Command List

telnet [<ipaddr> | <domain_name 255> | <ipv6addr>] {tcp_port <value 1-65535>}
show telnet source_ipif
config telnet source_ipif [<ipif_name 12> {<ipaddr> | <ipv6addr>} | none]

92-1 telnet

Description

This command is used to start the Telnet client to connect to the specific Telnet server. The parameters specified by the command will only be used for the establishment of this specific session. They will not affect the establishment of other sessions.

Format

telnet [<ipaddr> | <domain_name 255> | <ipv6addr>] {tcp_port <value 1-65535>}

Parameters

<ipaddr> - Enter the IP address of the Telnet server.
<domain_name 255> - Enter the domain name of the Telnet server.
<ipv6addr> - Enter the IPv6 address of the Telnet server.
tcp_port - (Optional) Specify 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-3000-28SC:admin#telnet 10.90.90.90
Command: telnet 10.90.90.90



                    DGS-3000-28SC Gigabit Ethernet Switch
                            Command Line Interface

                           Firmware: Build 5.00.020
          Copyright(C) 2014 D-Link Corporation. All rights reserved.

UserName:
```

92-2 show telnet source_ipif

Description

This command is used to show the source IP address for telnet.

Format

show telnet source_ipif

Parameters

None.

Restrictions

None.

Example

To display the source telnet IP address:

```
DGS-3000-28SC:admin# show telnet source_ipif
Command: show telnet source_ipif

Telnet Source IP Interface Configuration:

IP Interface             : System
IPv4 Address             : 10.90.90.90
IPv6 Address             : None

DGS-3000-28SC:admin
```

92-3 config telnet source_ipif

Description

This command is used to set the source ip address for telnet.

Format

config telnet source_ipif [<ipif_name 12> {<ipaddr> | <ipv6addr>} | none]

Parameters

<ipif_name 12> - Specify the IP interface name which will be used as the source for the telnet server.
<ipaddr> - (Optional) Specify the IPv4 address on the source IP interface used as the source address.
<ipv6addr> - (Optional) Specify the IPv6 address on the source IP interface used as the source address.
none - Remove the specified source address.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To Telnet to a host by specifying the domain name and the server port:

```
DGS-3000-28SC:admin# telnet ctrl.iplanet.org tcp_port 2323
Command: telnet ctrl.iplanet.org tcp_port 2323


Login:

UserName:
```

To Telnet to a Switch by specifying the IPv6 address 3000::12:1:

```
DGS-3000-28SC:admin# telnet ctrl.iplanet.org tcp_port 2323
Command: telnet ctrl.iplanet.org tcp_port 2323


Login:

UserName:
```

Chapter 93 TFTP Client Command List

download [firmware_fromTFTP [<ipaddr> | <ipv6addr> | <domain_name 255>] src_file <path_filename 64> {[unit<unit_id> | all]} {dest_file <pathname>} {boot_up} | cfg_fromTFTP [<ipaddr> | <ipv6addr> | <domain_name 255>] src_file <path_filename 64> {[unit <unit_id> | all]} {[increment | dest_file <pathname>]}]
upload [cfg_toTFTP [<ipaddr> | <ipv6addr> | <domain_name 255>] dest_file <path_filename 64> {unit <unit_id>} {src_file <pathname>} {[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> {unit <unit_id>} | firmware_toTFTP [<ipaddr> | <ipv6addr> | <domain_name 255>] dest_file <path_filename 64> {unit <unit_id>} {src_file <pathname>}]
show tftp source_ipif
config tftp source_ipif [<ipif_name12> {<ipaddr> | <ipv6addr>} | none]

93-1 download

Description

This command is used to download a new firmware or a switch configuration file.

Format

download [firmware_fromTFTP [<ipaddr> | <ipv6addr> | <domain_name 255>] src_file <path_filename 64> {[unit<unit_id> | all]} {dest_file <pathname>} {boot_up} | cfg_fromTFTP [<ipaddr> | <ipv6addr> | <domain_name 255>] src_file <path_filename 64> {[unit <unit_id> | all]} {[increment | dest_file <pathname>]}]

Parameters

firmware_fromTFTP - Download and install new firmware on the switch from a TFTP server.
- **<ipaddr>** - Enter the IP address of the TFTP server.
- **<ipv6addr>** - Enter the IPv6 address of the TFTP server.
- **<domain_name 255>** - Enter the domain name of the TFTP server. This name can be up to 255 characters long.
- **src_file** - Specify the path name and file name of the TFTP server. It can be a relative path name or an absolute path name. If path name is not specified, it refers to the TFTP server path. The maximum length is 64 characters.
  - **<path_filename 64>** - Enter the path name and file name of the TFTP server. It can be a relative path name or an absolute path name. If path name is not specified, it refers to the TFTP server path. The maximum length is 64 characters.
- **unit** - (Optional) Specify the unit for the TFTP server.
  - **<unit_id>** - Enter the unit ID for the TFTP server.
- **all** - (Optional) Specify all the unit ID's.
- **dest_file** - (Optional) Specify an absolute path name on the device file system. If path name is not specified, it overwrites the boot-up image on the Switch.
  - **<pathname>** - Enter an absolute path name on the device file system.
- **boot_up** - (Optional) Specify as boot-up file.

cfg_fromTFTP - Download and install new configuration file on the switch from a TFTP server.
- **<ipaddr>** - Enter the IP address of the TFTP server.
- **<ipv6addr>** - Enter the IPv6 address of the TFTP server.

<domain_name 255> - Enter the domain name of the TFTP server. This name can be up to 255 characters long.
src_file - Specify the path name and file name of the FTP server. It can be a relative path name or an absolute path name. If path name is not specified, it refers to the TFTP server path. The maximum length is 64 characters.
<path_filename> - Enter the path name and file name of the FTP server. It can be a relative path name or an absolute path name. If path name is not specified, it refers to the TFTP server path. The maximum length is 64 characters.
unit - (Optional) Specify the file unit.
<unit_id> - Enter the unit ID here.
all - (Optional) Specify all the unit ID's.
incremental - (Optional) Specify the incremental unit ID's.
dest_file - (Optional) Specify an absolute path name on the device. If path name is not specified, it refers to the boot-up configuration file.
<pathname> - Enter an absolute path name on the device.

Restrictions

Only Administrator-level users can issue this command.

Example

To download runtime firmware from a TFTP server:

```
DGS-3000-28SC:admin#download firmware_fromTFTP 10.0.0.66 src_file runtime.had
dest_file runtime.had
Command: download firmware_fromTFTP 10.0.0.66 src_file runtime.had dest_file
runtime.had

 Connecting to server.................. Done.
 Download firmware..................... Done.  Do not power off!
 Please wait, programming flash......... Done.


DGS-3000-28SC:admin#
```

93-2 upload

Description

This command is used to upload the firmware, configuration file, system log, or attack log to the TFTP server.

Format

upload [cfg_toTFTP [<ipaddr> | <ipv6addr> | <domain_name 255>] dest_file <path_filename 64> {unit <unit_id>} {src_file <pathname>} {[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> {unit <unit_id>} | firmware_toTFTP [<ipaddr> | <ipv6addr> | <domain_name 255>] dest_file <path_filename 64> {unit <unit_id>} {src_file <pathname>}]

Parameters

cfg_toTFTP - Used to upload a configuration file from the Switch to the TFTP server.
- **<ipaddr>** - Enter the IP address of the TFTP server.
- **<ipv6addr>** - Enter the IPv6 address of the TFTP server.
- **<domain_name 255>** - Enter the domain name of the TFTP server here. This name can be up to 255 characters long.
- **dest_file** - Specify the path name on the TFTP server.
  - **<path_filename 64>** - Enter the location of the Switch configuration file on the TFTP server. This file will be replaced by the uploaded file from the Switch. The maximum length is 64 characters.
    - **unit** - (Optional) Specify the unit for the TFTP server.
      - **<unit_id>** - Enter the unit ID for the TFTP server.
- **src_file** - (Optional) Specify the source file's path name on the Switch file system. If the path name is not specified, it refers to the boot-up configuration file.
  - **<path_filename 64>** - Enter the location of the Switch configuration file on device. The maximum length is 64 characters.
- **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>** - Enter a filter string enclosed by the quotation mark symbol. Thus, the filter string itself cannot contain the quotation mark character. The filter string is case sensitive.
    - **<filter_string 80>** - (Optional) Enter a filter string enclosed by the quotation mark symbol.
      - **<filter_string 80>** - (Optional) Enter a filter string enclosed by the quotation mark symbol.
  - **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>** - Enter a filter string enclosed by the quotation mark symbol. Thus, the filter string itself cannot contain the quotation mark character. The filter string is case sensitive.
      - **<filter_string 80>** - (Optional) Enter a filter string enclosed by the quotation mark symbol.
        - **<filter_string 80>** - (Optional) Enter a filter string enclosed by the quotation mark symbol.

log_toTFTP - Used to upload the log file from the Switch to the TFTP server.
- **<ipaddr>** - Enter the IP address of the TFTP server.
- **<ipv6addr>** - Enter the IPv6 address of the TFTP server.
- **<domain_name 255>** - Enter the domain name of the TFTP server here. This name can be up to 255 characters long.
- **dest_file** - Specify the path name to the TFTP server.
  - **<path_filename 64>** - Enter the path name to the TFTP server.

attack_log_toFTP - Used to upload the attack log from the Switch to the TFTP server.
- **<ipaddr>** - Enter the IP address of the TFTP server.
- **<ipv6addr>** - Enter the IPv6 address of the TFTP server.
- **<domain_name 255>** - Enter the domain name of the TFTP server here. This name can be up to 255 characters long.
- **dest_file** – (Optional) Specify the path name on the TFTP server.
  - **<path_filename 64>** - Enter the location of the Switch configuration file on the TFTP server. This file will be replaced by the uploaded file from the Switch. The maximum length is 64 characters.
    - **unit** - (Optional) Specify the unit for the TFTP server.
      - **<unit_id>** - Enter the unit ID for the TFTP server.

firmware_toTFTP - Used to upload firmware from the Switch to the TFTP server.
- **<ipaddr>** - Enter the IP address of the TFTP server.
- **<ipv6addr>** - Enter the IPv6 address of the TFTP server.

<domain_name 255> - Enter the domain name of the TFTP server here. This name can be up to 255 characters long.
dest_file - Specify the path name to the TFTP server.
<path_filename 64> - Enter the path name to the TFTP server.
unit - (Optional) Specify the unit for the TFTP server.
<unit_id> - Enter the unit ID for the TFTP server.
src_file - (Optional) Specify the source file's path name on the Switch file system. If the path name is not specified, it refers to the boot-up image.
<pathname> - Enter the source file's path name on the Switch file system. If the path name is not specified, it refers to the boot-up image.

Restrictions

Only Administrators and Operators can issue this command.

Example

To upload firmware from a file system device to a TFTP server:

```
DGS-3000-28SC: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-3000-28SC:admin#
```

To display a scenario where the uploading of the firmware to the TFTP server failed, because of an incorrect or missing filename from the source. This error can also be found if the directory, on the source, does not exit.

```
DGS-3000-28SC:admin#upload firmware_toTFTP 10.90.90.10 dest_file
D:/firmware.had src_file firmware.had
Command: upload firmware_toTFTP 10.90.90.10 dest_file D:/firmware.had src_file
firmware.had

 No such file or directory.

Fail!

DGS-3000-28SC:admin#
```

To upload configuration from TFTP:

```
DGS-3000-28SC: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-3000-28SC:admin#
```

To display a scenario where the uploading of the config file to the TFTP server failed, because of an incorrect or missing filename from the source. This error can also be found if the directory, on the source, does not exit.

```
DGS-3000-28SC: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-3000-28SC:admin#
```

To upload the attack log from the Switch to the TFTP server:

```
DGS-3000-28SC: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-3000-28SC:admin#
```

93-3 show tftp source_ipif

Description

This command is used to display the TFTP Client source IP address.

Format

show tftp source_ipif

Parameters

None.

Restrictions

None.

Example

To display the TFTP client's source IP address:

```
DGS-3000-28SC:admin# show tftp source_ipif
Command: show tftp source_ipif

Tftp Source IP Interface Configuration:

IP Interface : System
IPv4 Address : 10.90.90.90
IPv6 Address : None

DGS-3000-28SC:admin#
```

93-4 config tftp source_ipif

Description

This command is used to select an address of an interface as the source address for TFTP client.

Format

config tftp source_ipif [<ipif_name12> {<ipaddr> | <ipv6addr>} | none]

Parameters

<ipif_name12> - Enter the IP interface name which will be used as the source for the TFTP. **<ipaddr>** - (Optional) Enter the IPv4 address on the source IP interface used as the source address. **<ipv6addr>** - (Optional) Enter the IPv6 address on the source IP interface used as the source address.
none - Specify to remove the specified source address.

Restrictions

Only Administrators, Operators, and Power Users can issue this command.

Example

To configure the IP 10.90.90.90 on the System interface as the source address:

```
DGS-3000-28SC:admin# config tftp source_ipif System 10.90.90.90
Command: config tftp source_ipif System 10.90.90.90

Success.

DGS-3000-28SC:admin#
```

Chapter 94 Time Range Command List

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

94-1 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

<range_name 32> - Enter the time range name used here. This name can be up to 32 characters long.
hours - Specify the time of a day. **start_time** - Specify the starting time of a day. **<time hh:mm:ss>** - Enter the starting time here. (24-hr time). For example, 19:00:00 means 7PM. The time specified in the start_time parameter must be smaller than the time specified in the end_time parameter. **end_time** - Specify the ending time of a day. (24-hr time) **<time hh:mm:ss>** - Enter the ending time here. (24-hr time). For example, 19:00:00 means 7PM. The time specified in the start_time parameter must be smaller than the time specified in the end_time parameter. **weekdays** - Specify the list of days contained in the time range. Use a dash to define a period of days. Use a comma to separate specific days. **<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 - Specify to delete 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 and then delete it:

```
DGS-3000-28SC: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-3000-28SC:admin#config time_range 1 delete
Command: config time_range 1 delete

Success.

DGS-3000-28SC:admin#
```

94-2 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-3000-28SC: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-3000-28SC:admin#
```

Chapter 95 Time and SNTP Command List

config sntp {primary <ipaddr> | secondary <ipaddr> | poll-interval <int 30-99999>}(1)
config sntp ipv6server {primary <ipv6addr> | secondary <ipv6addr> }(1)
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_daysun-sat> | s_mth <start_mth 1-12> | s_time <start_timehh:mm> | e_week <end_week 1-4,last> | e_day <end_daysun-sat> | e_mth <end_mth 1-12> | e_time <end_timehh:mm> | offset [30 | 60 | 90 | 120]} | annual {s_date <start_date 1-31> | s_mth <start_mth 1-12> | s_time <start_timehh:mm> | e_date <end_date 1-31> | e_mth <end_mth 1-12> | e_time <end_timehh:mm> | offset [30 | 60 | 90 | 120]}]
show time

95-1 config sntp

Description

This command is used to change SNTP configurations.

Format

configure sntp {primary <ipaddr> | secondary <ipaddr> | poll-interval <int 30-99999>}(1)

Parameters

primary - SNTP primary server IP address. **<ipaddr>** - Enter the IP address used for this configuration here.
secondary - SNTP secondary server IP address. **<ipaddr>** - Enter the IP address used for this configuration here.
poll-interval - Specify 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-3000-28SC: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-3000-28SC:admin#
```

95-2 config sntp ipv6server

Description

This command is used to configure the SNTP IPv6 server information.

Format

config sntp ipv6server {primary <ipv6addr> | secondary <ipv6addr> }(1)

Parameters

primary - SNTP primary IPv6 server address. **<ipv6addr>** - Enter the IPv6 address of the Primary SNTP IPv6 server.
secondary - SNTP secondary IPv6 server address. **<ipv6addr>** - Enter the IPv6 address of the Secondary SNTP IPv6 server.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure SNTP (primary IPv6 server: 1000::1, secondary IPv6 server: 1000::2):

```
DGS-3000-28SC:admin#config sntp ipv6server primary 1000::1 secondary 1000::2
Command: config sntp ipv6server primary 1000::1 secondary 1000::2

Success.

DGS-3000-28SC:admin#
```

95-3 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-3000-28SC:admin#show sntp
Command: show sntp

Current Time Source   : System Clock
SNTP Status           : Disabled
IPv4 Primary SNTP Server  : 10.1.1.1
IPv4 Secondary SNTP Server: 10.1.1.2
IPv6 Primary SNTP Server  : ::
IPv6 Secondary SNTP Server: ::
SNTP Poll Interval        : 30 sec

DGS-3000-28SC:admin#
```

95-4 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-3000-28SC:admin#enable sntp
Command: enable sntp

Success.

DGS-3000-28SC:admin#
```

95-5 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-3000-28SC:admin#disable sntp
Command: disable sntp

Success.

DGS-3000-28SC:admin#
```

95-6 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> - Enter the system clock date. An example would look like this: '30jun2010'.
<time hh:mm:ss> - Enter 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-3000-28SC:admin#config time 30jun2014 16:30:30
Command: config time 30jun2014 16:30:30

Success.

DGS-3000-28SC:admin#
```

95-7 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) Specify the operator of time zone. **[+ | -]** - Specify that time should be added or subtracted to or from the GMT.
hour - (Optional) Specify 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) Specify 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-3000-28SC:admin#config time_zone operator + hour 2 min 30
Command: config time_zone operator + hour 2 min 30

Success.

DGS-3000-28SC:admin#
```

95-8 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_daysun-sat> | s_mth <start_mth 1-12> | s_time <start_timehh:mm> | e_week <end_week 1-4,last> | e_day <end_daysun-sat> | e_mth <end_mth 1-12> | e_time <end_timehh:mm> | offset [30 | 60 | 90 | 120]} | annual {s_date <start_date 1-31> | s_mth <start_mth 1-12> | s_time <start_timehh:mm> | e_date <end_date 1-31> | e_mth <end_mth 1-12> | e_time <end_timehh:mm> | offset [30 | 60 | 90 | 120]}]

Parameters

disable - Specify to disable the Daylight Saving Time of the Switch.

repeating - Sets the Daylight Saving Time to repeating mode.
- **s_week** - (Optional) Specify 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) Specify the start day number of Daylight Saving Time.
  - **<start_day 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) Specify 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) Specify 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) Specify 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) Specify the end day number of Daylight Saving Time.
  - **<end_day 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) Specify 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) Specify 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** - Specify that the offset range will 30 minutes.
  - **60** - Specify that the offset range will 60 minutes.
  - **90** - Specify that the offset range will 90 minutes.
  - **120** - Specify that the offset range will 120 minutes.

annual - Set the Daylight Saving Time to annual mode.
- **s_date** - (Optional) Specify 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 an 31.
- **s_mth** - (Optional) Specify 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) Specify 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) Specify 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 an 31.
e_mth - (Optional) Specify 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) Specify 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 - Specify that the offset range will 30 minutes.
60 - Specify that the offset range will 60 minutes.
90 - Specify that the offset range will 90 minutes.
120 - Specify that the offset range will 120 minutes.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure time:

```
DGS-3000-28SC:admin#config dst repeating s_week 2 s_day tue s_mth 4 s_time
15:00 e_week2 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-3000-28SC:admin#
```

95-9 show time

Description

This command is used to display time states.

Format

show time

Parameters

None.

Restrictions

None.

Example

To show time:

```
DGS-3000-28SC:admin#show time
Command: show time

     Current Time Source  : System Clock
     Boot Time    : 9 May 2014  06:20:55
     Current Time : 9 May 2014  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-3000-28SC:admin#
```

Chapter 96 Trace Route Command List

traceroute [<ipaddr> | <domain_name 255>] {ttl <value 1-60> | port <value 30000-64900> | timeout <sec 1-65535> | probe <value 1-9>} | frequency <sec 0-86400>}
traceroute6 [<ipv6addr> | <domain_name 255>] {ttl <value 1-60> | port <value 30000-64900> | timeout <sec 1-65535> | probe <value 1-9> | frequency <sec 0-86400>}

96-1 traceroute

Description

This command is used to trace the routed path between the Switch and a destination end station.

Format

traceroute [<ipaddr> | <domain_name 255>] {ttl <value 1-60> | port <value 30000-64900> | timeout <sec 1-65535> | probe <value 1-9>} | frequency <sec 0-86400>}

Parameters

<ipaddr> - Enter 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 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) Specify 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.
frequency - (Optional) Specify the frequency used. **<sec 0-86400>** - Enter the frequency value here. This value must be between 0 and 86400 seconds.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To trace the routed path between the Switch and 10.48.74.121:

```
DGS-3000-28SC: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-3000-28SC:admin#
```

96-2 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> | frequency <sec 0-86400>}

Parameters

<ipv6addr> - Enter the IPv6 address of the destination end station.
<domain_name 255> - Enter the domain name of the destination end station.
ttl - (Optional) 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) Specify 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.
frequency - (Optional) Specify the frequency used. **<sec 0-86400>** - Enter the frequency value here. This value must be between 0 and 86400 seconds.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To trace the IPv6 routed path between the Switch and 3000::1:

```
DGS-3000-28SC: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-3000-28SC:admin#
```

To trace the IPv6 routed path between the Switch and 1210:100::11 with port 40000:

```
DGS-3000-28SC: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-3000-28SC:admin#
```

Chapter 97 Traffic Control Command List

config traffic control [<portlist> | all] {broadcast [enable | disable] | multicast [enable | disable] | unicast [enable | disable] | action [drop | shutdown] | [threshold <value 0-1488100> | {broadcast_threshold <value 0-1488100> | multicast_threshold <value 0-1488100> | unicast_threshold <value 0-1488100>}(1)] | countdown [<min0> | <min 3-30> | disable] | time_interval <sec 5-600>}(1)
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>]

97-1 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 0-1488100> | {broadcast_threshold <value 0-1488100> | multicast_threshold <value 0-1488100> | unicast_threshold <value 0-1488100>}(1)] | countdown [<min 0> | <min 3-30> | disable] | time_interval <sec 5-600>}(1)

Parameters

<portlist> - Enter a range of ports to be configured.
all - Specify that all the ports will be used for this configuration.
broadcast - Specify to enable or disable broadcast storm control. **enable** - Specify that broadcast storm control will be enabled. **disable** - Specify that broadcast storm control will be disabled.
multicast - Specify to enable or disable multicast storm control. **enable** - Specify that multicast storm control will be enabled. **disable** - Specify that multicast storm control will be disabled.
unicast - Specify to enable or disable unknown packet storm control. (Supported for drop mode only) **enable** - Specify that unicast storm control will be enabled. **disable** - Specify that unicast storm control will be disabled.
action - 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** - Specify that the action applied will be drop mode. **shutdown** - Specify that the action applied will be shutdown mode.
threshold - 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 0-148100>** - Enter the upper threshold value here. This value must be between 0 and 148100.
broadcast_threshold - The broadcast threshold, at which point the specified storm control is triggered. The <value> is the number of broadcast 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. **<value0-1488100>** - Enter the upper threshold value here. This value must be between 0 and 148100.
multicast_threshold - The multicast threshold, at which point the specified storm control is triggered. The <value> is the number of multicast packets per second received by the Switch that will trigger the storm traffic control measure. The threshold is expressed as PPS (packets per second) and must be an unsigned integer. **<value0-1488100>** - Enter the upper threshold value here. This value must be between 0 and 148100.
unicast_threshold – The unicast threshold, at which point the specified storm control is triggered. The <value> is the number of 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. **<value0-1488100>** - Enter the upper threshold value here. This value must be between 0 and 148100.
countdown - Timer for shutdown mode. If a port enters the shutdown Rx state and this timer runs out, port will be shutdown forever. The parameter is not applicable if “drop” (mode) is specified for the “action” parameter. **<min 0>** - Enter 0 to disable 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** – Specify that the countdown timer will be disabled.
time_interval - 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-3000-28SC: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-3000-28SC:admin#
```

97-2 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-3000-28SC:admin#config traffic trap both
Command: config traffic trap both

Success.

DGS-3000-28SC:admin#
```

97-3 show traffic control

Description

This command is used to display the current traffic control settings.

Format

show traffic control {<portlist>}

Parameters

<portlist> - (Optional) Enter 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-3000-28SC:admin#show traffic control  1-10
Command: show traffic control 1-10


Traffic Control Trap             : [None]
Traffic Control Log              : Enabled
Traffic Control Auto Recover Time: 0 Minutes

Port  Broadcast/ Multicast/ Unicast/  Action   Count    Time      Shutdown
      Threshold  Threshold  Threshold          down     Interval  Forever
----  ---------  ---------  --------- -------- -------- --------- --------
1     Disabled   Disabled   Disabled  drop     0        5
      131072     131072     131072
2     Disabled   Disabled   Disabled  drop     0        5
      131072     131072     131072
3     Disabled   Disabled   Disabled  drop     0        5
      131072     131072     131072
4     Disabled   Disabled   Disabled  drop     0        5
      131072     131072     131072
5     Disabled   Disabled   Disabled  drop     0        5
      131072     131072     131072
6     Disabled   Disabled   Disabled  drop     0        5
      131072     131072     131072
7     Disabled   Disabled   Disabled  drop     0        5
      131072     131072     131072
8     Disabled   Disabled   Disabled  drop     0        5
      131072     131072     131072
9     Disabled   Disabled   Disabled  drop     0        5
      131072     131072     131072
10    Disabled   Disabled   Disabled  drop     0        5
      131072     131072     131072

DGS-3000-28SC:admin#
```

97-4 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-3000-28SC:admin#config traffic control log state enable
Command: config traffic control log state enable

Success.

DGS-3000-28SC:admin#
```

97-5 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> - Enter 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-3000-28SC:admin#config traffic control auto_recover_time 5
Command: config traffic control auto_recover_time 5

Success.

DGS-3000-28SC:admin#
```

Chapter 98 Traffic Segmentation Command List

config traffic_segmentation [<portlist> | all] forward_list [null | all | <portlist>]
show traffic_segmentation {<portlist>}

98-1 config traffic_segmentation

Description

This command is used to configure the traffic segmentation.

Format

config traffic_segmentation [<portlist> | all] forward_list [null | all | <portlist>]

Parameters

<portlist> - Enter a range of ports to be configured.
all - Specify that all the ports will be used for this configuration.
forward_list - Specify a range of port forwarding domain. **null** - Specify a range of port forwarding domain is null. **all** - Specify all ports to be configured. **<portlist>** - Enter a range of ports to be configured.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure traffic segmentation:

```
DGS-3000-28SC:admin#config traffic_segmentation 1-10 forward_list 11-15
Command: config traffic_segmentation 1-10 forward_list 11-15

Success.

DGS-3000-28SC:admin#
```

98-2 show traffic_segmentation

Description

This command is used to display current traffic segmentation table.

Format

show traffic_segmentation {<portlist>}

Parameters

<portlist> - (Optional) Enter a range of ports to be displayed.
If no parameter is specified, the system will display all current traffic segmentation tables.

Restrictions

None.

Example

To display traffic segmentation table:

```
DGS-3000-28SC:admin#show traffic_segmentation 1-10
Command: show traffic_segmentation 1-10

Traffic Segmentation Table

Port  Forward Portlist
----  ------------------------------------------------------------------------
1      11-15
2      11-15
3      11-15
4      11-15
5      11-15
6      11-15
7      11-15
8      11-15
9      11-15
10     11-15


DGS-3000-28SC:admin#
```

Chapter 99 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

99-1 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> - Enter the trusted host IP address.
<ipv6addr> - Enter the trusted host IPv6 address.
network - The network address of the trusted network. The network address takes the form of: xxx.xxx.xxx.xxx/y. Where “x” represents an IP number. **<network_address>** - Enter the network address used here.
ipv6_prefix - Specify that IPv6 prefix here. **<ipv6networkaddr>** - Enter the IPv6 network address here.
snmp - (Optional) Specify trusted host for SNMP.
telnet - (Optional) Specify trusted host for TELENT.
ssh - (Optional) Specify trusted host for SSH.
http - (Optional) Specify trusted host for HTTP.
https - (Optional) Specify trusted host for HTTPs.
ping - (Optional) Specify trusted host for PING.

Restrictions

Only Administrators and Operators can issue this command.

Example

To create the trusted host:

```
DGS-3000-28SC:admin#create trusted_host 10.48.74.121
Command: create trusted_host 10.48.74.121

Success.

DGS-3000-28SC:admin#
```

99-2 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-3000-28SC:admin#delete trusted_host ipaddr 10.48.74.121
Command: delete trusted_host ipaddr 10.48.74.121

Success.

DGS-3000-28SC:admin#
```

99-3 config trusted_host

Description

This command is used to configure the access interfaces for the trusted host.

Format

config trusted_host [<ipaddr> | <ipv6addr> | network <network_address> | ipv6_prefix <ipv6networkaddr>] [add | delete] {snmp | telnet | ssh | http | https | ping | all}

Parameters

<ipaddr> - Enter the trusted host IP address.
<ipv6addr> - Enter the trusted host IPv6 address.
network - The network address of the trusted network. The network address takes the form of: xxx.xxx.xxx.xxx/y where “x” represents an IP number. **<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 - Specify to add interfaces for that trusted host.
delete - Specify to delete interfaces for that trusted host.
snmp - (Optional) Specify trusted host for SNMP.
telnet - (Optional) Specify trusted host for TELENT.
ssh - (Optional) Specify trusted host for SSH.
http - (Optional) Specify trusted host for HTTP.
https - (Optional) Specify trusted host for HTTPs.
ping - (Optional) Specify trusted host for PING.
all - (Optional) Specify trusted host for all applications.

Restrictions

Only Administrators and Operators can issue this command.

Example

To configure the trusted host:

```
DGS-3000-28SC:admin#config trusted_host 10.48.74.121 add ssh telnet
Command: config trusted_host 10.48.74.121 add ssh telnet

Success.

DGS-3000-28SC:admin#
```

99-4 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-3000-28SC: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-3000-28SC:admin#
```

Chapter 100 User Account Command List

create account [admin | operator | power_user | user] <username 15> {encrypt [plain_text | sha_1] <password>}
config account <username 15> {encrypt [plain_text | sha_1] <password>}
show account
delete account <username 15>
enable password encryption
disable password encryption

100-1 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 - Specify the name of the admin account.
operator - Specify the name for a operator user account.
power_user - Specify the name for a Power-user account.
user - Specify the name of the user account.
<username 15> - Enter the username used here. This name can be up to 15 characters long.
encrypt - (Optional) Specify the encryption applied to the account. **plain_text** - Specify the password in plain text form. **sha_1** - Specify the password in the SHA-1 encrypted form. **<password>** - The password for the user account. The length for of password in plain-text form and in encrypted form are different. For the plain-text form, passwords must have a minimum of 0 character and can have a maximum of 15 characters. For the encrypted form password, the length is fixed to 35 bytes long. The password is case-sensitive.

Restrictions

Only Administrators can issue this command.

Example

To create the admin-level user “dlink”:

```
DGS-3000-28SC: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-3000-28SC:admin#
```

To create the user-level user “Remote-Manager”:

```
DGS-3000-28SC: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-3000-28SC:admin#
```

100-2 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 15> {encrypt [plain_text | sha_1] <password>}

Parameters

<username 15> - Enter the user name of the account that has been defined.
encrypt - (Optional) Specify that the password will be encrypted. **plain_text** - Specify the password in plain text form. **sha_1** - Specify the password in the SHA-1 enacrpted 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-3000-28SC: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-3000-28SC:admin#
```

To configure the user password of “administrator” account:

```
DGS-3000-28SC:admin#config account administrator encrypt sha_1
*@&cRDtpNCeBiq15KOQsKVyrA0sAiCIZQwq
Command: config account administrator encrypt sha_1
*@&cRDtpNCeBiq15KOQsKVyrA0sAiCIZQwq

Success.

DGS-3000-28SC:admin#
```

100-3 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-3000-28SC:admin#show account
Command: show account

 Current Accounts:
 Username              Access Level
 ---------------       ------------
 admin                 Admin
 oper                  Operator
 power                 Power_user
 user                  User

 Total Entries : 4

DGS-3000-28SC:admin#
```

100-4 delete account

Description

This command is used to delete an existing account.

Format

delete account <username 15>

Parameters

<username15> - Enter to delete the name of the user.

Restrictions

Only Administrators can issue this command.

Example

To delete the user account “System”:

```
DGS-3000-28SC:admin#delete account System
Command: delete account System

Success.

DGS-3000-28SC:admin#
```

100-5 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-3000-28SC:admin#enable password encryption
Command: enable password encryption

Success.

DGS-3000-28SC:admin#
```

100-6 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 Specify the password in plain text form, the password will be in plan text form. However, if the user Specify 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-3000-28SC:admin#disable password encryption
Command: disable password encryption

Success.

DGS-3000-28SC:admin#
```

Chapter 101 VLAN Counter Command List

create vlan_counter [vlan <vlan_name> | vlanid <vidlist>] {ports [<portlist> | all]} [all_frame | broadcast | multicast | unicast] [packet | byte] {[rx | tx]}
show vlan_counter {[vlan <vlan_name> | vlanid <vidlist>]} {[rx | tx]}
clear vlan_counter statistics [all | [vlan <vlan_name> | vlanid <vidlist>] [all | ports <portlist>]] {[rx | tx]}
show vlan_counter statistics {[vlan <vlan_name> | vlanid <vidlist>] {ports <portlist>}} {[rx | tx]}
delete vlan_counter [all | [vlan <vlan_name> | vlanid <vidlist>] [all | ports <portlist> [all | [all_frame | broadcast | multicast | unicast] [packet | byte]]]] {[rx | tx]}

101-1 create vlan_counter

Description

This command is used to create the control entry for VLAN traffic flow statistics. A control entry can be created to count ingress and/or egress statistics for a specific VLAN or to count statistics for a specific port on a specific VLAN on the ingress pipeline or egress pipeline. The statistics can be counted for different frame types either by byte or by packet. Both ingress and egress statistics are created if the direction is not specified.

Format

create vlan_counter [vlan <vlan_name> | vlanid <vidlist>] {ports [<portlist> | all]} [all_frame | broadcast | multicast | unicast] [packet | byte] {[rx | tx]}

Parameters

vlan - Specify the VLAN name that will be used for this configuration. **<vlan_name>** - Enter the VLAN name that will be used for this configuration.
vlanid - Specify the VLAN ID that will be used for this configuration. **<vidlist>** - Enter the VLAN ID that will be used for this configuration.
ports - (Optional) Specify the list of ports that will be used for this configuration. **<portlist>** - Enter the list of ports that will be used for this configuration. **all** - Specify that all ports will be used for this configuration.
all_frame - Specify that all packets will be counted regardless of the packet type.
broadcast - Specify that only broadcast packets will be counted.
multicast - Specify that only multicast packets will be counted.
unicast - Specify that only unicast packets will be counted.
packet - Specify that the statistics is counted by packets.
byte - Specify that the statistics is counted by bytes.
rx - (Optional) Specify that the statistics is counted for ingress traffic.
tx - (Optional) Specify that the statistics is counted for egress traffic.

Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

Example

To begin counting ingress and egress broadcast traffic for port 3 of VLAN 1 by packets, create a control entry as below:

```
DGS-3000-28SC:admin# create vlan_counter vlanid 1 ports 1:3 broadcast packet
Command: create vlan_counter vlanid 1 ports 1:3 broadcast packet

Success.

DGS-3000-28SC:admin#
```

To begin counting ingress multicast traffic for port 3 of VLAN 2 by packets, create a control entry as below:

```
DGS-3000-28SC:admin#create vlan_counter vlanid 2 ports 1:3 multicast packet rx
Command: create vlan_counter vlanid 2 ports 1:3 multicast packet rx

Success.

DGS-3000-28SC:admin#
```

To begin counting egress unicast traffic for port 5 of VLAN 4 by packets, create a control entry as below:

```
DGS-3000-28SC:admin#create vlan_counter vlanid 4 ports 1:5 unicast packet tx
Command: create vlan_counter vlanid 4 ports 1:5 unicast packet tx

Success.

DGS-3000-28SC:admin#
```

101-2 show vlan_counter

Description

This command is used to display the VLANs traffic flow statistics.

Format

show vlan_counter {[vlan <vlan_name> | vlanid <vidlist>]} {[rx | tx]}

Parameters

vlan - (Optional) Specify the VLAN name that will be used for this display. **<vlan_name>** - Enter the VLAN name that will be used for this display..
vlanid - (Optional) Specify the VLAN ID that will be used for this display. **<vidlist>** - Enter the VLAN ID that will be used for this display.
rx - (Optional) Specify that the control entries for ingress traffic will be displayed.
tx - (Optional) Specify that the control entries for egress traffic will be displayed.

Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

Example

To display the VLAN counter information:

```
DGS-3000-28SC:admin# show vlan_counter
Command: show vlan_counter

VLAN  Frame Type            Ports
----  --------------------  -------------------------------------------------
-
1     RX Broadcast(Packet)  3
2     RX Multicast(Packet)  3
1     TX Broadcast(Packet)  3
4     TX Unicast(Packet)    5

CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

101-3 clear vlan_counter statistics

Description

This command is used to clear statistics gathered by VLAN control entries for VLAN traffic flow statistics.

Format

clear vlan_counter statistics [all | [vlan <vlan_name> | vlanid <vidlist>] [all | ports <portlist>]] {[rx | tx]}

Parameters

all - Specify that all of the statistics will be cleared.
vlan - Specify the VLAN name that will be used for this configuration. **<vlan_name>** - Enter the VLAN name that will be used for this configuration.
vlanid - Specify the VLAN ID that will be used for this configuration. **<vidlist>** - Enter the VLAN ID that will be used for this configuration.
all - Specify that all ports will be used for this configuration.
ports - Specify the list of ports that will be used for this configuration. **<portlist>** - Enter the list of ports that will be used for this configuration.
rx - (Optional) Specify that the statistics for ingress traffic will be cleared.
tx - (Optional) Specify that the statistics for egress traffic will be cleared.

Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

Example

To clear all of the statistics gathered by the control entries:

```
DGS-3000-28SC:admin# clear vlan_counter statistics all
Command: clear vlan_counter statistics all

Success.

DGS-3000-28SC:admin#
```

101-4 show vlan_counter statistics

Description

This command is used to display the VLAN level traffic statistics.

Format

show vlan_counter statistics {[vlan <vlan_name> | vlanid <vidlist>] {ports <portlist>}} {[rx | tx]}

Parameters

vlan - (Optional) Specify the VLAN name that will be used for this display. **<vlan_name>** - Enter the VLAN name that will be used for this display.
vlanid - (Optional) Specify the VLAN ID that will be used for this display. **<vidlist>** - Enter the VLAN ID that will be used for this display
ports - (Optional) Specify the list of ports that will be used for this display. **<portlist>** - Enter the list of ports that will be used for this display.
rx - (Optional) Specify that the statistics for ingress traffic will be cleared.
tx - (Optional) Specify that the statistics for egress traffic will be cleared.

Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

Example

To display the VLAN counter statistics:

```
DGS-3000-28SC:admin# show vlan_counter statistics
Command: show vlan_counter statistics

VLAN  Port  Frame Type            Frames/Bytes            Frames/Bytes Per Sec
----  ----  -------------------  ----------------------  --------------------
-
1     3     RX Broadcast(Packet)  0                       0
2     3     RX Multicast(Packet)  0                       0
1     3     TX Broadcast(Packet)  0                       0
4     5     TX Unicast(Packet)    0                       0

CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

101-5 delete vlan_counter

Description

This command is used to delete the control entry for VLAN traffic flow statistics.

Format

delete vlan_counter [all | [vlan <vlan_name> | vlanid <vidlist>] [all | ports <portlist> [all | [all_frame | broadcast | multicast | unicast] [packet | byte]]]] {[rx | tx]}

Parameters

all - Specify that all control entries will be deleted.
vlan - Specify the VLAN name that will be used for this configuration. **<vlan_name>** - Enter the VLAN name that will be used for this configuration.
vlanid - Specify the VLAN ID that will be used for this configuration. **<vidlist>** - Enter the VLAN ID that will be used for this configuration.
all - Specify that all ports will be used for this configuration.
ports - (Optional) Specify the list of ports that will be used for this configuration. **<portlist>** - Enter the list of ports that will be used for this configuration. **all** - Specify that all frame types to be deleted. **all_frame** - Specify that the frame type of the control entry to be deleted is all. **broadcast** - Specify that the frame type of the control entry to be deleted is broadcast. **multicast** - Specify that the frame type of the control entry to be deleted is multicast. **unicast** - Specify that the frame type of the control entry to be deleted is unicast. **packet** - Specify that the statistic of the control entry to be deleted is based on packets. **byte** - Specify that the statistic of the control entry to be deleted is based on bytes.
rx - (Optional) Specify that the control entries for ingress traffic to be deleted.
tx - (Optional) Specify that the control entries for egress traffic to be deleted.

Restrictions

Only Administrator, Operator and Power-User level users can issue this command.

Example

To delete all of the control entries for both ingress and egress traffic:

```
DGS-3000-28SC:admin#delete vlan_counter all
Command: delete vlan_counter all

Success.

DGS-3000-28SC:admin#
```

Chapter 102 VLAN Trunking Command List

enable vlan_trunk
disable vlan_trunk
config vlan_trunk ports [<portlist> | all] state [enable | disable]
show vlan_trunk

102-1 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-3000-28SC:admin#enable vlan_trunk
Command: enable vlan_trunk

Success.

DGS-3000-28SC:admin#
```

102-2 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-3000-28SC:admin#disable vlan_trunk
Command: disable vlan_trunk

Success.

DGS-3000-28SC:admin#
```

102-3 config vlan_trunk ports

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 configurethe 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 atutomatically 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 by 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 - Specify that all the ports will be used for this configuration.

state - Specify that the port is a VLAN trunk port or not. **enable** - Specify that the port is a VLAN trunk port. **disable** - Specify that the port is not a VLAN trunk port.

Restrictions

Only Administrators can issue this command.

Example

To configure VLAN trunk ports:

```
DGS-3000-28SC:admin#config vlan_trunk ports 1-5 state enable
Command: config vlan_trunk ports 1-5 state enable

Success.

DGS-3000-28SC:admin#
```

Port 6 is LA-1 member port; port 7 is LA-2 master port:

```
DGS-3000-28SC: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-3000-28SC:admin#config vlan_trunk ports 7 state disable
Command: config vlan_trunk ports 7 state disable

Success.

DGS-3000-28SC: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-3000-28SC:admin#
```

Port 6 is LA-1 member port; port 7 is LA-1 master port:

```
DGS-3000-28SC:admin#config vlan_trunk ports 6-7 state enable
Command: config vlan_trunk ports 6-7 state enable

Success.

DGS-3000-28SC: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-3000-28SC:admin#config vlan_trunk ports 7 state disable
Command: config vlan_trunk ports 7 state disable

Success.

DGS-3000-28SC:admin#config vlan_trunk ports 6-7 state disable
Command: config vlan_trunk ports 6-7 state disable

Success.

DGS-3000-28SC:admin#
```

102-4 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-3000-28SC:admin#show vlan_trunk
Command: show vlan_trunk


VLAN Trunk Global Setting
----------------------------
VLAN Trunk Status  : Disabled
VLAN Trunk Member Ports : 1-5


DGS-3000-28SC:admin#
```

The following example displays the VLAN information which will also display VLAN trunk setting:

```
DGS-3000-28SC: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-3000-28SC:admin#
```

Chapter 103 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

103-1 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 - Specify 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-3000-28SC:admin#enable voice_vlan v2
Command: enable voice_vlan v2

Success.

DGS-3000-28SC:admin#
```

103-2 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-3000-28SC:admin#disable voice_vlan
Command: disable voice_vlan

Success.

DGS-3000-28SC:admin#
```

103-3 config voice_vlan priority

Description

This command is used to configure the voice VLAN priority. The voice VLAN priority will be the priority associated with the voice VLAN traffic to distinguish the QoS of the voice traffic from data traffic.

Format

config voice_vlan priority <int 0-7>

Parameters

<int 0-7> - Enter the priotity of the voice VLAN. This value must be between 0 and 7. The default priority is 5.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To set the priority of the voice VLAN to be 6:

```
DGS-3000-28SC:admin#config voice_vlan priority 6
Command: config voice_vlan priority 6

Success.

DGS-3000-28SC:admin#
```

103-4 config voice_vlan oui

Description

This command is used to configure the user-defined voice traffic's OUI. The OUI is used to identify the voice traffic. There are a number of pre-defined OUIs. The user can further define the user-defined OUIs if needed.The user-defined OUI cannot be the same as the pre-defined OUI.

The following are the pre-defined voice traffic's OUI:

OUI	Vendor	Mnemonic Name
00:E0:BB	3COM.	3com
00:03:6B	Cisco	cisco
00:E0:75	Veritel	veritel
00:D0:1E	Pingtel	pingtel
00:01:E3	Siemens	siemens
00:60:B9	NEC/ Philips	nec&philips
00:0F:E2	Huawei-3COM	huawei&3com
00:09:6E	Avaya	avaya

Format

config voice_vlan oui [add | delete] <macaddr> <macmask> {description <desc 32>}

Parameters

add - Adds a user-defined OUI of a voice device vendor.
delete - Delets a user-defined OUI of a voice device vendor.
<macaddr> - Enter the user-defined OUI MAC address.
<macmask> - Enter the user-defined OUI MAC address mask.

description - (Optional) The description for the user-defined OUI. **<desc 32>** - Enter the description here. This value can be up to 32 characters long.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To add a user-defined OUI for a voice device:

```
DGS-3000-28SC:admin#config voice_vlan oui add 00-0A-0B-00-00-00 FF-FF-FF-00-00-
00
Command: config voice_vlan oui add 00-0A-0B-00-00-00 FF-FF-FF-00-00-00

Success.

DGS-3000-28SC:admin#
```

103-5 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 - Specify to configure all ports.
state - The voice VLAN function state on ports. The default state is disabled. **enable** - Specify that the voice VLAN function for this switch will be enabled. **disable** - Specify that the voice VLAN function for this switch will be disabled.
mode - The voice VLAN mode. The default mode is auto. **auto** - Specify that the voice VLAN mode will be set to auto. **tag** - (Optional) When the port is working in auto-tagged mode, and learns about a voice device through the device's OUI, it will join the voice VLAN as a tagged member automatically. When the voice device sends voice VLAN tagged packets, the Switch will change its priority. When the voice device sends untagged packets, it will forward them to port's PVID VLAN. **untag** - (Optional) When the port is working in auto-untagged mode, and the port captures a voice device through the device's OUI, it will join the voice VLAN as an untagged member automatically. When the voice device sends voice VLAN tagged packets, the Switch will forward them according to the tag. When the voice device sends voice VLAN untagged packets, it will assign priority and voice VLAN ID into this packet. When the Switch receives LLDP-MED packets, it checks the VLAN ID, tagged flag and priority flag.The switch should follow the tagged flag and priority setting. By default, the mode is auto untagged. **manual** - Specify 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-3000-28SC:admin#config voice_vlan ports 4-6 state enable
Command: config voice_vlan ports 4-6 state enable

Success.

DGS-3000-28SC:admin#
```

To set the mode auto to voice VLAN ports 3-5:

```
DGS-3000-28SC:admin#config voice_vlan ports 3-5 mode auto
Command: config voice_vlan ports 3-5 mode auto

Success.

DGS-3000-28SC:admin#
```

103-6 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-3000-28SC:admin#config voice_vlan aging_time 60
Command: config voice_vlan aging_time 60

Success.

DGS-3000-28SC:admin#
```

103-7 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 - Specify that the sending of a voice VLAN log will be enabled.
disable - Specify 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-3000-28SC:admin#config voice_vlan log state enable
Command: config voice_vlan log state enable

Success.

DGS-3000-28SC:admin#
```

103-8 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-3000-28SC: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-3000-28SC:admin#
```

To display the voice VLAN global information when voice VLAN is disabled:

```
DGS-3000-28SC: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-3000-28SC:admin#
```

103-9 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-3000-28SC: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-3000-28SC:admin#
```

103-10 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-3000-28SC: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-3000-28SC:admin#
```

103-11 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) Specify 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-3000-28SC: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-3000-28SC:admin#
```

103-12 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-3000-28SC: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-3000-28SC:admin#
```

Chapter 104 Web-based Access Control (WAC) Command List

enable wac
disable wac
config wac authorization attributes {radius [enable | disable] | local [enable | disable]}(1)
config wac ports [<portlist> | all] {state [enable | disable] | aging_time [infinite | <min 1-1440>] | idle_time [infinite | <min 1-1440>] | block_time [<sec 0-300>]}(1)
config wac method [local | radius]
config wac default_redirpath <string 128>
config wac clear_default_redirpath
config wac virtual_ip {<ipaddr> | <ipv6addr>}(1)
config wac switch_http_port <tcp_port_number 1-65535> {[http | https]}
create wac user <username 15> {[vlan <vlan_name 32> | vlanid <vlanid 1-4094>]}
delete wac [user <username 15> | all_users]
config wac user <username 15> [vlan <vlan_name 32> | vlanid <vlanid 1-4094> | clear_vlan]
show wac
show wac ports {<portlist>}
show wac user
show wac auth_state ports {<portlist>}
clear wac auth_state [ports [<portlist> | all] {authenticated | authenticating | blocked} | macaddr <macaddr>]
config wac authentication_page element [default | page_title <desc 128> | login_window_title <desc 64> | user_name_title <desc 32> | password_title <desc 32> | logout_window_title <desc 64> | notification_line <value 1-5> <desc 128>]
show wac authenticate_page
config wac trap state [enable | disable]

104-1 enable wac

Description

This command is used to enable the WAC function.

Format

enable wac

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To enable the WAC function:

```
DGS-3000-28SC:admin#enable wac
Command: enable wac

Success.

DGS-3000-28SC:admin#
```

104-2 disable wac

Description

This command is used to disable the WAC function.

Format

disable wac

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To disable the WAC function:

```
DGS-3000-28SC:admin#disable wac
Command: disable wac

Success.

DGS-3000-28SC:admin#
```

104-3 config wac authorization attributes

Description

This command is used to configure the acceptance of an authorized configuration. When the authorization is enabled for WAC's RADIUS, the authorized data assigned by the RADUIS server will be accepted if the global authorization network is enabled. When the authorization is enabled for WAC's local, the authorized data assigned by the local database will be accepted.

Format

config wac authorization attributes {radius [enable | disable] | local [enable | disable]}(1)

Parameters

radius - If specified to enable, the authorized data assigned by the RADUIS server will be accepted if the global authorization network is enabled. The default state is enabled. **enable** - Specify to enable authorized data assigned by the RADIUS server to be accepted. **disable** - Specify to disable authorized data assigned by the RADIUS server from being accepted.
local - If specified to enable, the authorized data assigned by the local database will be accepted if the global authorization network is enabled. The default state is enabled. **enable** - Specify to enable authorized data assigned by the local database to be accepted. **disable** - Specify to disable authorized data assigned by the local database from being accepted.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the acceptance of an authorized configuration:

```
DGS-3000-28SC:admin#config wac authorization attributes local disable
Command: config wac authorization attributes local disable

Success.

DGS-3000-28SC:admin#
```

104-4 config wac ports

Description

This command is used to configure the WAC port parameters.

Format

config wac ports [<portlist> | all] {state [enable | disable] | aging_time [infinite | <min 1-1440>] | idle_time [infinite | <min 1-1440>] | block_time [<sec 0-300>]}(1)

Parameters

<portlist> - Enter a range of ports to configure.
all - Specify to configure all ports.
state - Specify to enable or disable the WAC state. **enable** - Specify to enable the WAC state. **disable** - Specify to disable the WAC state.
aging_time - Specify a time period during which an authenticated host will be kept in authenticated state. The default value is 1440 minutes. **infinite** - Specify to indicate the authenticated host on the port will not ageout. **<min 1-1440>** - Enter an ageout value between 1 and 1440 minutes.
idle_time - Specify a time period after which an authenticated host will be moved to un-authenticated state if there is no traffic during that period. The default value is infinite. **infinite** - Specify to indicate the host will not be removed from the authenticated state due to

idle of traffic. **<min 1-1440>** - Enter an idle time between 1 and 1440 minutes.
block_time - If a host fails to pass the authentication, it will be blocked for this period of time before it can be re-authenticated.The default value is 60 seconds. **<sec 0-300>** - Enter a block time between 0 and 300 seconds.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the WAC port state:

```
DGS-3000-28SC:admin#config wac ports 1-8 state enable
Command: config wac ports 1-8 state enable

Success.

DGS-3000-28SC:admin#
```

To configure the WAC port aging time:

```
DGS-3000-28SC:admin#config wac ports 1-5 aging_time 200
Command: config wac ports 1-5 aging_time 200

Success.

DGS-3000-28SC:admin#
```

104-5 config wac method

Description

This command is used to allow specification of the RADIUS protocol used by WAC to complete RADIUS authentication. WAC shares other RADIUS configuration with 802.1X. When using this command to set the RADIUS protocol, users must make sure the RADIUS server added by the config RADIUS command supports the protocol.

Format

config wac method [local | radius]

Parameters

local - Specify the authentication will be done via the local database.
radius - Specify the authentication will be done via the RADIUS server.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the WAC authentication method:

```
DGS-3000-28SC:admin#config wac method radius
Command: config wac method radius

Success.

DGS-3000-28SC:admin#
```

104-6 config wac default_redirpath

Description

This command is used to configure the WAC default redirect path. If default redirect path is configured, the user will be redirected to the default redirect path after successful authentication. When the string is cleared, the client will not be redirected to another URL after successful authentication.

Format

config wac default_redirpath <string 128>

Parameters

<string 128> - Enter the URL that the client will be redirected to after successful authentication. By default, the redirected path is cleared.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the WAC default redirect path:

```
DGS-3000-28SC:admin#config wac default_redirpath http://www.dlink.com
Command: config wac default_redirpath http://www.dlink.com

Success.

DGS-3000-28SC:admin#
```

104-7 config wac clear_default_redirpath

Description

This command is used to clear the WAC default redirect path. When the string is cleared, the client will not be redirected to another URL after successful authentication.

Format

config wac clear_default_redirpath

Parameters

None.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To clear the WAC default redirect path:

```
DGS-3000-28SC:admin#config wac clear_default_redirpath
Command: config wac clear_default_redirpath

Success.

DGS-3000-28SC:admin#
```

104-8 config wac virtual_ip

Description

This command is used to configure the virtual IP address for WAC. The virtual IP of WAC is used to accept authentication request from unauthenticated host. Only requests sent to this IP will get response correctly.

This IP does not respond to ARP request or ICMP packet!

NOTE: The WAC virtual IP address should be configured before enabling WAC because WAC will not work correctly if the virtual IP address is not set. A warning message “Warning! WAC virtual IPv4 or IPv6 address is not configured.” will be prompted even when enabling WAC successfully.

Format

config wac virtual_ip {<ipaddr> | <ipv6addr>}(1)

Parameters

<ipaddr> - Enter the IPv4 address of the virtual IP.
<ipv6addr> - Enter the IPv6 address of the virtual IP

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

Set virtual IP address:

```
DGS-3000-28SC:admin# config wac virtual_ip 1.1.1.1
Command: config wac virtual_ip 1.1.1.1

Success.

DGS-3000-28SC:admin#
```

104-9 config wac switch_http_port

Description

This command is used to configure the TCP port which the WAC switch listens to. The TCP port for HTTP or HTTPs is used to identify the HTTP or HTTPs packets that will be trapped to CPU for authentication processing, or to access the login page. If not specified, the default port number for HTTP is 80, and the default port number for HTTPS is 443. If no protocol is specified, the protocol is HTTP.

Format

config wac switch_http_port <tcp_port_number 1-65535> {[http | https]}

Parameters

<tcp_port_number 1-65535> - Enter a TCP port which the WAC switch listens to and uses to finish the authenticating process.
http - (Optional) Specify that WAC runs HTTP protocol on this TCP port.
https - (Optional) Specify that WAC runs HTTPS protocol on this TCP port.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure a TCP port which the WAC switch listens to:

```
DGS-3000-28SC:admin# config wac switch_http_port 8888 http
Command: config wac switch_http_port 8888 http

Success.

DGS-3000-28SC:admin#
```

104-10 create wac user

Description

This command is used to create accounts for Web-based Access Control. This user account is independent of the login user account. If VLAN is not specified, the user will not get a VLAN assigned after the authentication.

Format

create wac user <username 15> {[vlan <vlan_name 32> | vlanid <vlanid 1-4094>]}

Parameters

<username 15> - Enter the user account for Web-based Access Control.
vlan - (Optional) Specify the authentication VLAN name. **<vlan_name 32>** - Enter the authentication VLAN name. The VLAN name can be up to 32 characters long.
vlanid - (Optional) Specify the authentication VLAN ID number. **<vlanid 1-4094>** - Enter the authentication VLAN ID number. The VLAN ID must be between 1 and 4094.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To create a WAC account:

```
DGS-3000-28SC:admin# create wac user abc vlanid 123
Command: create wac user abc vlanid 123
Enter a case-sensitive new password:**
 Enter the new password again for confirmation:**
Success.

DGS-3000-28SC:admin#
```

104-11 delete wac

Description

This command is used to delete an account.

Format

delete wac [user <username 15> | all_users]

Parameters

user - Specify the user account for Web-based Access Control. **<username 15>** - Enter the user account for Web-based Access Control. The username can be up to 15 characters long.

all_users - Specify this option to delete all current WAC users.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To delete a WAC account:

```
DGS-3000-28SC:admin#delete wac user duhon
Command: delete wac user duhon

Success.

DGS-3000-28SC:admin#
```

104-12 config wac user

Description

This command is used to change the VLAN associated with a user.

Format

config wac user <username 15> [vlan <vlan_name 32> | vlanid <vlanid 1-4094> | clear_vlan]

Parameters

<username 15> - Enter the name of user account which will change its VID.
vlan - Specify the authentication VLAN name. **<vlan_name 32>** - Enter the authentication VLAN name. The VLAN name can be up to 32 characters long.
vlanid - Specify the authentication VLAN ID. **<vlanid 1-4094>** - Enter the authentication VLAN ID. The VLAN ID must be between 1 and 4094.
clear_vlan - Specify to clear the specified VLAN.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To configure the user's VLAN:

```
DGS-3000-28SC:admin# config wac user abc vlanid 100
Command: config wac user abc vlanid 100

Enter a old password:**
Enter a case-sensitive new password:**
Enter the new password again for confirmation:**
Success.

DGS-3000-28SC:admin#
```

104-13 show wac

Description

This command is used to display the WAC global setting.

Format

show wac

Parameters

None.

Restrictions

None.

Example

To show WAC:

```
DGS-3000-28SC:admin# show wac
Command: show wac

Web-based Access Control
-----------------------------------
State                   : Enabled
Method                  : RADIUS
Redirect Path           : http://www.dlink.com
Virtual IP              : 0.0.0.0
Virtual IPv6            : 2000::20
Switch HTTP Port        : 80 (HTTP)
RADIUS Authorization    : Enabled
Local Authorization     : Enabled
Trap State              : Enabled

DGS-3000-28SC:admin#
```

104-14 show wac ports

Description

This command is used to display WAC port information.

Format

show wac ports {<portlist>}

Parameters

<portlist> - (Optional) Enter a range of member ports to display the status.

Restrictions

None.

Example

To display WAC ports 1 to 3:

```
DGS-3000-28SC:admin# show wac ports 1-3
Command: show wac ports 1-3

Port        State         Aging Time      Idle Time      Block Time
                          (min)           (min)          (sec)
-------    --------      ------------     ----------     -----------
1          Disabled      1440             Infinite       60
2          Disabled      1440             Infinite       60
3          Disabled      1440             Infinite       60

DGS-3000-28SC:admin#
```

104-15 show wac user

Description

This command is used to display WAC user accounts.

Format

show wac user

Parameters

None.

Restrictions

None.

Example

To show Web authentication user accounts:

```
DGS-3000-28SC:admin# show wac user
Command: show wac user

User Name          Password           VID
-----------------  -----------------  ---------
123                ************       1000

Total Entries   : 1

DGS-3000-28SC:admin#
```

104-16 show wac auth_state ports

Description

This command is used to display the authentication state for ports.

Format

show wac auth_state ports {<portlist>}

Parameters

<portlist> - (Optional) Enter the list of ports whose WAC authentication state will be displayed.

Restrictions

None.

Example

To display the WAC authentication status of ports:

```
DGS-3000-28SC:admin# show wac auth_state ports
Command: show wac auth_state ports

P:Port-based   Pri:Priority

Port    MAC Address       Original  State       VID Pri Aging Time/ Idle
                           RX VID                    Block Time  Time
------ ------------------- ---- -------------- ---- -- ----------- ----
  31   00-05-5D-F9-16-76    1    Authenticating -    -  27          -

 Total Authenticating Hosts  : 1
 Total Authenticated Hosts   : 0
 Total Blocked Hosts         : 0

DGS-3000-28SC:admin#
```

104-17 clear wac auth_state

Description

This command is used to clear the authentication state of a port. The port will return to un-authenticated state. All the timers associated with the port will be reset.

Format

clear wac auth_state [ports [<portlist> | all] {authenticated | authenticating | blocked} | macaddr <macaddr>]

Parameters

ports - Specify the list of ports whose WAC state will be cleared.	
	<portlist> - Enter a range of ports.
	all - Specify to clear all ports.
	authenticated - (Optional) Specify to clear all authenticated users for a port.
	authenticating - (Optional) Specify to clear all authenticating users for a port.
	blocked - (Optional) Specify to clear all blocked users for a port.
macaddr - Specify to clear a specific user.	
	<macaddr> - Enter the MAC address here.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To clear the WAC authentication state of ports 1 to 5:

```
DGS-3000-28SC:admin# clear wac auth_state ports 1-5
Command: clear wac auth_state ports 1-5

Success.

DGS-3000-28SC:admin#
```

104-18 config wac authentication_page element

Description

This command is used to customize the authenticate page elements.

Format

config wac authentication_page element [default | page_title <desc 128> | login_window_title <desc 64> | user_name_title <desc 32> | password_title <desc 32> | logout_window_title <desc 64> | notification_line <value 1-5> <desc 128>]

Parameters

default - Specify to reset the page elements to default.
page_title - Specify to configure the title of the authentication page. **<desc 128>** - Enter the page title used here. This value can be up to 128 characters long.
login_window_title - Specify to configure the login window title of the authentication page **<desc 64>** - Enter the login window title used here. This value can be up to 64 characters long.
user_name_title - Specify to configure the user name title of the authentication page **<desc 32>** - Enter the user name title used here. This value can be up to 32 characters long.
password_title - Specify to configure the password title of the authentication page. **<desc 32>** - Enter the password title used here. This value can be up to 32 characters long.
logout_window_title - Specify to configure the logout window title of the authentication page. **<desc 64>** - Enter the lohout window title used here. This value can be up to 64 characters long.
notification_line - Specify to set the notification information by line in authentication Web pages. **<value 1-5>** - Enter the notification line number used here. This value must be between 1 and 5. **<desc 128>** - Enter the notification line description used here. This value can be up to 128 characters long.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

To customize the authenticate page elements:

```
DGS-3000-28SC:admin# config wac authentication_page element notification_line 1
Copyright @ 2014 D-Link All Rights Reserved
Command: config wac authentication_page element notification_line 1 Copyright @
2014 D-Link All Rights Reserved


Success.


DGS-3000-28SC:admin#
```

104-19 show wac authenticate_page

Description

This command is used to show the elements of the customized authenticate pages.

Format

show wac authenticate_page

Parameters

None.

Restrictions

None.

Example

The following example displays the authentication page elements:

```
DGS-3000-28SC:admin# show wac authenticate_page
Command: show wac authenticate_page

Page Title                              : D-Link
Login Window Title                      : Authentication Login
User Name Title                         : User Name
Password Title                          : Password
Logout Window Title                     : Logout
Notification                            :
Copyright @ 2014 D-Link All Rights Reserved
Site: http://support.dlink.com

DGS-3000-28SC:admin#
```

104-20 config wac trap state

Description

This command is used to enable or disable the WAC trap state.

Format

config wac trap state [enable | disable]

Parameters

enable - Specify to enable the WAC trap state.
disable - Specify to disable the WAC trap state.

Restrictions

Only Administrators, Operators and Power-Users can issue this command.

Example

This example show how to enable the WAC trap state.

```
DGS-3000-28SC:admin# config wac trap state enable
Command: config wac trap state enable

Success.

DGS-3000-28SC: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                                          V5.00.003
-------------------------------------------------------------------------------

  Power On Self Test ....................................  100 %

  MAC Address   : 00-01-02-03-04-00
  H/W Version   : A1

  Please Wait, Loading V5.00.020 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. The option **force_agree** means to reset the whole configuration 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.

Command	Parameters
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	Log Description	Severity
MAC-based Access Control	Event description: A host failed to pass the authentication Log Message: MAC-based Access Control unauthenticated host (MAC: <macaddr>, Port <[unitID:]portNum>, VID: <vid>) Parameters description: macaddr: MAC address unitID: The unit ID. portNum: The port number. vid: VLAN ID on which the host exists	Critical
	Event description: The authorized user number on a port has reached the maximum user limit. Log Message: Port < [unitID:]portNum> enters MAC-based Access Control stop learning state. Parameters description: unitID: The unit ID. portNum: The port number.	Warning
	Event description: The authorized user number on a port is below the maximum user limit in a time interval (interval is project dependent). Log Message: Port <[unitID:]portNum> recovers from MAC-based Access Control stop learning state. Parameters description: unitID: The unit ID. portNum: The port number.	Warning
	Event description: The authorized user number on the whole device has reached the maximum user limit. Log Message: MAC-based Access Control enters stop learning state. Parameters description: None	Warning
	Event description: The authorized user number on the whole device is below the maximum user limit in a time interval (interval is project dependent). Log Message: MAC-based Access Control recovers from stop learning state. Parameters description: None	Warning
	Event description: A host has passed the authentication. Log Message: MAC-based Access Control host login successful (MAC: <macaddr>, port: <[unitID]portNum>, VID: <vid>) Parameters description: macaddr: The MAC address. unitID: The unit ID. portNum: The port number. vid: The VLAN ID on which the host exists.	Informational
	Event description: A host has aged out. Log Message: MAC-based Access Control host aged out (MAC: <macaddr>, port: <[unitID]portNum>, VID: <vid>) Parameters description: macaddr: The MAC address unitID: The unit ID. portNum: The port number. vid: The VLAN ID on which the host exists.	Informational
DHCPv6 client	Event description: DHCPv6 client interface administrator state changed. Log Message: DHCPv6 client on interface <ipif-name> changed state to [enabled | disabled]. Parameters description:	Informational

	<ipif-name>: Name of the DHCPv6 client interface.	
	Event description: DHCPv6 client obtains an ipv6 address from a DHCPv6 server. Log Message: DHCPv6 client obtains an ipv6 address < ipv6address > on interface <ipif-name>. Parameters description: ipv6address: ipv6 address obtained from a DHCPv6 server. ipif-name: Name of the DHCPv6 client interface.	Informational
	Event description: The ipv6 address obtained from a DHCPv6 server starts renewing. Log Message: The IPv6 address < ipv6address > on interface <ipif-name> starts renewing. Parameters description: ipv6address: ipv6 address obtained from a DHCPv6 server. ipif-name: Name of the DHCPv6 client interface.	Informational
	Event description: The ipv6 address obtained from a DHCPv6 server renews success. Log Message: The IPv6 address < ipv6address > on interface <ipif-name> renews success. Parameters description: ipv6address: ipv6 address obtained from a DHCPv6 server. ipif-name: Name of the DHCPv6 client interface.	Informational
	Event description: The ipv6 address obtained from a DHCPv6 server starts rebinding Log Message: The IPv6 address < ipv6address > on interface <ipif-name> starts rebinding. Parameters description: ipv6address: ipv6 address obtained from a DHCPv6 server. ipif-name: Name of the DHCPv6 client interface.	Informational
	Event description: The ipv6 address obtained from a DHCPv6 server rebinds success Log Message: The IPv6 address < ipv6address > on interface <ipif-name> rebinds success. Parameters description: ipv6address: ipv6 address obtained from a DHCPv6 server. ipif-name: Name of the DHCPv6 client interface..	Informational
	Event description: The ipv6 address from a DHCPv6 server was deleted. Log Message: The IPv6 address < ipv6address > on interface <ipif-name> was deleted. Parameters description: ipv6address: ipv6 address obtained from a DHCPv6 server. ipif-name: Name of the DHCPv6 client interface.	Informational
	Event description: DHCPv6 client PD interface administrator state changed. Log Message: [DHCPv6_CLIENT(8):]DHCPv6 client PD on interface <intf-name> changed state to <enabled | disabled> Parameters description: intf-name: Name of the DHCPv6 client PD interface.	Informational
	Event description: DHCPv6 client PD obtains an IPv6 prefix from a delegation router. Log Message: [DHCPv6_CLIENT(9):]DHCPv6 client PD obtains an ipv6 prefix < ipv6networkaddr> on interface <intf-name> Parameters description: ipv6networkaddr: ipv6 preifx obtained from a delegation router. intf-name: Name of the DHCPv6 client PD interface.	Informational
	Event description: The IPv6 prefix obtained from a delegation router starts renewing. Log Message: [DHCPv6_CLIENT(10):]The IPv6 prefix < ipv6networkaddr > on interface <intf-name> starts renewing. Parameters description: ipv6networkaddr: IPv6 prefix obtained from a delegation router. intf-name: Name of the DHCPv6 client PD interface.	Informational
	Event description: The IPv6 prefix obtained from a delegation router renews success. Log Message: [DHCPv6_CLIENT(11):]The IPv6 prefix < ipv6networkaddr > on interface <intf-name> renews success.	Informational

	Parameters description: ipv6anetworkaddr: IPv6 prefix obtained from a delegation router. intf-name: Name of the DHCPv6 client PD nterface.	
	Event description: The IPv6 prefix obtained from a delegation router starts rebinding. Log Message: [DHCPv6_CLIENT(12):]The IPv6 prefix < ipv6networkaddr > on interface <intf-name> starts rebinding. Parameters description: ipv6address: IPv6 prefix obtained from a delegation router. intf-name: Name of the DHCPv6 client PD interface.	Informational
	Event description: The IPv6 prefix obtained from a delegation router rebinds success. Log Message: [DHCPv6_CLIENT(13):]The IPv6 prefix < ipv6networkaddr > on interface <intf-name> rebinds success. Parameters description: ipv6address: IPv6 prefix obtained from a delegation router. intf-name: Name of the DHCPv6 client PD interface.	Informational
	Event description: The IPv6 prefix from a delegation router was deleted. Log Message: [DHCPv6_CLIENT(14):]The IPv6 prefix < ipv6networkaddr > on interface <intf-name> was deleted. Parameters description: ipv6address: IPv6 prefix obtained from a delegation router. intf-name: Name of the DHCPv6 client PD interface.	Informational
DHCPv6 relay	Event description: DHCPv6 relay on a specify interface's administrator state changed Log Message: DHCPv6 relay on interface <ipif-name> changed state to [enabled | disabled] Parameters description: <ipif-name>: Name of the DHCPv6 relay agent interface.	Informational
IP directed-broadcast	Event description: IP Directed-broadcast rate exceed 50 packets per second on a certain subnet. Log Message: IP Directed Broadcast packet rate is high on subnet. [(IP: %s)] Parameters description: IP: the Broadcast IP destination address.	Informational
	Event description: IP Directed-broadcast rate exceed 100 packets per second Log Message: IP Directed Broadcast rate is high. Parameters description:	Informational
RCP	Event description: Firmware upgraded successfully. Log Message: [Unit <unitID>,] Firmware upgraded by <session> successfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>, Server IP: <serverIP>, File Name: <pathFile>) Parameters description: unitID: Represent the id of the device in the stacking system. session: The user's session, ex: console, SNMP, WEB… username: Represent current login user. (It should be community name for SNMP.) ipaddr: Represent client IP address. macaddr: Represent client MAC address. serverIP: RCP Server IP address pathFile: Path and file name on RCP Server.	Informational
	Event description: Firmware upgrade was unsuccessful Log Message: [Unit <unitID>,] Firmware upgrade by <session> unsuccessfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>, Server IP: <serverIP>, File Name: <pathFile>) Parameters description: unitID: Represent the id of the device in the stacking system. session: The user's session, ex: console, SNMP, WEB…	warning

	username: Represent current login user. (It should be community name for SNMP.) ipaddr: Represent client IP address. macaddr: Represent client MAC address. serverIP: RCP Server IP address pathFile: Path and file name on RCP Server.	
	Event description: Firmware successfully uploaded. Log Message: Log Message: Firmware uploaded by <session> successfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>, Server IP: <serverIP>, File Name: <pathFile>) Parameters description: session: The user's session, ex: console, SNMP, WEB… username: Represent current login user. (It should be community name for SNMP.) ipaddr: Represent client IP address. macaddr: Represent client MAC address. serverIP: RCP Server IP address pathFile: Path and file name on RCP Server.	informational
	Event description: Firmware upload was unsuccessful. Log Message: Firmware upload by <session> unsuccessfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>, Server IP: <serverIP>, File Name: <pathFile>) Parameters description: session: The user's session, ex: console, SNMP, WEB… username: Represent current login user. (It should be community name for SNMP.) ipaddr: Represent client IP address. macaddr: Represent client MAC address. serverIP: RCP Server IP address pathFile: Path and file name on RCP Server.	warning
	Event description: Configuration successfully downloaded. Log Message: Configuration downloaded by <session> successfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>, Server IP: <serverIP>, File Name: <pathFile>) Parameters description: session: The user's session, ex: console, SNMP, WEB… username: Represent current login user. (It should be community name for SNMP.) ipaddr: Represent client IP address. macaddr: Represent client MAC address. serverIP: RCP Server IP address pathFile: Path and file name on RCP Server.	informational
	Event description: Configuration download was unsuccessful. Log Message: Configuration download by <session> unsuccessfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>, Server IP: <serverIP>, File Name: <pathFile>) Parameters description: session: The user's session, ex: console, SNMP, WEB… username: Represent current login user. (It should be community name for SNMP.) ipaddr: Represent client IP address. macaddr: Represent client MAC address. serverIP: RCP Server IP address pathFile: Path and file name on RCP Server.	warning
	Event description: Configuration successfully uploaded.	informational

	Log Message: Configuration uploaded by <session> successfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>, Server IP: <serverIP>, File Name: <pathFile>) Parameters description: session: The user's session, ex: console, SNMP, WEB… username: Represent current login user. (It should be community name for SNMP.) ipaddr: Represent client IP address. macaddr: Represent client MAC address. serverIP: RCP Server IP address pathFile: Path and file name on RCP Server.	
	Event description: Configuration upload was unsuccessful. Log Message: Configuration upload by <session> unsuccessfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>, Server IP: <serverIP>, File Name: <pathFile>) Parameters description: session: The user's session, ex: console, SNMP, WEB… username: Represent current login user. (It should be community name for SNMP.) ipaddr: Represent client IP address. macaddr: Represent client MAC address. serverIP: RCP Server IP address pathFile: Path and file name on RCP Server.	warning
	Event description: Log message successfully uploaded. Log Message: Log message uploaded by <session> successfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>, Server IP: <serverIP>, File Name: <pathFile>) Parameters description: session: The user's session, ex: console, SNMP, WEB… username: Represent current login user. (It should be community name for SNMP.) ipaddr: Represent client IP address. macaddr: Represent client MAC address. serverIP: RCP Server IP address pathFile: Path and file name on RCP Server.	informational
	Event description: Log message upload was unsuccessful. Log Message: Log message upload by <session> unsuccessfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>, Server IP: <serverIP>, File Name: <pathFile>) Parameters description: session: The user's session, ex: console, SNMP, WEB… username: Represent current login user. (It should be community name for SNMP.) ipaddr: Represent client IP address. macaddr: Represent client MAC address. serverIP: RCP Server IP address pathFile: Path and file name on RCP Server.	warning
TFTP/FTP	Event description: Firmware upgraded successfully. Log Message: [Unit <unitID>,] Firmware upgraded by <session> successfully (Username: <username>, IP: <ipaddr>, MAC: <macaddr>, Server IP: <serverIP>, File Name: <pathFile>) Parameters description: unitID: Represent the id of the device in the stacking system.	Informational

	session: The user's session, ex: console, SNMP, WEB… username: Represent current login user. (It should be community name for SNMP.) ipaddr: Represent client IP address. macaddr: Represent client MAC address. serverIP: TFTP/FTP Server IP address pathFile: Path and file name on TFTP/FTP Server.	
	Event description: Firmware upgrade was unsuccessful Log Message: [Unit <unitID>,] Firmware upgrade by <session> was unsuccessful! (Username: <username>, IP: <ipaddr>, MAC: <macaddr>, Server IP: <serverIP>, File Name: <pathFile>) Parameters description: unitID: Represent the id of the device in the stacking system. session: The user's session, ex: console, SNMP, WEB… username: Represent current login user. (It should be community name for SNMP.) ipaddr: Represent client IP address. macaddr: Represent client MAC address. serverIP: TFTP/FTP Server IP address pathFile: Path and file name on TFTP/FTP Server.	warning
	Event description: Firmware successfully uploaded. Log Message: Firmware successfully uploaded by <session> (Username: <username>, IP: <ipaddr>, MAC: <macaddr>, Server IP: <serverIP>, File Name: <pathFile>) Parameters description: session: The user's session, ex: console, SNMP, WEB… username: Represent current login user. (It should be community name for SNMP.) ipaddr: Represent client IP address. macaddr: Represent client MAC address. serverIP: TFTP/FTP Server IP address pathFile: Path and file name on TFTP/FTP Server.	informational
	Event description: Firmware upload was unsuccessful. Log Message: Firmware upload by <session> was unsuccessful! (Username: <username>, IP: <ipaddr>, MAC: <macaddr>, Server IP: <serverIP>, File Name: <pathFile>) Parameters description: session: The user's session, ex: console, SNMP, WEB… username: Represent current login user. (It should be community name for SNMP.) ipaddr: Represent client IP address. macaddr: Represent client MAC address. serverIP: TFTP/FTP Server IP address pathFile: Path and file name on TFTP/FTP Server.	warning
	Event description: Configuration successfully downloaded. Log Message: Configuration successfully downloaded by <session> (Username: <username>, IP: <ipaddr>, MAC: <macaddr>, Server IP: <serverIP>, File Name: <pathFile>) Parameters description: session: The user's session, ex: console, SNMP, WEB… username: Represent current login user. (It should be community name for SNMP.) ipaddr: Represent client IP address. macaddr: Represent client MAC address. serverIP: TFTP/FTP Server IP address	informational

	pathFile: Path and file name on TFTP/FTP Server.	
	Event description: Configuration download was unsuccessful. Log Message: Configuration download by <session> was unsuccessful! (Username: <username>, IP: <ipaddr>, MAC: <macaddr>, Server IP: <serverIP>, File Name: <pathFile>) Parameters description: session: The user's session, ex: console, SNMP, WEB… username: Represent current login user. (It should be community name for SNMP.) ipaddr: Represent client IP address. macaddr: Represent client MAC address. serverIP: TFTP/FTP Server IP address pathFile: Path and file name on TFTP/FTP Server.	warning
	Event description: Configuration successfully uploaded. Log Message: Configuration successfully uploaded by <session> (Username: <username>, IP: <ipaddr>, MAC: <macaddr>, Server IP: <serverIP>, File Name: <pathFile>) Parameters description: session: The user's session, ex: console, SNMP, WEB… username: Represent current login user. (It should be community name for SNMP.) ipaddr: Represent client IP address. macaddr: Represent client MAC address. serverIP: TFTP/FTP Server IP address pathFile: Path and file name on TFTP/FTP Server.	informational
	Event description: Configuration upload was unsuccessful. Log Message: Configuration upload by <session> was unsuccessful! (Username: <username>, IP: <ipaddr>, MAC: <macaddr>, Server IP: <serverIP>, File Name: <pathFile>) Parameters description: session: The user's session, ex: console, SNMP, WEB… username: Represent current login user. (It should be community name for SNMP.) ipaddr: Represent client IP address. macaddr: Represent client MAC address. serverIP: TFTP/FTP Server IP address pathFile: Path and file name on TFTP/FTP Server.	warning
	Event description: Log message successfully uploaded. Log Message: Log message successfully uploaded by <session> (Username: <username>, IP: <ipaddr>, MAC: <macaddr>, Server IP: <serverIP>, File Name: <pathFile>) Parameters description: session: The user's session, ex: console, SNMP, WEB… username: Represent current login user. (It should be community name for SNMP.) ipaddr: Represent client IP address. macaddr: Represent client MAC address. serverIP: TFTP/FTP Server IP address pathFile: Path and file name on TFTP/FTP Server.	informational
	Event description: Log message upload was unsuccessful. Log Message: Log message upload by <session> was unsuccessful! (Username: <username>, IP: <ipaddr>, MAC: <macaddr>, Server IP: <serverIP>, File Name: <pathFile>)	warning

	Parameters description: session: The user's session, ex: console, SNMP, WEB… username: Represent current login user. (It should be community name for SNMP.) ipaddr: Represent client IP address. macaddr: Represent client MAC address. serverIP: TFTP/FTP Server IP address pathFile: Path and file name on TFTP/FTP Server.	
DNS Resolver	Event description: Duplicate Domain name cache added, leads a dynamic domain name cache be deleted Log Message: [DNS_RESOLVER(1):]Duplicate Domain name case name: <domainname>, static IP: <ipaddr>, dynamic IP:<ipaddr> Parameters description: domainame: the domain name string. ipaddr: IP address.	Informational
ARP	Event description: Gratuituios ARP detected duplicate IP. Log Message: Conflict IP was detected with this device (IP: <ipaddr>, MAC: <macaddr>, Port <[unitID:]portNum>, Interface: <ipif_name>). Parameters description: ipaddr: The IP address which is duplicated with our device. macaddr: The MAC address of the device that has duplicated IP address as our device. unitID: 1.Interger value;2.Represent the id of the device in the stacking system. portNum: 1.Interger value;2.Represent the logic port number of the device. ipif_name: The name of the interface of the switch which has the conflic IP address.	Warning
TELNET	Event description: Successful login through Telnet. Log Message: Successful login through Telnet (Username: <username>, IP: <ipaddr>) Parameters description: ipaddr: The IP address of telnet client. username: the user name that used to login telnet server.	Informational
	Event description: Login failed through Telnet. Log Message: Login failed through Telnet (Username: <username>, IP: <ipaddr>) Parameters description: ipaddr: The IP address of telnet client. username: the user name that used to login telnet server.	Warning
	Event description: Logout through Telnet. Log Message: Logout through Telnet (Username: <username>, IP: <ipaddr>) Parameters description: ipaddr: The IP address of telnet client. username: the user name that used to login telnet server.	Informational
	Event description: Telnet session timed out. Log Message: Telnet session timed out (Username: <username>, IP: <ipaddr>). Parameters description: ipaddr: The IP address of telnet client. username: the user name that used to login telnet server.	Informational
Interface	Event description: Port link up. Log Message: Port <[unitID:]portNum> link up, <link state> Parameters description: unitID: 1.Interger value;2.Represent the id of the device in the stacking system. portNum: 1.Interger value;2.Represent the logic port number of the device. link state: for ex: , 100Mbps FULL duplex	Informational
	Event description: Port link down. Log Message: Port <[unitID:]portNum> link down Parameters description: unitID: 1.Interger value;2.Represent the id of the device in the stacking system. portNum: 1.Interger value;2.Represent the logic port number of the device.	Informational
802.1X	Event description: 802.1X Authentication failure. Log Message: 802.1X Authentication failure [for <reason>] from (Username: <username>, Port: <[unitID:]portNum>, MAC: <macaddr>)	Warning

	Parameters description: reason: The reason for the failed authentication. username: The user that is being authenticated. unitID: The unit ID. portNum: The switch port number. macaddr: The MAC address of thr authenticated device.	
	Event description: 802.1X Authentication successful. Log Message: 802.1X Authentication successful from (Username: <username>, Port: <[unitID:]portNum>, MAC: <macaddr>) Parameters description: username: The user that is being authenticated. unitID: The unit ID. portNum: The switch port number. macaddr: The MAC address of the authenticated device.	Informational
RADIUS	Event description: VID assigned from RADIUS server after RADIUS client is authenticated by RADIUS server successfully .This VID will be assigned to the port and this port will be the VLAN untagged port member. Log Message: RADIUS server <ipaddr> assigned VID :<vlanID> to port <[unitID:]portNum> (account :<username>) Parameters description: ipaddr: The IP address of the RADIUS server. vlanID: The VID of RADIUS assigned VLAN. unitID: The unit ID. portNum: The port number. Username: The user that is being authenticated.	Informational
	Event description: Ingress bandwidth assigned from RADIUS server after RADIUS client is authenticated by RADIUS server successfully .This Ingress bandwidth will be assigned to the port. Log Message: RADIUS server <ipaddr> assigned ingress bandwith :<ingressBandwidth> to port <[unitID:]portNum> (account : <username>) Parameters description: ipaddr: The IP address of the RADIUS server. ingressBandwidth: The ingress bandwidth of RADIUS assign. unitID: The unit ID. portNum: The port number. Username: The user that is being authenticated.	Informational
	Event description: Egress bandwidth assigned from RADIUS server after RADIUS client is authenticated by RADIUS server successfully .This egress bandwidth will be assigned to the port. Log Message: RADIUS server <ipaddr> assigned egress bandwith :<egressBandwidth> to port <[unitID:]portNum> (account: <username>) Parameters description: ipaddr: The IP address of the RADIUS server. egressBandwidth: The egress bandwidth of RADIUS assign. unitID: The unit ID. portNum: The port number. Username: The user that is being authenticated.	Informational
	Event description: 802.1p default priority assigned from RADIUS server after RADIUS client is authenticated by RADIUS server successfully. This 802.1p default priority will be assigned to the port. Log Message: RADIUS server <ipaddr> assigned 802.1p default priority:<priority> to port <[unitID:]portNum> (account : <username>) Parameters description: ipaddr: The IP address of the RADIUS server. priority: Priority of RADIUS assign. unitID: The unit ID. portNum: The port number. Username: The user that is being authenticated.	Informational
	Event description: Failed to assign ACL profiles/rules from RADIUS server. Log Message: RADIUS server <ipaddr> assigns <username> ACL failure at port <[unitID]portNum> (<string>)	Warning

	Parameters description: ipaddr: The IP address of the RADIUS server. unitID: The unit ID. portNum: The port number. Username: The user that is being authenticated. string: The failed RADIUS ACL command string.	
LLDP-MED	Event description: LLDP-MED topology change detected Log Message: LLDP-MED topology change detected (on port <portNum>. chassis id: <chassisType>, <chassisID>, port id: <portType>, <portID>, device class: <deviceClass>) Parameters description: portNum: The port number. chassisType: chassis ID subtype. Value list: 1. chassisComponent(1) 2. interfaceAlias(2) 3. portComponent(3) 4. macAddress(4) 5. networkAddress(5) 6. interfaceName(6) 7. local(7) chassisID: chassis ID. portType: port ID subtype. Value list: 1. interfaceAlias(1) 2. portComponent(2) 3. macAddress(3) 4. networkAddress(4) 5. interfaceName(5) 6. agentCircuitId(6) 7. local(7) portID: port ID. deviceClass: LLDP-MED device type.	Notice
	Event description: Conflict LLDP-MED device type detected Log Message: Conflict LLDP-MED device type detected (on port < portNum >, chassis id: < chassisType>, <chassisID>, port id: < portType>, <portID>, device class: <deviceClass>) Parameters description: portNum: The port number. chassisType: chassis ID subtype. Value list: 1. chassisComponent(1) 2. interfaceAlias(2) 3. portComponent(3) 4. macAddress(4) 5. networkAddress(5) 6. interfaceName(6) 7. local(7) chassisID: chassis ID. portType: port ID subtype. Value list: 1. interfaceAlias(1) 2. portComponent(2) 3. macAddress(3) 4. networkAddress(4) 5. interfaceName(5) 6. agentCircuitId(6) 7. local(7) portID: port ID. deviceClass: LLDP-MED device type.	Notice
	Event description: Incompatible LLDP-MED TLV set detected Log Message: Incompatible LLDP-MED TLV set detected (on port < portNum >, chassis id: < chassisType>, <chassisID>, port id: < portType>, <portID>, device class: <deviceClass>) Parameters description:	Notice

	portNum: The port number. chassisType: chassis ID subtype. Value list: 1. chassisComponent(1) 2. interfaceAlias(2) 3. portComponent(3) 4. macAddress(4) 5. networkAddress(5) 6. interfaceName(6) 7. local(7) chassisID: chassis ID. portType: port ID subtype. Value list: 1. interfaceAlias(1) 2. portComponent(2) 3. macAddress(3) 4. networkAddress(4) 5. interfaceName(5) 6. agentCircuitId(6) 7. local(7) portID: port ID. deviceClass: LLDP-MED device type.	
Voice VLAN	Event description: When a new voice device is detected in the port. Log Message: New voice device detected (Port <portNum>, MAC <macaddr>) Parameters description: portNum : The port number. macaddr: Voice device MAC address	Informational
	Event description: When a port which is in auto Voice VLAN mode joins the Voice VLAN Log Message: Port < portNum > add into Voice VLAN <vid > Parameters description: portNum : The port number. vid:VLAN ID	Informational
	Event description: When a port leaves the Voice VLAN and at the same time, no voice device is detected in the aging interval for that port, the log message will be sent. Log Message: Port < portNum > remove from Voice VLAN <vid > Parameters description: portNum : The port number. vid:VLAN ID	Informational
DULD	Event description: A unidirectional link has been detected on this port Log Message: Detected unidirectional link on (Port<[unitID:]portNum>) Parameters description: unitID: the unit ID portNum: port number	Informational
Stacking	Event description: Hot insertion. Log Message: Unit: <unitID>, MAC: <macaddr> Hot insertion. Parameters description: unitID: Box ID. Macaddr: MAC address.	Informational
	Event description: Hot removal. Log Message: Unit: <unitID>, MAC: <macaddr> Hot removal. Parameters description: unitID: Box ID. Macaddr: MAC address.	Informational
	Event description: Stacking topology change. Log Message: Stacking topology is <Stack_TP_TYPE>. Master(Unit <unitID>, MAC:<macaddr>). Parameters description: Stack_TP_TYPE: The stacking topology type is one of the following: 1. Ring, 2. Chain.	Informational

	unitID: Box ID. Macaddr: MAC address.	
	Event description: Backup master changed to master. Log Message: Backup master changed to master. Master (Unit: <unitID>). Parameters description: unitID: Box ID.	Informational
	Event description: Slave changed to master Log Message: Slave changed to master. Master (Unit: <unitID>). Parameters description: unitID: Box ID.	Informational
	Event description: Box ID conflict. Log Message: Hot insert failed, box ID conflict: Unit <unitID> conflict (MAC: <macaddr> and MAC: <macaddr>). Parameters description: unitID: Box ID. macaddr: The MAC addresses of the conflicting boxes.	Critical
SNMP	Event Description: SNMP request received with invalid community string Log Message: SNMP request received from <ipaddr> with invalid community string. Parameters Description: ipaddr: The IP address.	Informational
Web (SSL)	Event description: Successful login through Web. Log Message: Successful login through Web (Username: <username>, IP: <ipaddr>). Parameters description: username: The use name that used to login HTTP server. ipaddr: The IP address of HTTP client.	Informational
	Event description: Login failed through Web. Log Message: Login failed through Web (Username: <username>, IP: <ipaddr>). Parameters description: username: The use name that used to login HTTP server. ipaddr: The IP address of HTTP client.	Warning
	Event description: Web session timed out. Log Message: Web session timed out (Username: <usrname>, IP: <ipaddr>). Parameters description: username: The use name that used to login HTTP server. ipaddr: The IP address of HTTP client.	Informational
	Event description: Logout through Web. Log Message: Logout through Web (Username: %S, IP: %S). Parameters description: username: The use name that used to login HTTP server. ipaddr: The IP address of HTTP client.	Informational
	Event description: Successful login through Web(SSL). Log Message: Successful login through Web(SSL) (Username: <username>, IP: <ipaddr>). Parameters description: username: The use name that used to login SSL server. ipaddr: The IP address of SSL client.	Informational
	Event description: Login failed through Web(SSL). Log Message: Login failed through Web(SSL) (Username: <username>, IP: <ipaddr>). Parameters description: username: The use name that used to login SSL server. ipaddr: The IP address of SSL client.	Warning
	Event description: Web(SSL) session timed out. Log Message: Web(SSL) session timed out (Username: <username>, IP: <ipaddr>). Parameters description: username: The use name that used to login SSL server.	Information

	ipaddr: The IP address of SSL client.	
	Event description: Logout through Web(SSL). Log Message: Logout through Web(SSL) (Username: <username>, IP: <ipaddr>). Parameters description: username: The use name that used to login SSL server. ipaddr: The IP address of SSL client.	Information
Port Security	Event description: Address full on a port Log Message: Port security violation (MAC: < macaddr > on port:: < unitID: portNum >) Parameters description: macaddr: The violation MAC address. unitID: The unit ID. portNum: The port number.	Warning
Safe Guard	Event description: The host enters the mode of normal. Log Message: Unit< unitID >, Safeguard Engine enters NORMAL mode Parameters description: unitID: The unit ID.	Informational
	Event description: The host enters the mode of exhausted. Log Message: Unit< unitID >, Safeguard Engine enters EXHAUSTED mode Parameters description: unitID: The unit ID.	Warning
DoS Log	Event description: The DOS is possibly snoofed. Log Message: Possible spoofing attack from IP: <ipaddr>, MAC: <macaddr>, port: <unitID: portNum> Parameters description: Ipaddr: The ip address macaddr: The violation MAC address. unitID: The unit ID. portNum: The port number.	Critical
	Event description: The DOS attack is blocked. Log Message:<dos_name> is blocked from (IP: <ipaddr> Port: < portNum >): Parameters description: <dos_name>: the DoS attack type Ipaddr: The ip address portNum: The port number.	Informational
AAA	Event description: Successful login. Log Message: Successful login through <Console | Telnet | Web(SSL) | SSH>(Username: <username>, IP: <ipaddr | ipv6address>). Parameters description: ipaddr: IP address. username: user name. ipv6address: IPv6 address.	Informational
	Event description: Login failed. Log Message: Login failed through <Console | Telnet | Web(SSL)| SSH> (Username: <username>, IP: <ipaddr | ipv6address>). Parameters description: ipaddr: IP address. username: user name. ipv6address: IPv6 address.	Warning
	Event description: Logout. Log Message: Logout through <Console | Telnet | Web(SSL)| SSH> (Username: <username>, IP: <ipaddr | ipv6address>). Parameters description: ipaddr: IP address. username: user name. ipv6address: IPv6 address.	Informational
	Event description: session timed out. Log Message: <Console | Telnet | Web(SSL)| SSH> session timed out (Username: <username>, IP: <ipaddr | ipv6address>).	Informational

	Parameters description: ipaddr: IP address. username: user name. ipv6address: IPv6 address.	
	Event description: SSH server is enabled. Log Message: SSH server is enabled	Informational
	Event description: SSH server is disabled. Log Message: SSH server is disabled	Informational
	Event description: Authentication Policy is enabled. Log Message: Authentication Policy is enabled (Module: AAA).	Informational
	Event description: Authentication Policy is disabled. Log Message: Authentication Policy is disabled (Module: AAA).	Informational
	Event description: Login failed due to AAA server timeout or improper configuration. Log Message: Login failed through <Console | Telnet | Web(SSL)| SSH> from <ipaddr | ipv6address> due to AAA server <ipaddr | ipv6address> timeout or improper configuration (Username: <username>). Parameters description: ipaddr: IP address. ipv6address: IPv6 address. username: user name.	Warning
	Event description: Successful Enable Admin authenticated by AAA local or none or server. Log Message: Successful Enable Admin through <Console | Telnet | Web(SSL)| SSH> from <ipaddr | ipv6address> authenticated by AAA <local | none | server <ipaddr | ipv6address>> (Username: <username>). Parameters description: local: enable admin by AAA local method. none: enable admin by AAA none method. server: enable admin by AAA server method. ipaddr: IP address. ipv6address: IPv6 address. username: user name.	Informational
	Event description: Enable Admin failed due to AAA server timeout or improper configuration. Log Message: Enable Admin failed through <Console | Telnet | Web(SSL)| SSH> from <ipaddr | ipv6address> due to AAA server <ipaddr | ipv6address> timeout or improper configuration (Username: <username>) Parameters description: ipaddr: IP address. ipv6address: IPv6 address. username: user name.	Warning
	Event description: Enable Admin failed authenticated by AAA local or server. Log Message: Enable Admin failed through <Console | Telnet | Web(SSL)| SSH> from <ipaddr | ipv6address> authenticated by AAA < local | server <ipaddr | ipv6address>> (Username: <username>). Parameters description: local: enable admin by AAA local method. server: enable admin by AAA server method. ipaddr: IP address. ipv6address: IPv6 address. username: user name.	Warning
	Event description: Successful login authenticated by AAA local or none or server. Log Message: Successful login through <Console | Telnet | Web(SSL) | SSH> from < ipaddr | ipv6address > authenticated by AAA <local | none | server <ipaddr | ipv6address>> (Username: <username>). Parameters description: local: specify AAA local method. none: specify none method. server: specify AAA server method. ipaddr: IP address. ipv6address: IPv6 address. username: user name.	Informational
	Event description: Login failed authenticated by AAA local or server.	Warning

	Log Message: Login failed through <Console | Telnet | Web(SSL)| SSH> from <ipaddr | ipv6address> authenticated by AAA <local | server <ipaddr | ipv6address>> (Username: <username>). Parameters description: local: specify AAA local method. server: specify AAA server method. ipaddr: IP address. ipv6address: IPv6 address. username: user name.	
WAC	Event description: When a client host fails to authenticate. Log Message: WAC unauthenticated user (User Name: <string>, IP: <ipaddr | ipv6address>, MAC: <macaddr>, Port: <[unitID:]portNum>) Parameters description: string: User name ipaddr: IP address ipv6address: IPv6 address macaddr: MAC address unitID: The unit ID portNum : The port number	Warning
	Event description: This log will be triggered when the number of authorized users reaches the maximum user limit on the whole device. Log Message: WAC enters stop learning state.	Warning
	Event description: This log will be triggered when the number of authorized users is below the maximum user limit on whole device in a time interval (5 min). Log Message: WAC recovered from stop learning state.	Warning
	Event description: When a client host authenticated successful. Log Message: WAC authenticated user (Username: <string>, IP: <ipaddr | ipv6address>, MAC: <macaddr>, Port: <[unitID:] portNum>) Parameters description: string: User name ipaddr: IP address ipv6address: IPv6 address macaddr: MAC address unitID: The unit ID portNum : The port number	Informational
LBD	Event Description: Loop back is detected under port-based mode. Log Message: Port < [unitID:] portNum> LBD loop occurred. Port blocked. Parameters Description: portNum: The port number.	Critical
	Event Description: Port recovered from LBD blocked state under port-based mode. Log Message: Port < [unitID:] portNum>LBD port recovered. Loop detection restarted Parameters Description: portNum: The port number.	Informational
	Event Description: Loop back is detected under VLAN-based mode. Log Message: Port < [unitID:] portNum> VID <vlanID> LBD loop occurred. Packet discard begun Parameters Description: portNum: The port number. vlanID: the VLAN ID number.	Critical
	Event Description: Port recovered from LBD blocked state under VLAN-based mode. Log Message: Port < [unitID:] portNum> VID <vlanID> LBD recovered. Loop detection restarted Parameters Description: portNum: The port number. vlanID: the VLAN ID number.	Informational
	Event Description: The number of VLAN in which loop back occurs hit the specified number. Log Message: Loop VLAN number overflow. Parameters Description: None	Informational

IMPB	Event description: Dynamic IMPB entry conflicts with static ARP. Log Message: Dynamic IMPB entry conflicts with static ARP(IP: <ipaddr>, MAC: <macaddr>, Port <[unitID:]portNum>) Parameters description: ipaddr: IP address macaddr: MAC address unitID: The unit ID portNum : The port number	Warning
	Event description: Dynamic IMPB entry conflicts with static FDB. Log Message: Dynamic IMPB entry conflicts with static FDB(IP: [<ipaddr> | <ipv6addr>], MAC: <macaddr>, Port <[unitID:]portNum>) Parameters description: ipaddr: IP address ipv6addr: IPv6 address macaddr: MAC address unitID: The unit ID portNum : The port number	Warning
	Event description: Dynamic IMPB entry conflicts with static IMPB. Log Message: Dynamic IMPB entry conflicts with static IMPB(IP: [<ipaddr> | <ipv6addr>], MAC: <macaddr>, Port <[unitID:]portNum>). Parameters description: ipaddr: IP address ipv6addr: IPv6 address macaddr: MAC address unitID: The unit ID portNum : The port number	Warning
	Event description: Creating IMPB entry failed due to no ACL rule being available. Log Message: Creating IMPB entry failed due to no ACL rule being available(IP:[<ipaddr> | <ipv6addr>], MAC: <macaddr>, Port <[unitID:]portNum>) Parameters description: ipaddr: IP address ipv6addr: IPv6 address macaddr: MAC address unitID: The unit ID portNum : The port number	Warning
	Event description: IMPB checks a host illegal. Log Message: Unauthenticated IP-MAC address and discarded by IMPB (IP: [< ipaddr > | < ipv6addr >], MAC :< macaddr >, Port <[unitID:]portNum >). Parameters description: ipaddr: IP address ipv6addr: IPv6 address macaddr: MAC address unitID: The unit ID portNum : The port number	Warning
	Event description: Dynamic IMPB entry conflicts with static ND Log Message: Dynamic IMPB entry conflicts with static ND (IP: [< ipaddr > | < ipv6addr >], MAC: <macaddr>, Port <[unitID:]portNum>) Parameters description: ipaddr: IP address ipv6addr: IPv6 address macaddr: MAC address unitID: The unit ID portNum : The port number	Warning
	Event description: Port shutdown due to the DHCP rate excludes the rate limiting. Log Message: Port < [unitID:] portNum> is currently shut down due to the DHCP rate excludes the rate limiting. Parameters description: unitID: The unit ID portNum : The port number	Warning
	Event description: Port recovery due to the DHCP auto-recovery timer is timeout.	Informational

	Log Message: Port < [unitID:] portNum> is currently recovery due to the DHCP auto-recovery timer is timeout. Parameters description: unitID: The unit ID portNum : The port number	
Traffic Control	Event description: Broadcast storm occurrence. Log Message: Port <portNum> Broadcast storm is occurring. Parameters description: portNum: The port number.	Warning
	Event description: Broadcast storm cleared. Log Message: Port <portNum> Broadcast storm has cleared. Parameters description: portNum: The port number.	Informational
	Event description: Multicast storm occurrence. Log Message: Port <portNum> Multicast storm is occurring. Parameters description: portNum: The port number.	Warning
	Event description: Multicast Storm cleared. Log Message: Port <portNum>Multicast storm has cleared. Parameters description: portNum: The port number.	Informational
	Event description: Port shut down due to a packet storm Log Message: Port <portNum> is currently shut down due to a packet storm Parameters description: portNum: The port number.	Warning
DHCP Server Screening	Event description: Detected untrusted DHCP server IP address. Log Message: Detected untrusted DHCP server(IP: <ipaddr>, Port <portNum>) Parameters description: ipaddr: The untrusted IP address which has been detected with our device. portNum : Represent the logic port number of the device.	Informational
DHCPv6 Server Screening	Event Description: Detected untrusted DHCPv6 server IP address Log Message: Detected untrusted DHCPv6 server (IP: <ipv6addr>, Port:<[unitID:]portNum>) Parameters Description: ipv6addr: The untrusted source IP of DHCPv6 server which has been detected with our device. unitID: The unit ID.	Informational
ICMPv6 Router Advertisement Filter	Event Description: Detected untrusted source IP in ICMPv6 Router Advertisement Message. Log Message: Detected untrusted source IP of ICMPv6 Router Advertisement message (IP: <ipv6addr>, Port:<[unitID:]portNum>) Parameters Description: Ipv6addr: The untrusted ICMPv6 Router Advertisement address which has been detected with our device unitID: The unit ID. portNum: The port number.	Informational
ERPS	Event description: Signal failure detected Log Message: Signal failure detected on node (MAC: <macaddr>) Parameters description: macaddr: The system MAC address of the node	Notice
	Event description: Signal failure cleared Log Message: Signal failure cleared on node (MAC: <macaddr>) Parameters description: macaddr: The system MAC address of the node	Notice
	Event description: RPL owner conflict Log Message: RPL owner conflicted on the ring (MAC: <macaddr>) Parameters description:	Warning

	macaddr: The system MAC address of the node	
MSTP Debug Enhancement	Event description: Topology changed. Log Message: Topology changed [([Instance:<InstanceID>] ,port:<[unitID:] portNum> ,MAC: <macaddr>)] Parameters description: InstanceID: Instance ID. portNum:Port ID macaddr: MAC address	Notice
	Event description: Spanning Tree new Root Bridge Log Message: [CIST | CIST Regional | MSTI Regional] New Root bridge selected([Instance: <InstanceID>]MAC: <macaddr> Priority :<value>) Parameters description: InstanceID: Instance ID. macaddr: Mac address value: priority value	Informational
	Event description: Spanning Tree Protocol is enabled Log Message: Spanning Tree Protocol is enabled	Informational
	Event description: Spanning Tree Protocol is disabled Log Message: Spanning Tree Protocol is disabled	Informational
	Event description: New root port Log Message: New root port selected [([Instance:<InstanceID>], port:<[unitID:] portNum>)] Parameters description: InstanceID: Instance ID. portNum:Port ID	Notice
	Event description: Spanning Tree port status changed Log Message: Spanning Tree port status changed [([Instance:<InstanceID>], port:<[unitID:] portNum>)] <old_status> -> <new_status> Parameters description: InstanceID: Instance ID. portNum: Port ID old_status: Old status new_status: New status	Notice
	Event description: Spanning Tree port role changed. Log Message: Spanning Tree port status changed. [([Instance:<InstanceID>], port:<[unitID:] portNum>)] <old_role> -> <new_role> Parameters description: InstanceID: Instance ID. portNum:Port ID/ old_role: Old role new_status:New role	Informational
	Event description: Spannnig Tree instance created. Log Message: Spanning Tree instance created. Instance:<InstanceID> Parameters description: InstanceID: Instance ID.	Informational
	Event description: Spannnig Tree instance deleted. Log Message: Spanning Tree instance deleted. Instance:<InstanceID> Parameters description: InstanceID: Instance ID.	Informational
	Event description: Spanning Tree Version changed. Log Message: Spanning Tree version changed. New version:<new_version> Parameters description: new_version: New STP version.	Informational
	Event description: Spanning Tree MST configuration ID name and revision level changed. Log Message: Spanning Tree MST configuration ID name and revision level changed (name:<name> ,revision level <revision_level>). Parameters description:	Informational

	name : New name. revision_level:New revision level.	
	Event description: Spanning Tree MST configuration ID VLAN mapping table deleted. Log Message: Spanning Tree MST configuration ID VLAN mapping table changed (instance: <InstanceID> delete vlan <startvlanid> [- <endvlanid>]). Parameters description: InstanceID: Instance ID. startvlanid- endvlanid:VLANlist	Informational
	Event description: Spanning Tree MST configuration ID VLAN mapping table added. Log Message: Spanning Tree MST configuration ID VLAN mapping table changed (instance: <InstanceID> add vlan <startvlanid> [- <endvlanid>]). Parameters description: InstanceID: Instance ID. startvlanid- endvlanid:VLANlist	Informational
CFM	Event description: Cross-connect is detected Log Message: CFM cross-connect. VLAN:<vlanid>, Local(MD Level:<mdlevel>, Port <[unitID:]portNum>, Direction:<mepdirection>) Remote(MEPID:<mepid>, MAC:<macaddr>) Parameters description: vlanid: Represents the VLAN identifier of the MEP. mdlevel: Represents the MD level of the MEP. unitID: Represents the ID of the device in the stacking system. portNum: Represents the logical port number of the MEP. mepdirection: Can be "inward" or "outward". mepid: Represents the MEPID of the MEP. The value 0 means unknown MEPID. macaddr: Represents the MAC address of the MEP. The value all zeros mean unknown MAC address. Note: In CFM hardware mode, remote MEP information (mepid and macaddr) is unknown.	Critical
	Event description: Error CFM CCM packet is detected Log Message: CFM error ccm. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <[unitID:]portNum>, Direction:<mepdirection>) Remote(MEPID:<mepid>, MAC:<macaddr>) Parameters description: vlanid: Represents the VLAN identifier of the MEP. mdlevel: Represents MD level of the MEP. unitID: Represents the ID of the device in the stacking system. portNum: Represents the logical port number of the MEP. mepdirection: Can be "inward" or "outward". mepid: Represents the MEPID of the MEP. The value 0 means unknown MEPID. macaddr: Represents the MAC address of the MEP. The value all zeros means unknown MAC address. Note: In CFM hardware mode, remote MEP information (mepid and macaddr) is unknown.	Warning
	Event description: Can not receive the remote MEP's CCM packet Log Message: CFM remote down. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <[unitID:]portNum>, Direction:<mepdirection>) Parameters description: vlanid: Represents the VLAN identifier of the MEP. mdlevel: Represents the MD level of the MEP. unitID: Represents the ID of the device in the stacking system. portNum: Represents the logical port number of the MEP. mepdirection: Represents the MEP direction, which can be "inward" or "outward". mepid: Represents the MEPID of the MEP. macaddr: Represents the MAC address of the MEP.	Warning
	Event description: Remote MEP's MAC reports an error status Log Message: CFM remote MAC error. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <[unitID:]portNum>, Direction:<mepdirection>) Parameters description: vlanid: Represents the VLAN identifier of the MEP.	Warning

	mdlevel: Represents the MD level of the MEP. unitID: Represents the ID of the device in the stacking system. portNum: Represents the logical port number of the MEP. mepdirection: Represents the MEP direction, which can be "inward" or "outward". mepid: Represents the MEPID of the MEP. macaddr: Represents the MAC address of the MEP.	
	Event description: Remote MEP detects CFM defects Log Message: CFM remote detects a defect. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <[unitID:]portNum>, Direction:<mepdirection>) Parameters description: vlanid: Represents the VLAN identifier of the MEP. mdlevel: Represents the MD level of the MEP. unitID: Represents the ID of the device in the stacking system. portNum: Represents the logical port number of the MEP. mepdirection: Represents the MEP direction, which can be "inward" or "outward". mepid: Represents the MEPID of the MEP. macaddr: Represents the MAC address of the MEP.	Informational
CFM Extension	Event description: AIS condition detected Log Message: AIS condition detected. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <[unitID:]portNum>, Direction:<mepdirection>, MEPID:<mepid>) Parameters description: vlanid: Represents the VLAN identifier of the MEP. mdlevel: Represents the MD level of the MEP. unitID: Represents the ID of the device in the stacking system. portNum: Represents the logical port number of the MEP. mepdirection: Represents the direction of the MEP. This can be "inward" or "outward". mepid: Represents the MEPID of the MEP.	Notice
	Event description: AIS condition cleared Log Message: AIS condition cleared. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <[unitID:]portNum>, Direction:<mepdirection>, MEPID:<mepid>) Parameters description: vlanid: Represents the VLAN identifier of the MEP. mdlevel: Represents the MD level of the MEP. unitID: Represents the ID of the device in the stacking system. portNum: Represents the logical port number of the MEP. mepdirection: Represents the direction of the MEP. This can be "inward" or "outward". mepid: Represents the MEPID of the MEP.	Notice
	Event description: LCK condition detected Log Message: LCK condition detected. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <[unitID:]portNum>, Direction:<mepdirection>, MEPID:<mepid>) Parameters description: vlanid: Represents the VLAN identifier of the MEP. mdlevel: Represents the MD level of the MEP. unitID: Represents the ID of the device in the stacking system. portNum: Represents the logical port number of the MEP. mepdirection: Represents the direction of the MEP. This can be "inward" or "outward". mepid: Represents the MEPID of the MEP.	Notice
	Event description: LCK condition cleared Log Message: LCK condition cleared. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <[unitID:]portNum>, Direction:<mepdirection>, MEPID:<mepid>) Parameters description: vlanid: Represents the VLAN identifier of the MEP. mdlevel: Represents the MD level of the MEP. unitID: Represents the ID of the device in the stacking system. portNum: Represents the logical port number of the MEP. mepdirection: Represents the direction of the MEP. This can be "inward" or "outward". mepid: Represents the MEPID of the MEP.	Notice
Port	Event description: port linkup Log Message: Port <port> link up, <nway> Parameters description: port: Represents the logical port number.	Informational

	nway: Represents the speed and duplex of link.	
	Event description: port linkdown Log Message: Port <port> link down Parameters description: port: Represents the logical port number.	Informational
DDM	Event description: DDM recover from DDM alarm or warning threshold Log Message: Port <[unitID:]portNum> optic module [thresholdType] back to normal Parameters description: unitID: The unit ID. portNum: The port number. thresholdType: the DDM threshold type. The value should be one of the following values: temperature, supply voltage, bias current, TX power, RX power.	critical
	Event description: DDM exceeded DDM alarm threshold Log Message: Port <[unitID:]portNum> optic module [thresholdType] exceeded the [thresholdSubType] alarm threshold Parameters description: unitID: The unit ID. portNum: The port number. thresholdType: the DDM threshold type. The value should be one of the following values: temperature, supply voltage, bias current, TX power, RX power. thesholdSubType: the DDM threshold sub type, the value should be “high” or “low”.	warning
	Event description: DDM exceeded DDM warning threshold Log Message: Port <[unitID:]portNum> optic module [thresholdType] exceeded the [thresholdSubType] warning threshold Parameters description: unitID: The unit ID. portNum: The port number. thresholdType: the DDM threshold type. The value should be one of the following values: temperature, supply voltage, bias current, TX power, RX power. thesholdSubType: the DDM threshold sub type, the value should be “high” or “low”.	warning
BPDU Attack Protection	Event description: BPDU attack happened. Log Message: Port<[unitID:]portNum> enter BPDU under protection state (mode: drop / block / shutdown) Parameters description: unitID: The unit ID. portNum: The port number. mode:The BPDU currnt state	Informational
	Event description: BPDU attack automatically recover. Log Message: Port <[unitID:]portNum> recover from BPDU under protection state automatically Parameters description: unitID: The unit ID. portNum: The port number.	Informational
	Event description: BPDU attack manually recover. Log Message: Port<[unitID:]portNum> recover from BPDU under protection state automatically Parameters description: unitID: The unit ID. portNum: The port number.	Informational
SSH	Event description: Successfully download client public keys. Log Message: SSH client public keys file was upgraded successfully (Username: <username>, IP: < ipaddr | ipv6address >) Parameters description: username: The username upgraded client public keys file. ipaddr: Represent client IP address. ipv6address: Represent client IP address.	Informational

OAM	Event description: Dying gasp event(remote) Log Message: OAM dying gasp event received (Port<[unitID:] portNum>) Parameters description: unitID: The unit ID. portNum: The port number.	Warning
	Event description: Dying gasp event(local) Log Message: Device encountered an OAM dying gasp event.	Warning
	Event description: Critical event(remote) Log Message: OAM critical event received (Port<[unitID:] portNum>) Parameters description: unitID: The unit ID. portNum: The port number.	Warning
	Event description: Critical event(local) Log Message: Device encountered an OAM critical event	Warning
	Event description: Errored Symbol Period Event(remote) Log Message: Errored symbol period event received (Port <[unitID:]portNum>) Parameters description: unitID: The unit ID. portNum: The port number.	Warning
	Event description: Errored Frame Event Log Message: Errored frame event received(Port <[unitID:] portNum>) Parameters description: unitID: The unit ID. portNum: The port number.	Warning
	Event description: Errored Frame Period Event Log Message: Errored frame period event received(Port <[unitID:]portNum>) Parameters description: unitID: The unit ID. portNum: The port number.	Warning
	Event description: Errored Frame Seconds Summary Event Log Message: Errored frame seconds summary event received (Port <[unitID:]portNum>) Parameters description: unitID: The unit ID. portNum: The port number.	Warning
	Event description: Remote loopback start Log Message: OAM Remote loopback started (Port <[unitID:] portNum>) Parameters description: unitID: The unit ID. portNum: The port number.	Warning
	Event description: Remote loopback stop Log Message: OAM Remote loopback stopped (Port <[unitID:] portNum>) Parameters description: unitID: The unit ID. portNum: The port number.	Warning
Fan	Event description: Right Side Fan failed Log Message: [Uint <unitID>], Right Side Fan <value> failed Parameters description: unitID: The unit ID. value : Fans ID.	Critical
	Event description: Right Side Fan recovered Log Message: [Uint <unitID>], Right Side Fan <value> recovered	Critical

	Parameters description: unitID: The unit ID. value : Fans ID	
Temperature	Event description: Temperature sensor enters alarm state. Log Message: [Uint <unitID>], Temperature sensor <sensorID> enters alarm state (current temperature: <temperature>) Parameters description: unitID: The unit ID. sensorID: The sensor ID. temperature: The temperature.	Warning
	Event description: Temperature recovers to normal. Log Message: [Uint <unitID>], Temperature sensor <sensorID> recovers to normal state (current temperature: <temperature>) Parameters description: unitID: The unit ID. sensorID: The sensor ID. temperature: The temperature.	Informational
Power	Event description: Internal Power failed. Log Message: [Uint <unitID>], Internal Power failed Parameters description: unitID: The unit ID.	Critical
	Event description: Internal Power is recovered. Log Message: [Uint <unitID>], Internal Power is recovered Parameters description: unitID: The unit ID.	Critical
	Event description: Redundant Power failed. Log Message: [Uint <unitID>], Redundant Power failed Parameters description: unitID: The unit ID.	Critical
	Event description: Redundant Power is working. Log Message: [Uint <unitID>], Redundant Power is working Parameters description: unitID: The unit ID.	Critical

Appendix C Trap Log Entries

This table lists the trap logs found on the Switch.

Category	Trap Name	Description	OID
MAC Notification	swL2macNotification	This trap indicates the MAC addresses variation in address table Binding objects: (1)swL2macNotifyInfo	1.3.6.1.4.1.171.11.133.5.2.100.1.2.0.1
MAC-based Access Control	swMacBasedAccessControlLoggedSuccess	The trap is sent when a MAC-based Access Control host is successfully logged in. Binding objects: (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 objects: (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 objects: (1) swMacBasedAuthInfoMacIndex (2) swMacBasedAuthInfoPortIndex (3) swMacBasedAuthVID	1.3.6.1.4.1.171.12.35.11.1.0.3
LLDP(-MED)	lldpRemTablesChange	A lldpRemTablesChange notification is sent when the value of lldpStatsRemTableLastChangeTime changes. Binding objects: (1) lldpStatsRemTablesInserts (2) lldpStatsRemTablesDeletes (3) lldpStatsRemTablesDrops (4) lldpStatsRemTablesAgeouts	1.0.8802.1.1.2.0.0.1
	lldpXMedTopologyChangeDetected	A notification generated by the local device sensing a change in the topology that indicates that a new remote device attached to a local port, or a remote device disconnected or moved from one port to another. Binding objects: (1) lldpRemChassisIdSubtype (2) lldpRemChassisId (3) lldpXMedRemDeviceClass	1.0.8808.1.1.2.1.5.4795.0.1
802.3ah OAM	dot3OamThresholdEvent	This notification is sent when a local or remote threshold crossing event is detected. Binding objects: (1) dot3OamEventLogTimestamp (2) dot3OamEventLogOui (3)dot3OamEventLogType (4)dot3OamEventLogLocation (5)dot3OamEventLogWindowHi (6)dot3OamEventLogWindowLo (7)dot3OamEventLogThresholdHi (8)dot3OamEventLogThresholdLo (9)dot3OamEventLogValue (10)dot3OamEventLogRunningTotal	1.3.6.1.2.1.158.0.1

		(11)dot3OamEventLogEventTotal	
	dot3OamNonThresholdEvent	This notification is sent when a local or remote non-threshold crossing event is detected. Binding objects: (1) dot3OamEventLogTimestamp (2) dot3OamEventLogOui (3) dot3OamEventLogType (4)dot3OamEventLogLocation (5)dot3OamEventLogEventTotal	1.3.6.1.2.1.158.0.2
Up/Down-Load	agentFirmwareUpgrade	This trap is sent when the process of upgrading the firmware via SNMP has finished. Binding objects: (1) swMultiImageVersion	1.3.6.1.4.1.171.12.1.7.2.0.7
	agentCfgOperCompleteTrap	The trap is sent when the configuration is completely saved, uploaded or downloaded Binding objects: unitID agentCfgOperate agentLoginUserName	1.3.6.1.4.1.171.12.1.7.2.0.9
Gratuitous ARP	agentGratuitousARPTrap	The trap is sent when IP address conflicted. Binding objects: (1) ipaddr (2) macaddr (3) portNumber (4) agentGratuitousARPInterfaceName	1.3.6.1.4.1.171.12.1.7.2.0.5
Stacking	swUnitInsert	Unit Hot Insert notification. Binding objects: (1) swUnitMgmtId. (2) swUnitMgmtMacAddr.	1.3.6.1.4.1.171.12.11.2.2.1.0.1
	swUnitRemove	Unit Hot Remove notification. Binding objects: (1) swUnitMgmtId. (2) swUnitMgmtMacAddr.	1.3.6.1.4.1.171.12.11.2.2.1.0.2
	swUnitFailure	Unit Failure notification. Binding objects: (1) swUnitMgmtId.	1.3.6.1.4.1.171.12.11.2.2.1.0.3
	swUnitTPChange	The stacking topology change notification. Binding objects: (1) swStackTopologyType (2) swUnitMgmtId (3) swUnitMgmtMacAddr	1.3.6.1.4.1.171.12.11.2.2.1.0.4
	swUnitRoleChange	The stacking unit role change notification. Binding objects: (1) swStackRoleType (2) swUnitMgmtId	1.3.6.1.4.1.171.12.11.2.2.1.0.5
Port Security	swL2PortSecurityViolationTrap	When the port security trap is enabled, new MAC addresses that violate the pre-defined port security configuration will trigger trap messages to be sent out. Binding objects: (1)swPortSecPortIndex (2)swL2PortSecurityViolationMac	1.3.6.1.4.1.171.11.133.5.1.2.100.1.2.0.2
Safe Guard	swSafeGuardChgToNormal	This trap indicates system change operation mode from axhausted to normal. Binding objects: (1) swSafeGuardCurrentStatus	1.3.6.1.4.1.171.12.19.4.1.0.2

	swSafeGuardChgToExhausted	This trap indicates System change operation mode from normal to exhausted. Binding objects: (1) swSafeGuardCurrentStatus	1.3.6.1.4.1.171.12.19.4.1.0.1
LBD	swPortLoopOccurred	The trap is sent when a port loop occurs. Binding objects: (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 objects: (1) swLoopDetectPortIndex	1.3.6.1.4.1.171.12.41.10.0.2
	swVlanLoopOccurred	The trap is sent when a port loop occurs under LBD VLAN-based mode. Binding objects: (1) swLoopDetectPortIndex (2) swVlanLoopDetectVID	1.3.6.1.4.1.171.12.41.10.0.3
	swVlanLoopRestart	The trap is sent when a port loop restarts under LBD VLAN-based mode after the interval time. Binding objects: (1) swLoopDetectPortIndex (2) swVlanLoopDetectVID	1.3.6.1.4.1.171.12.41.10.0.4
BPDU Attack Protection	swBpduProtectionUnderAttackingTrap	BPDU attack happened, enter drop / block / shutdown mode.	1.3.6.1.4.1.171.12.76.4.0.1
	swBpduProtectionRecoveryTrap	BPDU attack automatically recover	1.3.6.1.4.1.171.12.76.4.0.2
IMPB	swIpMacBindingViolationTrap	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. Binding objects: (1) swIpMacBindingPortIndex (2) swIpMacBindingViolationIP (3) swIpMacBindingViolationMac	1.3.6.1.4.1.171.12.23.5.0.1
	swIpMacBindingIPv6ViolationTrap	When the IP-MAC Binding trap is enabled, if there's a new MAC that violates the pre-defined IPv6 IMPB configuration, a trap will be sent out. Binding objects: (1) swIpMacBindingPortIndex (2) swIpMacBindingViolationIPv6Addr (3) swIpMacBindingViolationMac	1.3.6.1.4.1.171.12.23.5.0.4
	swIpMacBindingShutdownTrap	When the rate limiting is shutdown mode and the DHCP rate excludes the limiting, a trap will be sent out. Binding objects: swIpMacBindingPortIndex	1.3.6.1.4.1.171.12.23.5.0.5
	swIpMacBindingRecoveryTrap	When the port is shutdown by DHCP rate limiting and the auto-recovery timer is timeout, a trap will be sent out. Binding objects: swIpMacBindingPortIndex	1.3.6.1.4.1.171.12.23.5.0.6
DHCP Server Screening	swFilterDetectedTrap	Send trap when an 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 objects:	1.3.6.1.4.1.171.12.37.100.0.1

		(1) swFilterDetectedIP (2) swFilterDetectedport	
	swFilterDHCPv6ServerDetectedTrap	Send trap when an illegal DHCPv6 server is detected. Binding objects: (1) swFilterDetectedIPv6 (2) swFilterDetectedport	1.3.6.1.4.1.171.12.37.100.0.2
	swFilterICMPv6RaAllNodesDetectedTrap	Send trap when an illegal ICMPv6 all-nodes RA is detected. Binding objects: (1) swFilterDetectedIPv6 (2) swFilterDetectedport	1.3.6.1.4.1.171.12.37.100.0.3
Traffic Control	swPktStormOccurred	When packet storm is detected by packet storm mechanism and take shutdown as action. Binding objects: (1) swPktStormCtrlPortIndex	1.3.6.1.4.1.171.12.25.5.0.1
	swPktStormCleared	When the packet storm is clear. Binding objects: (1) swPktStormCtrlPortIndex	1.3.6.1.4.1.171.12.25.5.0.2
ERPS	swERPSSFDetectedTrap	Signal fail detected on node.	1.3.6.1.4.1.171.12.78.4.0.1
	swERPSSFClearedTrap	Signal fail cleared on node.	1.3.6.1.4.1.171.12.78.4.0.2
	swERPSRPLOwnerConflictTrap	RPL owner conflicted on the ring.	1.3.6.1.4.1.171.12.78.4.0.3
MSTP	newRoot	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.	1.3.6.1.2.1.17.0.1
	topologyChange	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	1.3.6.1.2.1.17.0.2
CFM	dot1agCfmFaultAlarm	This trap is initiated when a connectivity defect is detected. Binding objects: (1) dot1agCfmMepHighestPrDefect	1.3.111.2.802.1.1.8.0.1
CFM Extension	swCFMExtAISOccurred	A notification is generated when local MEP enters AIS status. Binding objects: (1) dot1agCfmMdIndex (2) dot1agCfmMaIndex (3) dot1agCfmMepIdentifier	1.3.6.1.4.1.171.12.86.100.0.1
	swCFMExtAISCleared	A notification is generated when local MEP exits AIS status. Binding objects: (1) dot1agCfmMdIndex (2) dot1agCfmMaIndex (3) dot1agCfmMepIdentifier	1.3.6.1.4.1.171.12.86.100.0.2
	swCFMExtLockOccurred	A notification is generated when local MEP enters lock status. Binding objects:	1.3.6.1.4.1.171.12.86.100.0.3

		(1) dot1agCfmMdIndex (2) dot1agCfmMaIndex (3) dot1agCfmMepIdentifier	
	swCFMExtLockCleared	A notification is generated when local MEP exits lock status. Binding objects: (1) dot1agCfmMdIndex (2) dot1agCfmMaIndex (3) dot1agCfmMepIdentifier	1.3.6.1.4.1.171.12.86.100.0.4
Port	linkUp	A notification is generated when port linkup. Binding objects: (1) ifIndex, (2) if AdminStatus (3) ifOperStatu	1.3.6.1.6.3.1.1.5.4
	linkDown	A notification is generated when port linkdown. Binding objects: (1) ifIndex, (2) if AdminStatus (3) ifOperStatu	1.3.6.1.6.3.1.1.5.3
DDM	swDdmAlarmTrap	The trap is sent when any parameter value exceeds the alarm threshold value or recovers to normal status depending on the configuration of the trap action. Binding objects: (1) swDdmPort (2) swDdmThresholdType (3) swDdmThresholdExceedType (4) swDdmThresholdExceedOrRecover	1.3.6.1.4.1.171.12.72.4.0.1
	swDdmWarningTrap	The trap is sent when any parameter value exceeds the warning threshold value or recovers to normal status depending on the configuration of the trap action. Binding objects: (1) swDdmPort (2) swDdmThresholdType (3) swDdmThresholdExceedType (4) swDdmThresholdExceedOrRecover	1.3.6.1.4.1.171.12.72.4.0.2
DOS Attack Prevention	swDoSAttackDetected	This trap is sent when the specific DoS packet is received and trap is enabled. Binding objects: (1) swDoSCtrlType (2) swDoSNotifyVarIpAddr (3) swDoSNotifyVarPortNumber	1.3.6.1.4.1.171.12.59.4.0.1
System	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
Fan Status	swFanFailure	Fan Failure notification. Binding objects: 1:swFanUnitIndex 2:swFanID	1.3.6.1.4.1.171.12.11.2.2.3.0.1
	swFanRecover	Fan Recover notification. Binding objects: 1:swFanUnitIndex	1.3.6.1.4.1.171.12.11.2.2.3.0.2

		2:swFanID	
Temperature	swTemperatureHighAlarm	Temperature High Alarm notification. Binding objects: 1:swTemperatureUnitIndex 2:swTemperSensorID 3:swTemperatureCurrent	1.3.6.1.4.1.171.12.11.2.2.4.0.1.1
	swTemperatureHighRecover	Temperature High Recover notification. Binding objects: 1:swTemperatureUnitIndex 2:swTemperSensorID 3:swTemperatureCurrent	1.3.6.1.4.1.171.12.11.2.2.4.0.2.1
	swTemperatureLowAlarm	Temperature Low Alarm notification. Binding objects: 1:swTemperatureUnitIndex 2:swTemperSensorID 3:swTemperatureCurrent	1.3.6.1.4.1.171.12.11.2.2.4.0.3.1
	swTemperatureLowRecover	Temperature Low Recover notification. Binding objects: 1:swTemperatureUnitIndex 2:swTemperSensorID 3:swTemperatureCurrent	1.3.6.1.4.1.171.12.11.2.2.4.0.4.1
802.1X	swDot1xLoggedSuccess	The trap is sent when an 802.1X client pass the authentication. Binding objects: (1) swDot1xAuthPortNumber (2) swDot1xAuthVID (3) swDot1xAuthMACAddress (4) swDot1XAuthUserName	1.3.6.1.4.1.171.12.30.11.1.0.1
	swDot1xLoggedFail	The trap is sent when a 1x client failed to pass the authentication. Binding objects: (1) swDot1xAuthPortNumber (2) swDot1xAuthVID (3) swDot1xAuthMACAddress (4) swDot1XAuthUserName (5) swDot1XAuthFailReason	1.3.6.1.4.1.171.12.30.11.1.0.2
WAC	swWACLoggedSuccess	The trap is sent when a WAC client has successfully logged in. Binding objects: swWACAuthStatePort swWACAuthStateOriginalVid swWACAuthStateMACAddr swWACAuthUserName swWACClientAddrType swWACClientAddress	1.3.6.1.4.1.171.12.27.11.1.0.1
	swWACLoggedFail	The trap is sent when a WAC client fails to login. Binding objects: swWACAuthStatePort swWACAuthStateOriginalVid swWACAuthStateMACAddr swWACAuthUserName swWACClientAddrType swWACClientAddress	1.3.6.1.4.1.171.12.27.11.1.0.2
Single IP Management	swSingleIPMSColdStart	The commander switch will send this notification when its member generates a cold start notification. Binding objects: (1) swSingleIPMSID (2) swSingleIPMSMacAddr	1.3.6.1.4.1.171.12.8.6.0.11
	swSingleIPMSWarmStart	The commander switch will send this notification when its member generates a warm start notification. Binding objects:	1.3.6.1.4.1.171.12.8.6.0.12

		(1) swSingleIPMSID (2) swSingleIPMSMacAddr	
	swSingleIPMSLinkDown	The commander switch will send this notification when its member generates a link down notification. Binding objects: (1) swSingleIPMSID (2) swSingleIPMSMacAddr (3) ifIndex	1.3.6.1.4.1.171.12.8.6.0.13
	swSingleIPMSLinkUp	The commander switch will send this notification when its member generates a link up notification. Binding objects: (1) swSingleIPMSID (2) swSingleIPMSMacAddr (3) ifIndex	1.3.6.1.4.1.171.12.8.6.0.14
	swSingleIPMSAuthFail	The commander switch will send this notification when its member generates an authentation failure notification. Binding objects: (1) swSingleIPMSID (2) swSingleIPMSMacAddr	1.3.6.1.4.1.171.12.8.6.0.15
	swSingleIPMSnewRoot	The commander switch will send this notification when its member generates a new root notification. Binding objects: (1) swSingleIPMSID (2) swSingleIPMSMacAddr	1.3.6.1.4.1.171.12.8.6.0.16
	swSingleIPMSTopologyChange	The commander switch will send this notification when its member generates a topology change notification. Binding objects: (1) swSingleIPMSID (2) swSingleIPMSMacAddr	1.3.6.1.4.1.171.12.8.6.0.17
Authentication Fail	authenticationFailure	An authenticationFailure trap signifies that the SNMPv2 entity, acting in an agent role, has received a protocol message that is not properly authenticated. While all implementations of the SNMPv2 must be capable of generating this trap, the snmpEnableAuthenTraps object indicates whether this trap will be generated.	1.3.6.1.6.3.1.1.5.5
Power	swPowerStatusChg	Power Status change notification. Binding objects: 1:swPowerUnitIndex 2:swPowerID 3:swPowerStatus	1.3.6.1.4.1.171.12.11.2.2.2.0.1
	swPowerFailure	Power Failure notification. Binding objects: 1:swPowerUnitIndex 2:swPowerID 3:swPowerStatus	1.3.6.1.4.1.171.12.11.2.2.2.0.2
	swPowerRecover	Power Recover notification. Binding objects: 1:swPowerUnitIndex 2:swPowerID 3:swPowerStatus	1.3.6.1.4.1.171.12.11.2.2.2.0.3

Appendix D RADIUS Attributes Assignment

The RADIUS Attributes Assignment on the Switch 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”, the effective bandwidth will be set “no_limited”, and if the bandwidth is configured less than “0” or greater than maximum supported value, the bandwidth will be ignored.

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 terminatior).	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

A summary of the Tunnel-Private-Group-ID Attribute format is shown below.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Type    |   Length   |    Tag     |  String...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

The table below shows the definition of Tag field (different with RFC 2868):

Tag Field Value	String Field Format	Note	Usage
0x01	VLAN name (ASCII)	A tag field of greater than 0x1F is interpreted as the first octet of the field.	Required
0x02	VLAN ID (ASCII)	A tag field of greater than 0x1F is interpreted as the first octet of the field.	Required
Others (0x00, 0x03 ~ 0x1F, >0x1F)	1. When the switch receives the VLAN setting string, it will first check all existing VLAN IDs to find a	A tag field of greater than 0x1F is interpreted as	Required

Tag Field Value	String Field Format	Note	Usage
	match. 2. If a VLAN ID match was found, that VLAN will be removed. 3. If a VLAN ID match was not found, the switch will assume that the VLAN settings string uses the VLAN name. 4. It will then check all existing VLAN names to find a match.	the first octet of the field.	

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 profile_name profile1 ethernet vlan 0xFFF; ACL rule: config access_profile profile_id 1 add access_id auto_assign ethernet vlan_id 1 port all deny;	Required

If the user has configured the ACL attribute of the RADIUS server (for example, ACL profile: **create access_profile profile_id 1 profile_name profile1 ethernet vlan 0xFFF**; ACL rule: **config access_profile profile_id 1 add access_id auto_assign ethernet vlan_id 1 port all deny**), the device will assign the ACL profiles and rules according to the RADIUS server. For more information about the ACL module, please refer to the ACL chapter.