XSTACK®

# Command Line Interface Guide

Product Model: xStack® DGS-3620 Series

Layer 3 Managed Stackable Gigabit Switch

Release 2.00

# Table of Contents

# Chapter 1 Using the Command Line Interface

The DGS-3620 Layer 3 stackable Gigabit Ethernet switch series are members of the D-Link xStack® family. Ranging from 10/100/1000Mbps edge switches to core gigabit switches, the xStack® switch family has been future-proof designed to provide a stacking architecture with fault tolerance, flexibility, port density, robust security and maximum throughput with a user-friendly management interface for the networking professional.

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 Harware Installation Guide.

## 1-1 Accessing the Switch via the Serial Port

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

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

A computer running a terminal emulation program capable of emulating a VT-100 terminal and a serial port configured as above is then connected to the Switch's serial port via an RJ-45 to RS-232 DB-9 convertor cable.

With the serial port properly connected to a management computer, the following screen should be visible.

```
                          DGS-3620-28SC Gigabit Ethernet Switch
                                Command Line Interface

                               Firmware: Build 2.00.015
              Copyright(C) 2012 D-Link Corporation. All rights reserved.

UserName:
```

There is no initial username or password. Just press the **Enter** key twice to display the CLI input cursor – **DGS-3620-28SC: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                                          V1.00.016
-------------------------------------------------------------------------------


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

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

  Please Wait, Loading V2.00.015 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 Device 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-3620-28SC: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-3620-28SC: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-3620-28SC: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 bgp
clear bgp dampening
clear bgp flap_statistics
clear cfm pkt_cnt
clear counters
clear dhcp binding
clear dhcp conflict_ip
clear dhcpv6 binding
clear ethernet_oam ports
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-3620-28SC:admin#config account
Command: config account
Next possible completions:
<username>

DGS-3620-28SC: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-3620-28SC:admin# config account
Command: config account
Next possible completions:
<username>

DGS-3620-28SC: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-3620-28SC:admin#the
Available commands:
..                  ?                   cable_diag          cd
cfm                 change              clear               config
copy                create              debug               del
delete              dir                 disable             download
enable              erase               format              login
logout              md                  move                no
ping                ping6               rd                  reboot
reconfig            rename              reset               save
show                telnet              traceroute          traceroute6
upload

DGS-3620-28SC: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-3620-28SC:admin#show
```

```
Command: show

Next possible completions:
802.1p              802.1x              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   bgp
boot_file           bpdu_protection     broadcast_ping_reply
cfm                 command             command_history
community_encryption                    config              cpu
current_config      ddm                 device_status       dhcp
dhcp_local_relay    dhcp_relay          dhcp_server         dhcpv6
dhcpv6_relay        dhcpv6_server       dnsr
dot1v_protocol_group                    dscp                duld
dvmrp               ecmp                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
ip                  ip_tunnel           ipfdb               ipif
ipif_ipv6_link_local_auto               ipmc                ipmroute
iproute             ipv6                ipv6route           jumbo_frame
jwac                l2protocol_tunnel   lacp_port
limited_multicast_addr                  link_aggregation    lldp
lldp_med            log                 log_save_timing
log_software_module                     loopback            loopdetect
mac_based_access_control                mac_based_access_control_local
mac_based_vlan      mac_notification    max_mcast_group
mcast_filter_profile                    md5                 mirror
mld                 mld_proxy           mld_snooping        multicast
multicast_fdb       name_server         nlb                 ospf
ospfv3              out_band_ipif       packet              password_recovery
per_queue           pim                 pim-ssm             pim6
policy_route        port                port_group          port_security
port_security_entry                     port_vlan           ports
power_saving        private_vlan        ptp                 pvid
qinq                radius              rcp                 rip
ripng               rmon                route               route_map
router_ports        rspan               safeguard_engine    scheduling
scheduling_mechanism                    serial_port         session
sflow               sim                 snmp                sntp
ssh                 ssl                 stack_device        stack_information
stacking_mode       storage_media_info                      stp
sub_vlan            subnet_vlan         super_vlan          switch
syslog              system_severity     tech_support        terminal
time                time_range          traffic
traffic_segmentation                    trap                trusted_host
utilization         vlan                vlan_precedence     vlan_translation
vlan_trunk          voice_vlan          vrrp                wac
```

```

DGS-3620-28SC: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

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

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

| Syntax | Description |
|---|---|
| angle brackets < > | Encloses a variable or value. Users must specify the variable or value. For example, in the syntax<br>**create ipif <ipif_name 12> {<network_address>} <vlan_name 32> {secondary \| state [enable \| disable] \| proxy_arp [enable \| disable] {local [enable \| disable]}}**<br>users must supply an IP interface name for **<ipif_name 12>** and a VLAN name for **<vlan_name 32>** 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 syntax<br>**create account [admin \| operator \| power_user \| user] <username 15> {encrypt [plain_text \| sha_1] <password>}**<br>users must specify either the admin-, operator-, 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. For example, in the syntax<br>**reset {[config \|system]} {force_agree}**<br>users may choose config or system 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 syntax<br>**reset {[config \| system]} {force_agree}**<br>users may choose config or 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 syntax<br>**config dhcp_relay {hops <int 1-16> \| time <sec 0-65535>}(1)**<br>users have the option to specify hops or time or both of them. The "(1)" |

| | |
|---|---|
| | following the set of braces indicates at least one argument or value within the braces must be specified. DO NOT TYPE THE PARENTHESES. |
| ipif <ipif_name 12><br>metric <value 1-31> | **12** means the maximum length of the IP interface name.<br>**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. |
| CTRL+R | Toggle on and off. When toggled on, inserts text and shifts previous text to right. |
| Up Arrow | Repeats the previously entered command. Each time the up arrow is pressed, the command previous to that displayed appears. This way it is possible to review the command history for the current session. Use the down arrow to progress sequentially forward through the command history list. |
| Down Arrow | The down arrow will display the next command in the command history entered in the current session. This displays each command sequentially as it was entered. Use the up arrow to review previous commands. |
| Left Arrow | Move cursor to left. |
| Right Arrow | Move cursor to right |
| Tab | Help user to select appropriate token. |

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

## 1-5 Multiple Page Display Control Keys

| Keys | Description |
|---|---|
| Space | Displays the next page. |
| CTRL+C | Stops the display of remaining pages when multiple pages are to be displayed. |
| ESC | Stops the display of remaining pages when multiple pages are to be displayed. |
| n | Displays the next page. |
| p | Displays the previous page. |
| q | Stops the display of remaining pages when multiple pages are to be displayed. |
| r | Refreshes the pages currently displayed. |
| a | Displays the remaining pages without pausing between pages. |

| | |
|---|---|
| Enter | Displays the next line or table entry. |

# Chapter 2 Basic Management Commands

**create account** [admin | operator | power_user | user] <username 15> {encrypt [plain_text | sha_1] <password>}

**enable password encryption**

**disable password encryption**

**config account** <username> {encrypt [plain_text | sha_1] <password>}

**show account**

**delete account** <username>

**show session**

**show switch**

**show environment**

**config temperature** [trap | log] state [enable | disable]

**config temperature threshold** {high <temperature -500-500> | low <temperature -500-500>}(1)

**show serial_port**

**config serial_port** {baud_rate [9600 | 19200 | 38400 | 115200] | auto_logout [never | 2_minutes | 5_minutes | 10_minutes | 15_minutes]}(1)

**enable clipaging**

**disable clipaging**

**enable telnet** {<tcp_port_number 1-65535>}

**disable telnet**

**enable web** {<tcp_port_number 1-65535>}

**disable web**

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

**reboot** {force_agree}

**reset** {[config | system]} {force_agree}

**login**

**logout**

**clear**

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

**show terminal width**

**show device_status**

## 2-1 create account

### Description

This command creates user accounts. The username is between 1 and 15 characters, the password is between 0 and 15 characters. The number of accounts (including admin, operator, and user) is up to eight.

### 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 of the operator account.

**power_user** - Specify a power user level account. The power user level is lower than the operator level and higher than the user level.

**user** - Specify the name of the user account.

**<username 15>** - Specify a username of up to 15 characters.

**encrypt** - Specifies the encryption used.

- **plain_text** - Specify the password in plain text form.
- **sha_1** - Specify the password in SHA-1 encrypted form.
- **<password>** - The password for the user account. The length of a password in plain-text form and encrypted form are different. For a plain-text form password, the password must be a minimum of 0 characters and a maximum of 15 characters. For an encrypted form password, the length is fixed to 35 bytes long. The password is case-sensitive.

## Restrictions

Only Administrator-level users can issue this command.

## Example

To create the Administrator-level user “dlink”:

```
DGS-3620-28SC: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-3620-28SC:admin#
```

To create the Operator-level user “Sales”:

```
DGS-3620-28SC:admin##create account operator Sales
Command: create account operator Sales

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

DGS-3620-28SC:admin#
```

To create the User-level user “System”:

```
DGS-3620-28SC:admin##create account user System
Command: create account user System

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

DGS-3620-28SC:admin#
```

## 2-2 enable password encryption

### Description

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 when it is stored in the configuration file. When password encryption is disabled, the password will be in plain text form when it is stored in the configuration file. However, if the created user account directly uses the encrypted password, the password will still be in the encrypted form.

### Format

**enable password encryption**

### Parameters

None.

### Restrictions

Only Administrator-level users can issue this command.

### Example

To enable password encryption:

```
DGS-3620-28SC:admin#enable password encryption
Command: enable password encryption

Success.

DGS-3620-28SC:admin#
```

## 2-3 disable password encryption

### Description

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 when it is stored in the configuration file. When password encryption is disabled, the password will be in plain text form when it is stored in the configuration file. However, if the created user account directly uses the encrypted password, the password will still be in the encrypted form.

### Format

**disable password encryption**

### Parameters

None.

### Restrictions

Only Administrator-level users can issue this command.

### Example

To disable password encryption:

```
DGS-3620-28SC:admin#disable password encryption
Command: disable password encryption

Success.

DGS-3620-28SC:admin#
```

## 2-4 config account

### Description

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

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

### Format

**config account <username> {encrypt [plain_text | sha_1] <password>}**

### Parameters

**<username>** - Specify the name of the account. The account must already be defined.

**encrypt** - (Optional) Specify the encryption type, plain_text or sha_1.
- **plain_text** - Specify the password in plain text form. For the plain text form, passwords must have a minimum of 0 and a maximum of 15 characters. The password is case-sensitive
- **sha_1** - Specify the password in the SHA-1 encrypted form. For the encrypted form password, the length is fixed to 35 bytes long. The password is case-sensitive.

**<password>** - Specify the password.

### Restrictions

Only Administrator-level users can issue this command.

### Example

To configure the user password of the “dlink” account:

```
DGS-3620-28SC: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-3620-28SC:admin#
```

To configure the user password of the “administrator” account:

```
DGS-3620-28SC:admin#config account administrator encrypt sha_1
*@&NWoZK3kTsExUV00Ywo1G5jlUKKv+toYg
Command: config account administrator encrypt sha_1
*@&NWoZK3kTsExUV00Ywo1G5jlUKKv+toYg
Success.

DGS-3620-28SC:admin#
```

## 2-5 show account

### Description

This command is used to display user accounts that have been created.

### Format

**show account**

### Parameters

None.

### Restrictions

Only Administrator-level users can issue this command.

### Example

To display accounts that have been created:

```
DGS-3620-28SC:admin#show account
Command: show account

Current Accounts:
Username         Access Level
---------------  ------------
System           User
Sales            Operator
dlink            Admin

DGS-3620-28SC:admin#
```

## 2-6 delete account

### Description

This command is used to delete an existing account.

### Format

**delete account <username>**

### Parameters

**<username>** - Specify the name of the user who will be deleted.

### Restrictions

Only Administrator-level users can issue this command. One active admin user must exist.

### Example

To delete the user account “System”:

```
DGS-3620-28SC:admin#delete account System
Command: delete account System

Success.

DGS-3620-28SC:admin#
```

## 2-7 show session

### Description

This command is used to display a list of current users which are logged in to CLI sessions.

### Format

**show session**

### Parameters

None.

### Restrictions

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

### Example

To display accounts a list of currently logged-in users:

```
DGS-3620-28SC:admin#show session
Command: show session

ID  Live Time     From          Level   User
--  ------------  ------------  -----   --------------------
8   23:37:42.270  Serial Port   admin   Anonymous
```

```

Total Entries: 1

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

## 2-8 show switch

### Description

This command is used to display the switch information.

### Format

**show switch**

### Parameters

None.

### Restrictions

None.

### Example

To display the switch information:

```
DGS-3620-28SC:admin#show switch
Command: show switch

Device Type                : DGS-3620-28SC 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 1.00.016
Firmware Version           : Build 2.00.015
Hardware Version           : A1
Firmware Type              : EI
Serial Number              : D1234567890
System Name                :
System Location            :
System Uptime              : 0 days, 0 hours, 38 minutes, 12 seconds
System Contact             :
Spanning Tree              : Disabled
GVRP                       : Disabled
IGMP Snooping              : Disabled
MLD Snooping               : Disabled
RIP                        : Disabled
RIPng                      : Disabled
DVMRP                      : Disabled
```

```
PIM                        : Disabled
PIM6                       : Disabled
OSPF                       : Disabled
OSPFv3                     : Disabled
BGP                        : Disabled
VLAN Trunk                 : Disabled
Telnet                     : Enabled (TCP 23)
Web                        : Enabled (TCP 80)
SNMP                       : Disabled
SSL Status                 : Disabled
SSH Status                 : Disabled
802.1X                     : Disabled
Jumbo Frame                : Off
CLI Paging                 : Enabled
MAC Notification           : Disabled
Port Mirror                : Disabled
SNTP                       : Disabled
DHCP Relay                 : Disabled
DNSR Status                : Disabled
VRRP                       : Disabled
HOL Prevention State       : Enabled
Syslog Global State        : Disabled
Single IP Management       : Disabled
Password Encryption Status : Disabled
DNS Resolver               : Disabled

DGS-3620-28SC:admin#
```

## 2-9 show environment

### Description

This command is used to display the device’s internal and external power and internal temperature status.

### Format

**show environment**

### Parameters

None.

### Restrictions

None.

### Example

To display the switch hardware status:

```
DGS-3620-28SC:admin#show environment
```

```
Command: show environment

Internal Power      : Active
External Power      : Fail
Current Temperature(Celsius) :   56
High Warning Temperature Threshold(Celsius) :    79
Low Warning Temperature Threshold(Celsius)  :    11

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

## 2-10 config temperature

### Description

This command is used to configure the warning trap or log state of the system internal temperature.

### Format

**config temperature [trap | log] state [enable | disable]**

### Parameters

**trap** - Specify to configure the warning temperature trap.

**log** - Specify to configure the warning temperature log.

**state** - Enable or disable either the trap or log state for a warning temperature event. The default is enable.
**enable** - Enable either the trap or log state for a warning temperature event.
**disable** - Disable either the trap or log state for a warning temperature event.

### Restrictions

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

### Example

To enable the warning temperature trap state:

```
DGS-3620-28SC:admin#config temperature trap state enable
Command: config temperature trap state enable

Success.

DGS-3620-28SC:admin#
```

To enable the warning temperature log state:

```
DGS-3620-28SC:admin#config temperature log state enable
Command: config temperature log state enable

Success.

DGS-3620-28SC:admin#
```

## 2-11 config temperature threshold

### Description

This command is used to configure the warning temperature high threshold or low threshold. When temperature is above the high threshold or below the low threshold, SW will send alarm traps or keep the logs.

### Format

**config temperature threshold {high <temperature -500-500> | low <temperature -500-500>}(1)**

### Parameters

**high** - Specify the high threshold value. The high threshold must bigger than the low threshold.
**<temperature -500-500>** - Specify the high threshold value. This value must be between -500 and 500.

**low** - Specify the low threshold value.
**<temperature -500-500>** - Specify the low threshold value. This value must be between -500 and 500.

### Restrictions

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

### Example

To configure a warming temperature threshold high of 80:

```
DGS-3620-28SC:admin#config temperature threshold high 80
Command: config temperature threshold high 80

Success.

DGS-3620-28SC:admin#
```

## 2-12 show serial_port

### Description

This command is used to display the current console port setting.

### Format

**show serial_port**

### Parameters

None.

### Restrictions

None.

### Example

To display the console port setting:

```
DGS-3620-28SC:admin#show serial_port
Command: show serial_port

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

DGS-3620-28SC:admin#
```

## 2-13 config serial_port

### Description

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

### Format

**config serial_port {baud_rate [9600 | 19200 | 38400 | 115200] | auto_logout [never | 2_minutes | 5_minutes | 10_minutes | 15_minutes]}(1)**

### Parameters

**baud_rate** - Specify the baud rate value. The default baud rate is 115200.
- **9600** - Specify a baud rate of 9600.
- **19200** - Specify a baud rate of 19200.
- **38400** - Specify a baud rate of 38400.
- **115200** - Specify a baud rate of 115200.

**auto_logout** - Specify the timeout value. The default timeout is 10_minutes.
- **never** - Specify to never timeout.
- **2_minutes** - Specify when the idle value is over 2 minutes, the device will auto logout.
- **5_minutes** - Specify when the idle value over 5 minutes, the device will auto logout.
- **10_minutes** - Specify when the idle value is over 10 minutes, the device will auto logout.
- **15_minutes** - Specify when the idle value is over 15 minutes, the device will auto logout.

### Restrictions

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

### Example

To configure the baud rate:

```
DGS-3620-28SC:admin# config serial_port baud_rate 9600
```

```
Command: config serial_port baud_rate 9600

Success.

DGS-3620-28SC:admin#
```

## 2-14 enable clipaging

### Description

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

### Format

**enable clipaging**

### Parameters

None.

### Restrictions

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

### Example

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

```
DGS-3620-28SC:admin#enable clipaging
Command: enable clipaging

Success.

DGS-3620-28SC:admin#
```

## 2-15 disable clipaging

### Description

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

### Format

**disable clipaging**

### Parameters

None.

### Restrictions

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

### Example

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

```
DGS-3620-28SC:admin#disable clipaging
Command: disable clipaging

Success.

DGS-3620-28SC:admin#
```

## 2-16 enable telnet

### Description

This command is used to enable Telnet and configure a port number. The default setting is enabled and the port number is 23.

### Format

**enable telnet {<tcp_port_number 1-65535>}**

### Parameters

**<tcp_port_number 1-65535>** - (Optional) Specify 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 Administrator and Operator-level users can issue this command.

### Example

To enable Telnet and configure a port number:

```
DGS-3620-28SC:admin#enable telnet 23
Command: enable telnet 23

Success.

DGS-3620-28SC:admin#
```

## 2-17 disable telnet

### Description

This command is used to disable Telnet.

### Format

**disable telnet**

### Parameters

None.

### Restrictions

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

### Example

To disable Telnet:

```
DGS-3620-28SC:admin#disable telnet
Command: disable telnet

Success.

DGS-3620-28SC:admin#
```

## 2-18 enable web

### Description

This command is used to enable Web UI and configure the port number. The default setting is enabled and the port number is 80.

### Format

**enable web {<tcp_port_number 1-65535>}**

### Parameters

**<tcp_port_number 1-65535>** - (Optional) Specify the TCP port number. TCP ports are numbered between 1 and 65535. The "well-know" TCP port for the Web protocol is 80.

### Restrictions

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

### Example

To enable HTTP and configure port number:

```
DGS-3620-28SC:admin#enable web 80
Command: enable web 80

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

```

DGS-3620-28SC:admin#
```

## 2-19 disable web

### Description

This command is used to disable Web UI.

### Format

**disable web**

### Parameters

None.

### Restrictions

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

### Example

To disable HTTP:

```
DGS-3620-28SC:admin#disable web
Command: disable web

Success.

DGS-3620-28SC:admin#
```

## 2-20 save

### Description

This command is used to save the current configuration or log in non-volatile RAM.

### Format

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

### Parameters

**config** - (Optional) Specify to save configuration.
**<pathname>** - Specify the path name of the indicated configuration

**log** - (Optional) Specify to save log.

**all** - (Optional) Specify to save changes to currently active configuration and save logs.

**Note:** If no keyword is specified, all changes will be saved to bootup configuration file.

### Restrictions

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

### Example

To save the current configuration to the bootup configuration file:

```
DGS-3620-28SC:admin#save
Command: save

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

DGS-3620-28SC:admin#
```

To save the current configuration to destination file, named 1:

```
DGS-3620-28SC:admin#save config 1
Command: save config 1

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

DGS-3620-28SC:admin#
```

To save a log to NV-RAM:

```
DGS-3620-28SC:admin#save log
Command: save log

Saving all system logs to NV-RAM............. Done.

DGS-3620-28SC:admin#
```

To save all the configurations and logs to NV-RAM:

```
DGS-3620-28SC:admin#save all
Command: save all

Saving  configuration and logs to NV-RAM...... Done.

DGS-3620-28SC:admin#
```

## 2-21 reboot

### Description

This command is used to restart the switch.

### Format

**reboot {force_agree}**

### Parameters

**force_agree** – (Optional) Specify to immediately execute the reboot command without further confirmation.

### Restrictions

Only Administrator-level users can issue this command.

### Example

To restart the switch:

```
DGS-3620-28SC:admin#reboot
Command: reboot

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

## 2-22 reset

### Description

This command is used to reset all switch parameters to the factory defaults.

### Format

**reset {[config | system]} {force_agree}**

### Parameters

**config** - (Optional) Specify this keyword and all parameters are reset to default settings. However, the device will neither save nor reboot.

**system** - (Optional) Specify this keyword and all parameters are reset to default settings. Then the switch will do factory reset, save, and reboot.

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

✎ **Note:** If no keyword is specified, all parameters will be reset to default settings except IP address, user account, and history log, but the device will neither save nor reboot.

### Restrictions

Only Administrator-level users can issue this command.

### Example

To reset all the switch parameters except the IP address:

```
DGS-3620-28SC:admin#reset
Command: reset

```

```
Are you sure to proceed with system reset except IP address?(y/n)
Success.

DGS-3620-28SC:admin#
```

To reset the system configuration settings:

```
DGS-3620-28SC:admin#reset config
Command: reset config

Are you sure to proceed with system reset?(y/n)
Success.

DGS-3620-28SC:admin#
```

To reset all system parameters, save, and restart the switch:

```
DGS-3620-28SC:admin#reset system
Command: reset system

Are you sure to proceed with system reset, save and reboot?(y/n)
Loading factory default configuration… Done.
Saving all configuration to NV-RAM… Done.
Please wait, the switch is rebooting…
```

## 2-23 login

### Description

This command is used to log in to the switch.

### Format

**login**

### Parameters

None.

### Restrictions

None.

### Example

To login to the switch:

```
DGS-3620-28SC:admin#login
Command: login

UserName:
```

## 2-24 logout

### Description

This command is used to log out of the switch.

### Format

**logout**

### Parameters

None.

### Restrictions

None.

### Example

To logout of the switch:

```
DGS-3620-28SC:admin#logout
Command: logout

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



                      DGS-3620-28SC Gigabit Ethernet Switch
                             Command Line Interface

                            Firmware: Build 2.00.015
           Copyright(C) 2012 D-Link Corporation. All rights reserved.

UserName:

```

## 2-25 clear

### Description

This command is used to clear the terminal screen.

### Format

**clear**

### Parameters

None.

### Restrictions

None.

### Example

To clear the terminal screan:

```
DGS-3620-28SC:admin#clear
Command: clear
```

## 2-26 config terminal width

### Description

This command is used to configure the terminal width.

### Format

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

### Parameters

**default** - Specify the default terminal width value.

**<value 80-200>** - Specify a terminal width value between 80 and 200 characters. The default value is 80.

### Restrictions

None.

### Example

To configure the terminal width:

```
DGS-3620-28SC:admin#config terminal width 90
Command: config terminal width 90

Success.

DGS-3620-28SC:admin#
```

## 2-27 show terminal width

### Description

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

### Format

**show terminal width**

### Parameters

None.

### Restrictions

None.

### Example

To display the configuration of the current terminal width:

```
DGS-3620-28SC:admin#show terminal width
Command: show terminal width

Global terminal width     : 80
Current terminal width    : 80

DGS-3620-28SC:admin#
```

## 2-28 show device_status

### Description

This command displays 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, the number 1, 2, 3 etc represent the fan number:

```
DGS-3620-28SC:admin# show device_status
Command: show device_status

Unit 1:
    Internal Power: Active
    External Power: Fail
    Left Fan      : 1, 3 Fail
    Right Fan     : 2 Fail
    Back Fan      : OK
    CPU Fan       : Fail

Unit 2:
    Internal Power: Active
    External Power: Fail
    Left Fan      : 1 Fail
    Right Fan     : OK
    Back Fan      : 2, 4 Fail
    CPU Fan       : OK

DGS-3620-28SC:admin#
```

# Chapter 3 802.1X Commands

**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]

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

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

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

**config 802.1x fwd_pdu system** [enable | disable]

**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 authorization attributes radius** [enable | disable]

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

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

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

**create 802.1x guest_vlan** <vlan_name 32>

**delete 802.1x guest_vlan** <vlan_name 32>

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

**show 802.1x guest_vlan**

**config radius add** <server_index 1-3> [<server_ip> | <ipv6addr>] key <password 32> [default | {auth_port <udp_port_number 1-65535> | acct_port <udp_port_number 1-65535> | timeout <sec 1-255> | retransmit <int 1-20>}(1)]

**config radius delete** <server_index 1-3>

**config radius** <server_index 1-3> {ipaddress [<server_ip> | <ipv6addr>] | key <password 32> | auth_port [<udp_port_number 1-65535> | default] | acct_port [<udp_port_number 1-65535> | default] | timeout [<sec 1-255> | default] | retransmit [<int 1-20> | default]}(1)

**show radius**

**show auth_statistics** {ports <portlist>}

**show auth_diagnostics** {ports <portlist>}

**show auth_session_statistics** {ports <portlist>}

**show auth_client**

**show acct_client**

**config accounting service** [network | shell | system] state [enable | disable]

**show accounting service**

## 3-1 enable 802.1x

### Description

This command is used to enable the 802.1X function.

### Format

**enable 802.1x**

### Parameters

None.

### Restrictions

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

### Example

To enable the 802.1X function:

```
DGS-3620-28SC:admin#enable 802.1x
Command: enable 802.1x

Success.

DGS-3620-28SC:admin#
```

## 3-2 disable 802.1x

### Description

This command is used to disable the 802.1X function.

### Format

**disable 802.1x**

### Parameters

None.

### Restrictions

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

### Example

To disable the 802.1Xfunction:

```
DGS-3620-28SC:admin#disable 802.1x
Command: disable 802.1x

Success.

DGS-3620-28SC:admin#
```

## 3-3 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>** - Specify to add a user name.

### Restrictions

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

### Example

To create a user named “ctsnow”:

```
DGS-3620-28SC:admin#create 802.1x user ctsnow
Command: create 802.1x user ctsnow

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

Success.

DGS-3620-28SC:admin#
```

## 3-4 delete 802.1x user

### Description

This command is used to delete a specified user.

### Format

**delete 802.1x user <username 15>**

### Parameters

**<username 15>** - Specify to delete a user name.

### Restrictions

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

### Example

To delete the user named “Tiberius”:

```
DGS-3620-28SC:admin#delete 802.1x user Tiberius
Command: delete 802.1x user Tiberius

Success.

DGS-3620-28SC:admin#
```

## 3-5 show 802.1x user

### Description

This command is used to display 802.1X local user account information.

### Format

**show 802.1x user**

### Parameters

None.

### Restrictions

None.

### Example

To display 802.1X user information:

```
DGS-3620-28SC:admin#show 802.1x user
Command: show 802.1x user

Current Accounts:
Username         Password
---------------  ------------
ctsnow           gallinari

Total Entries : 1

DGS-3620-28SC:admin#
```

## 3-6 config 802.1x auth_protocol

### Description

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

### Format

**config 802.1x auth_protocol [local | radius_eap]**

### Parameters

**local** - Specifiy the authentication protocol as local.

**radius_eap** - Specify the authentication protocol as RADIUS EAP.

### Restrictions

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

### Example

To configure the 802.1X RADIUS EAP:

```
DGS-3620-28SC:admin#config 802.1x auth_protocol radius_eap
Command: config 802.1x auth_protocol radius_eap

Success.

DGS-3620-28SC:admin#
```

## 3-7 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 the 802.1X authentication state of some or all ports.

**auth_configuration** - (Optional) Specify to display 802.1X configuration of some or all ports.

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

### Restrictions

None.

### Example

To display 802.1X information:

```
DGS-3620-28SC:admin#show 802.1x
Command: show 802.1x

802.1X                  : Disabled
```

```
Authentication Protocol : RADIUS_EAP
Forward EAPOL PDU       : Disabled
Max User                : 448
RADIUS Authorization    : Enabled

DGS-3620-28SC:admin#
```

To display the 802.1x state for ports 1 to 5:

```
DGS-3620-28SC:admin# show 802.1x auth_state ports 1-4
Command: show 802.1x auth_state ports 1-4

Status:  A – Authorized; U – Unauthorized; (P): Port-Based 802.1X Pri: Priority
Port  MAC Address          Auth    PAE State      Backend    Status VID   Pri
                           VID                    State
----- -------------------- ------- -------------- ---------- ------ ----- -----
1     00-00-00-00-00-01    10      Authenticated  Idle       A      4004  3
1     00-00-00-00-00-02    10      Authenticated  Idle       A      1234  -
1     00-00-00-00-00-04    30      Authenticating Response   U       -    -
2     -                    (P)  -  Authenticating Request    U       -    -
3     -                    (P)  -  Connecting     Idle       U       -    -
4     -                    (P)  -  Held           Fail       U       -    -

Total Authenticating Hosts: 3
Total Authenticated Hosts : 2

DGS-3620-28SC:admin#
```

To display the 802.1x configuration for port 1:

```
DGS-3620-28SC:admin# show 802.1x auth_configuration ports 1:1
Command: show 802.1x auth_configuration ports 1:1

Port number                       : 1:1
Capability                        : None
AdminCrlDir                       : Both
OpenCrlDir                        : Both
Port Control                      : Auto
QuietPeriod                       : 60 Seconds
TxPeriod                          : 30 Seconds
SuppTimeout                       : 30 Seconds
ServerTimeout                     : 30 Seconds
MaxReq                            : 2 Times
ReAuthPeriod                      : 3600 Seconds
ReAuthenticate                    : Disabled
Forward EAPOL PDU On Port         : Enabled
Max User On Port                  : 10

DGS-3620-28SC:admin#
```

## 3-8 config 802.1x capability ports

### Description

This command is used to configure port capability.

### Format

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

### Parameters

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

**all** - Specify to configure all ports.

**authenticator** - The port that wishes to enforce authentication before allowing access to services that are accessible via that port adopts the authenticator role.

**none** – Disable authentication on specified port.

### Restrictions

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

### Example

To configure port capability for ports 1 to 10:

```
DGS-3620-28SC:admin#config 802.1x capability ports 1-10 authenticator
Command: config 802.1x capability ports 1-10 authenticator

Success.

DGS-3620-28SC:admin#
```

## 3-9 config 802.1x fwd_pdu ports

### Description

This command is used to configure the 802.1X PDU forwarding state on specific ports of the switch.

### Format

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

### Parameters

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

**all** - Specify all ports.

**enable** - Enable the 802.1X PDU forwarding state.

**disable** - Disable the 802.1X PDU forwarding state.

### Restrictions

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

### Example

To configure the 802.1X PDU forwarding state on ports 1 to 2:

```
DGS-3620-28SC:admin#config 802.1x fwd_pdu ports 1-2 enable
Command: config 802.1x fwd_pdu ports 1-2 enable

Success.

DGS-3620-28SC:admin#
```

## 3-10 config 802.1x fwd_pdu system

### Description

This command is used to configure the 802.1X PDU forwarding state.

### Format

**config 802.1x fwd_pdu system [enable | disable]**

### Parameters

**enable** - Enable the 802.1X PDU forwarding state.

**disable** - Disable the 802.1X PDU forwarding state.

### Restrictions

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

### Example

To configure the 802.1X PDU forwarding state:

```
DGS-3620-28SC:admin#config 802.1x fwd_pdu system enable
Command: config 802.1x fwd_pdu system enable

Success.

DGS-3620-28SC:admin#
```

## 3-11 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>** - Specify a range of ports to be configured. |
| **all** - Specify to configure all ports. |
| **default** - Set all parameters to the default value. |
| **direction** - (Optional) Set the direction of access control.<br>**both** - For bidirectional access control.<br>**in** - For ingress access control. |
| **port_control** - (Optional) Force a specific port to be unconditionally authorized or unauthorized by setting the parameter of port_control to be force_authorized or force_unauthorized. Besides, the controlled port will reflect the outcome of authentication if port_control is auto.<br>**force_auth** - The port transmits and receives normal traffic without 802.1X-based authentication of the client.<br>**auto** - The port begins in the unauthorized state, and relays authentication messages between the client and the authentication server.<br>**force_unauth** - The port will remain in the unauthorized state, ignoring all attempts by the client to authenticate. |
| **quiet_period** - (Optional) The initialization value of the quietWhile timer. The default value is 60 s and can be any value from 0 to 65535.<br>**<sec 0-65535>** - The quiet period value must be between 0 an 65535 seconds. |
| **tx_period** - (Optional) The initialization value of the txWhen timer. The default value is 30 s and can be any value from 1 to 65535.<br>**<sec 1-65535>** - The transmit period value must be between 1 an 65535 seconds. |
| **supp_timeout** - (Optional) The initialization value of the aWhile timer when timing out the supplicant. Its default value is 30 s and can be any value from 1 to 65535.<br>**<sec 1-65535>** - The timeout value must be between 1 an 65535 seconds. |
| **server_timeout** - (Optional) The initialization value of the aWhile timer when timing out the authentication server. Its default value is 30 and can be any value from 1 to 65535.<br>**<sec 1-65535>** - The server timeout value must be between 1 an 65535 seconds. |
| **max_req** - (Optional) The maximum number of times that the authenitcation PAE state machine will retransmit an EAP Request packet to the supplicant. Its default value is 2 and can be any number from 1 to 10.<br>**<value 1-10>** - The maximum require number must be between 1 and 10. |
| **reauth_period** - (Optional) It's a non-zero number of seconds, which is used to be the re-authentication timer. The default value is 3600.<br>**<sec 1-65535>** - The reauthentication period value must be between 1 an 65535 seconds. |
| **max_users** - (Optional) Set the maximum number of users between 1 and 448.<br>**<value 1-448>** - The maximum users value must be between 1 and 448.<br>**no_limit** - Set an unlimited number of users. |
| **enable_reauth** - (Optional) Enable or disable the re-authentication mechanism for a specific port.<br>**enable** - Enable the re-authentication mechanism for a specific port.<br>**disable** - Disable the re-authentication mechanism for a specific port. |

### Restrictions

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

### Example

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

```
DGS-3620-28SC:admin# config 802.1x auth_parameter ports 1-20 direction both
Command: config 802.1x auth_parameter ports 1-20 direction both

Success.

DGS-3620-28SC:admin#
```

## 3-12 config 802.1x authorization attributes radius

### Description

This command is used to enable or disable the acceptation of an authorized configuration. (To configure that attributes, regarding VLAN, 802.1p, ACL and Ingress/Egress Bandwidth, please refer to the Appendix section at the end of this document.)

### Format

**config 802.1x authorization attributes radius [enable | disable]**

### Parameters

**enable** - The authorization attributes such as 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.

**disable** - The authorization attributes assigned by the RADUIS server will not be accepted.

### Restrictions

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

### Example

To configure the 802.1X state of acceptation of an authorized configuration:

```
DGS-3620-28SC:admin#config 802.1x authorization attributes radius enable
Command: config 802.1x authorization attributes radius enable

Success.

DGS-3620-28SC:admin#
```

## 3-13 config 802.1x init

### Description

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

### Format

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

### Parameters

**port_based ports** - Used to configure authentication in port-based mode.
- **<portlist>** - Specify a range of ports to be configured.
- **all** - Specify to configure all ports.

**mac_based ports** - To configure authentication in host-based 802.1X mode.
- **<portlist>** - Specify a range of ports to be configured.
- **all** - Specify to configure all ports.

**mac_address** - (Optional) Specify the MAC address of the host.
- **<macaddr>** - Enter the MAC address here.

### Restrictions

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

### Example

To initialize the authentication state machine of some or all:

```
DGS-3620-28SC:admin# config 802.1x init port_based ports all
Command: config 802.1x init port_based ports all

Success.

DGS-3620-28SC:admin#
```

## 3-14 config 802.1x max_users

### Description

This command is used to configure the 802.1X maximum number of users of the system.

### Format

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

### Parameters

**<value 1-448>** - Specify the maximum number of users.

**no_limit** - Specify an unlimited number of users.

### Restrictions

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

### Example

To configure the 820.1X maximum numbers of the system:

```
DGS-3620-28SC:admin# config 802.1x max_users 2
Command: config 802.1x max_users 2

Success.

DGS-3620-28SC:admin#
```

## 3-15 config 802.1x reauth

### Description

This command is used to reauthenticate the device connected with the port. During the reauthentication period, the port status remains authorized until failed reauthentication.

### Format

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

### Parameters

**port_based ports** - The switch passes data based on its authenticated port.
- **<portlist>** - Specify a range of ports to be configured.
- **all** - Specify to configure all ports.

**mac_based ports** - The switch passes data based on the MAC address of authenticated RADIUS client.
- **<portlist>** - Specify a range of ports to be configured.
- **all** - Specify to configure all ports.

**mac_address** - (Optional) Specify the MAC address of the authenticated RADIUS client.
- **<macaddr>** - Enter the MAC address here.

### Restrictions

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

### Example

To reauthenticate the device connected with the port:

```
DGS-3620-28SC:admin# config 802.1x reauth port_based ports all
Command: config 802.1x reauth port_based ports all

Success.

DGS-3620-28SC:admin#
```

## 3-16 create 802.1x guest_vlan

### Description

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

### Format

**create 802.1x guest_vlan <vlan_name 32>**

### Parameters

**<vlan_name 32>** - Specify the static VLAN to be a guest VLAN.

### Restrictions

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

### Example

To assign a static VLAN to be a guest VLAN:

```
DGS-3620-28SC:admin# create 802.1x guest_vlan guestVLAN
Command: create 802.1x guest_vlan guestVLAN

Success.

DGS-3620-28SC:admin#
```

## 3-17 delete 802.1x guest_vlan

### Description

This command is used to delete a guest VLAN setting, but not to delete the static VLAN itself.

### Format

**delete 802.1x guest_vlan <vlan_name 32>**

### Parameters

**<vlan_name 32>** - Specify the guest VLAN name.

### Restrictions

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

### Example

To delete a guest VLAN configuration:

```
DGS-3620-28SC:admin# delete 802.1x guest_vlan guestVLAN
Command: delete 802.1x guest_vlan guestVLAN

Success.

DGS-3620-28SC:admin#
```

## 3-18 config 802.1x guest_vlan ports

### Description

This command is used to configure a guest VLAN setting.

### Format

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

### Parameters

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

**all** - Specify to configure all ports.

**state** - Specify the guest VLAN port state of the configured ports.
- **enable** - Join the guest VLAN.
- **disable** - Remove from guest VLAN.

### Restrictions

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

### Example

To configure a guest VLAN setting for ports 1 to 8:

```
DGS-3620-28SC:admin# config 802.1x guest_vlan ports 1-8 state enable
Command: config 802.1x guest_vlan ports 1-8 state enable

Warning, The ports are moved to Guest VLAN.

Success.

DGS-3620-28SC:admin#
```

## 3-19 show 802.1x guest_vlan

### Description

This command is used to display guest VLAN information.

### Format

**show 802.1x guest_vlan**

### Parameters

None.

### Restrictions

None.

### Example

To display guest VLAN information:

```
DGS-3620-28SC:admin#show 802.1x guest_vlan
Command: show 802.1x guest_vlan

Guest Vlan Setting
-----------------------------------------------------------
Guest vlan : guest
Enable guest vlan ports : 1-10

DGS-3620-28SC:admin#
```

## 3-20 config radius add

### Description

This command is used to add a new RADIUS server. The server with a lower index has higher authenticative priority.

### Format

**config radius add <server_index 1-3> [<server_ip> | <ipv6addr>] key <password 32> [default | {auth_port <udp_port_number 1-65535> | acct_port <udp_port_number 1-65535> | timeout <sec 1-255> | retransmit <int 1-20>}(1)]**

### Parameters

| |
|---|
| **<server_index 1-3>** - Specify the RADIUS server index. |
| **<server_ip>** - Specify the IP address of the RADIUS server.<br>**<ipv6add>** - Specifies the IPv6 address used. |
| **key** - Specify the key pre-negotiated between switch and the RADIUS server. It is used to encrypt user's authentication data before being transmitted over the Internet. The maximum length of the key is 32.<br>**<passwd 32>** - The maximum length of the password is 32 characters long. |
| **default** - Sets the auth_port to be 1812 and acct_port to be 1813. |
| **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.<br>**<udp_port_number 1-65535>** - The authentication port 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.<br>**<udp_port_number 1-65535>** - The accounting statistics value must be between 1 and 65535. |
| **timeout** - Specify the time, in seconds ,for waiting server reply. The default value is 5 seconds.<br>**<int 1-255>** - The timeout value must be between 1 and 255. |
| **retransmit** - Specify the count for re-transmit. The default value is 2.<br>**<int 1-20>** - The re-transmit value must be between 1 and 20. |

### Restrictions

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

### Example

To add a new RADIUS server:

```
DGS-3620-28SC: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-3620-28SC:admin#
```

## 3-21 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>** - Specify the RADIUS server index. The range is from 1 to 3.

### Restrictions

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

### Example

To delete a RADIUS server:

```
DGS-3620-28SC:admin#config radius delete 1
Command: config radius delete 1

Success.

DGS-3620-28SC:admin#
```

## 3-22 config radius

### Description

This command is used to configure a RADIUS server.

### Format

**config radius <server_index 1-3> {ipaddress [<server_ip> | <ipv6addr>] | key <password 32> | auth_port [<udp_port_number 1-65535> | default] | acct_port [<udp_port_number 1-65535> | default] | timeout [<sec 1-255> | default] | retransmit [<int 1-20> | default]}(1)**

### Parameters

**<server_index 1-3>** - Specify the RADIUS server index.

**ipaddress** - Specify the IP address of the RADIUS server.
**<server_ip>** - Enter the RADIUS server IP address here.
**<ipv6addr>** - Enter the IPv6 address here.

**key** - Specify the key pre-negotiated between the switch and the RADIUS server. It is used to encrypt user's authentication data before being transmitted over the Internet. The maximum length of the key is 32.
**<passwd 32>** - Specify the key pre-negotiated between the switch and the RADIUS server. It is used to encrypt user's authentication data before being transmitted over the Internet. The maximum length of the key is 32.

**auth_port** - Specify the UDP port number which is used to transmit RADIUS authentication data between the switch and the RADIUS server. The default is 1812.
**<udp_port_number 1-65535>** - The authentication port value must be between 1 and 65535.
**default** - Specify to use the default value.

**acct_port** - Specify the UDP port number which is used to transmit RADIUS accounting statistics between the switch and the RADIUS server. The default is 1813.
**<udp_port_number 1-65535>** - The accounting statistics value must be between 1 and 65535.
**default** - Specify to use the default value.

**timeout** - Specify the time in seconds for waiting for a server reply. The default value is 5 seconds.
**<int 1-255>** - Specify the time in seconds for waiting for a server reply. The timeout value must be between 1 and 255. The default value is 5 seconds.
**default** - Specify to use the default value.

**retransmit** - Specify the count for re-transmission. The default value is 2.
**<int 1-20>** - The re-transmit value must be between 1 and 20.
**default** - Specify to use the default value.

### Restrictions

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

### Example

To configure a RADIUS server:

```
DGS-3620-28SC:admin#config radius 1 ipaddress 10.48.74.121 key dlink
Command: config radius 1 ipaddress 10.48.74.121 key dlink

Success.

DGS-3620-28SC:admin#
```

## 3-23 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-3620-28SC:admin#show radius
Command: show radius

Index 1
    IP Address     : 192.168.69.1
    Auth-Port      : 1812
    Acct-Port      : 1813
    Timeout        : 5
    Retransmit     : 2
    Key            : 123456

Total Entries : 1

DGS-3620-28SC:admin#
```

## 3-24 show auth_statistics

### Description

This command is used to display authenticator statistics information

### Format

**show auth_statistics {ports <portlist>}**

### Parameters

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

### Restrictions

None.

### Example

To display authenticator statistics information for port 3:

```
DGS-3620-28SC:admin# show auth_statistics ports 3
Command: show auth_statistics ports 3

Auth VID    :100
MAC Address :00-00-00-00-00-03
Port number : 3

EapolFramesRx                           0
EapolFramesTx                           6
EapolStartFramesRx                      0
EapolReqIdFramesTx                      6
EapolLogoffFramesRx                     0
EapolReqFramesTx                        0
EapolRespIdFramesRx                     0
EapolRespFramesRx                       0
InvalidEapolFramesRx                    0
EapLengthErrorFramesRx                  0
LastEapolFrameVersion                   0
LastEapolFrameSource                    00-00-00-00-00-03

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

## 3-25 show auth_diagnostics

### Description

This command is used to display authenticator diagnostics information.

### Format

**show auth_diagnostics {ports <portlist>}**

### Parameters

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

### Restrictions

None.

### Example

To display authenticator diagnostics information for port 3:

```
DGS-3620-28SC:admin# show auth_diagnostics ports 3
Command: show auth_diagnostics ports 3

Auth VID                                100
```

```
MAC Address                               00-00-00-00-00-03
Port number : 1

EntersConnecting                          20
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
```

## 3-26 show auth_session_statistics

### Description

This command is used to display authenticator session statistics information.

### Format

**show auth_session_statistics {ports <portlist>}**

### Parameters

| |
|---|
| **ports** - (Optional) Specify a range of ports to be displayed.<br>**<portlist>** - Specify a range of ports to be displayed. |

### Restrictions

None.

### Example

To display authenticator session statistics information for port 1:

```
DGS-3620-28SC:admin# show auth_session_statistics ports 3
Command: show auth_session_statistics ports 3

Auth VID     : 100
MAC Address : 00-00-00-00-00-03
```

```
Port number : 3

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
```

## 3-27 show auth_client

### Description

This command is used to display authentication client information.

### Format

**show auth_client**

### Parameters

None.

### Restrictions

None.

### Example

To display authentication client information:

```
DGS-3620-28SC:admin# show auth_client
Command: show auth_client

radiusAuthClient ==>
radiusAuthClientInvalidServerAddresses   0
radiusAuthClientIdentifier               D-Link


radiusAuthServerEntry ==>
radiusAuthServerIndex :1

radiusAuthServerAddress                  0.0.0.0
radiusAuthClientServerPortNumber         X
radiusAuthClientRoundTripTime            0
radiusAuthClientAccessRequests           0
radiusAuthClientAccessRetransmissions    0
```

```
radiusAuthClientAccessAccepts            0
radiusAuthClientAccessRejects            0
radiusAuthClientAccessChallenges         0
radiusAuthClientMalformedAccessResponses 0
radiusAuthClientBadAuthenticators        0
radiusAuthClientPendingRequests          0
radiusAuthClientTimeouts                 0
radiusAuthClientUnknownTypes             0
radiusAuthClientPacketsDropped           0

radiusAuthClient ==>
radiusAuthClientInvalidServerAddresses   0
radiusAuthClientIdentifier               D-Link


radiusAuthServerEntry ==>
radiusAuthServerIndex :2

radiusAuthServerAddress                  0.0.0.0
radiusAuthClientServerPortNumber         X
radiusAuthClientRoundTripTime            0
radiusAuthClientAccessRequests           0
radiusAuthClientAccessRetransmissions    0
radiusAuthClientAccessAccepts            0
radiusAuthClientAccessRejects            0
radiusAuthClientAccessChallenges         0
radiusAuthClientMalformedAccessResponses 0
radiusAuthClientBadAuthenticators        0
radiusAuthClientPendingRequests          0
radiusAuthClientTimeouts                 0
radiusAuthClientUnknownTypes             0
radiusAuthClientPacketsDropped           0

radiusAuthClient ==>
radiusAuthClientInvalidServerAddresses   0
radiusAuthClientIdentifier               D-Link


radiusAuthServerEntry ==>
radiusAuthServerIndex :3

radiusAuthServerAddress                  0.0.0.0
radiusAuthClientServerPortNumber         X
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-3620-28SC:admin#
```

## 3-28 show acct_client

### Description

This command is used to display account client information

### Format

**show acct_client**

### Parameters

None.

### Restrictions

None.

### Example

To display account client information:

```
DGS-3620-28SC:admin# show acct_client
Command: show acct_client

radiusAcctClient ==>
radiusAcctClientInvalidServerAddresses   0
radiusAcctClientIdentifier               D-Link


radiusAuthServerEntry ==>
radiusAccServerIndex : 1

radiusAccServerAddress                   0.0.0.0
radiusAccClientServerPortNumber          X
radiusAccClientRoundTripTime             0
radiusAccClientRequests                  0
radiusAccClientRetransmissions           0
radiusAccClientResponses                 0
radiusAccClientMalformedResponses        0
radiusAccClientBadAuthenticators         0
radiusAccClientPendingRequests           0
radiusAccClientTimeouts                  0
radiusAccClientUnknownTypes              0
radiusAccClientPacketsDropped            0

```

```
radiusAcctClient ==>
radiusAcctClientInvalidServerAddresses   0
radiusAcctClientIdentifier               D-Link


radiusAuthServerEntry ==>
radiusAccServerIndex : 2

radiusAccServerAddress                   0.0.0.0
radiusAccClientServerPortNumber          X
radiusAccClientRoundTripTime             0
radiusAccClientRequests                  0
radiusAccClientRetransmissions           0
radiusAccClientResponses                 0
radiusAccClientMalformedResponses        0
radiusAccClientBadAuthenticators         0
radiusAccClientPendingRequests           0
radiusAccClientTimeouts                  0
radiusAccClientUnknownTypes              0
radiusAccClientPacketsDropped            0

radiusAcctClient ==>
radiusAcctClientInvalidServerAddresses   0
radiusAcctClientIdentifier               D-Link


radiusAuthServerEntry ==>
radiusAccServerIndex : 3

radiusAccServerAddress                   0.0.0.0
radiusAccClientServerPortNumber          X
radiusAccClientRoundTripTime             0
radiusAccClientRequests                  0
radiusAccClientRetransmissions           0
radiusAccClientResponses                 0
radiusAccClientMalformedResponses        0
radiusAccClientBadAuthenticators         0
radiusAccClientPendingRequests           0
radiusAccClientTimeouts                  0
radiusAccClientUnknownTypes              0
radiusAccClientPacketsDropped            0

DGS-3620-28SC:admin#
```

## 3-29 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 | disable]**

### Parameters

**network** - Specify the accounting service for 802.1X and WAC/JWAC port access control. By default, the service is disabled.

**shell** - Specify the accounting service for shell events. When a user logins or logouts of the switch (via the console, Telnet, or SSH) and when timeout occurs, accounting information will be collected and sent to the RADIUS server. By default, the service is disabled.

**system** - Specify the accounting service for system events: reset and reboot. By default, the service is disabled.

**state** - Specify the state of the accounting service.
**enable** - Enable the specified accounting service.
**disable** - Disable the specified accounting service.

### Restrictions

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

### Example

To configure the state of the RADIUS accounting service shell to enable:

```
DGS-3620-28SC:admin# config accounting service shell state enable
Command: config accounting service shell state enable

Success

DGS-3620-28SC:admin#
```

## 3-30 show accounting service

### Description

This command is used to display RADIUS accounting service information.

### Format

**show accounting service**

### Parameters

None.

### Restrictions

None.

### Example

To display accounting service information:

```
DGS-3620-28SC:admin#show accounting service
Command: show accounting service

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

DGS-3620-28SC:admin#
```

# Chapter 4 Access Authentication Control (AAC) Commands

**enable authen_policy**

**disable authen_policy**

**show authen_policy**

**create authen_login method_list_name** <string 15>

**config authen_login** [default | method_list_name <string 15>] method {tacacs | xtacacs | tacacs+ | radius | server_group <string 15> | local | none}(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] | 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] | timeout <int 1-255> | retransmit <int 1-20>}(1)

**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**

The TACACS / XTACACS / TACACS+ / RADIUS commands allows secure access to the Switch using the TACACS / XTACACS / TACACS+ / RADIUS protocols. When a user logs in to the Switch or tries to access the administrator level privilege, he or she is prompted for a password. If TACACS / XTACACS / TACACS+ / RADIUS authentication is enabled on the Switch, it will contact a TACACS / XTACACS / TACACS+ / RADIUS server to verify the user. If the user is verified, he or she is granted access to the Switch.

There are currently three versions of the TACACS security protocol, each a separate entity. The Switch's software supports the following versions of TACACS:

1. **TACACS (Terminal Access Controller Access Control System)** —Provides password checking and authentication, and notification of user actions for security purposes utilizing

via one or more centralized TACACS servers, utilizing the UDP protocol for packet transmission.

2. **Extended TACACS (XTACACS)** — An extension of the TACACS protocol with the ability to provide more types of authentication requests and more types of response codes than TACACS. This protocol also uses UDP to transmit packets.
3. **TACACS+ (Terminal Access Controller Access Control System plus)** — Provides detailed access control for authentication for network devices. TACACS+ is facilitated through Authentication commands via one or more centralized servers. The TACACS+ protocol encrypts all traffic between the Switch and the TACACS+ daemon, using the TCP protocol to ensure reliable delivery.

The Switch also supports the RADIUS protocol for authentication using the Access Authentication Control commands. RADIUS or Remote Authentication Dial In User Server also uses a remote server for authentication and can be responsible for receiving user connection requests, authenticating the user and returning all configuration information necessary for the client to deliver service through the user. RADIUS may be facilitated on this Switch using the commands listed in this section.

In order for the TACACS / XTACACS / TACACS+ / RADIUS security function to work properly, a TACACS / XTACACS / TACACS+ / RADIUS server must be configured on a device other than the Switch, called a server host and it must include usernames and passwords for authentication. When the user is prompted by the Switch to enter usernames and passwords for authentication, the Switch contacts the TACACS / XTACACS / TACACS+ / RADIUS server to verify, and the server will respond with one of three messages:

The server verifies the username and password, and the user is granted normal user privileges on the Switch. The server will not accept the username and password and the user is denied access to the Switch.

The server doesn’t respond to the verification query. At this point, the Switch receives the timeout from the server and then moves to the next method of verification configured in the method list.

The Switch has four built-in server groups, one for each of the TACACS, XTACACS, TACACS+ and RADIUS protocols. These built-in server groups are used to authenticate users trying to access the Switch. The users will set server hosts in a preferable order in the built-in server group and when a user tries to gain access to the Switch, the Switch will ask the first server host for authentication. If no authentication is made, the second server host in the list will be queried, and so on. The built-in server group can only have hosts that are running the specified protocol. For example, the TACACS server group can only have TACACS server hosts.

The administrator for the Switch may set up five different authentication techniques per user-defined method list (TACACS / XTACACS / TACACS+ / RADIUS / local / none) for authentication. These techniques will be listed in an order preferable, and defined by the user for normal user authentication on the Switch, and may contain up to eight authentication techniques. When a user attempts to access the Switch, the Switch will select the first technique listed for authentication. If the first technique goes through its server hosts and no authentication is returned, the Switch will then go to the next technique listed in the server group for authentication, until the authentication has been verified or denied, or the list is exhausted.

**Note:** User granted access to the Switch will be granted normal user privileges on the Switch. To gain access to admin level privileges, the user must enter the enable admin command and then enter a password, which was previously configured by the administrator of the Switch.

✎ **Note:** TACACS, XTACACS and TACACS+ are separate entities and are not compatible. The Switch and the server must be configured exactly the same, using the same protocol. (For example, if the Switch is set up for TACACS authentication, so must be the host server.)

## 4-1 enable authen_policy

### Description

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

### Format

**enable authen_policy**

### Parameters

None.

### Restrictions

Only Administrator-level users can issue this command.

### Example

To enable system access authentication policy:

```
DGS-3620-28SC:admin#enable authen_policy
Command: enable authen_policy

Success.

DGS-3620-28SC:admin#
```

## 4-2 disable authen_policy

### Description

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

### Format

**disable authen_policy**

### Parameters

None.

### Restrictions

Only Administrator-level users can issue this command.

### Example

To disable system access authentication policy:

```
DGS-3620-28SC:admin#disable authen_policy
Command: disable authen_policy

Success.

DGS-3620-28SC:admin#
```

## 4-3 show authen_policy

### Description

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

### Format

**show authen_policy**

### Parameters

None.

### Restrictions

Only Administrator-level users can issue this command.

### Example

To display system access authentication policy:

```
DGS-3620-28SC:admin#show authen_policy
Command: show authen_policy

Authentication Policy : Enabled

DGS-3620-28SC:admin#
```

## 4-4 create authen_login method_list_name

### 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 eight.

### Format

**create authen_login method_list_name <string 15>**

### Parameters

**<string 15>** - Specify the user-defined method list name.

### Restrictions

Only Administrator-level users can issue this command.

### Example

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

```
DGS-3620-28SC:admin#create authen_login method_list_name login_list_1
Command: create authen_login method_list_name login_list_1

Success.

DGS-3620-28SC:admin#
```

## 4-5 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 affect the authentication result. For example, if the sequence is TACACS+ first, then TACACS and local, when a user trys to login, the authentication request will be sent to the first server host in the TACACS+ built-in server group. If the first server host in the TACACS+ group is missing, the authentication request will be sent to the second server host in the TACACS+ group, and so on. If all server hosts in the TACACS+ group are missing, the authentication request will be sent to the first server host in the TACACS group. If all server hosts in a TACACS group are missing, the local account database in the device is used to authenticate this user. When a user logs in to 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 a user wants to get admin privilege level, the user must use the “enable admin” command to promote his privilege level. But when the 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** – Specify the default method list of authentication methods.

**method_list_name** - Specify the user-defined method list of authentication methods.
- **<string 15>** - Specify the user-defined method list of authentication methods. The method list name can be up to 15 characters long.

**method** - Choose the desired authentication method:
- **tacacs** - Specify authentication by the built-in server group TACACS.
- **xtacacs** - Specify authentication by the built-in server group XTACACS.
- **tacacs+** - Specify authentication by the built-in server group TACACS+.
- **radius** - Specify authentication by the built-in server group RADIUS.
- **server_group** - Specify authentication by the user-defined server group.
  - **<string 15>** - Specify authentication by the user-defined server group. The server group value can be up to 15 characters long.
- **local** - Specify authentication by local user account database in the device.
- **none** - Specify no authentication.

### Restrictions

Only Administrator-level users can issue this command.

### Example

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

```
DGS-3620-28SC: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-3620-28SC:admin#
```

## 4-6 delete authen_login method_list_name

### 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>** - Specify the user-defined method list name.

### Restrictions

Only Administrator-level users can issue this command.

### Example

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

```
DGS-3620-28SC:admin#delete authen_login method_list_name login_list_1
Command: delete authen_login method_list_name login_list_1

Success.

DGS-3620-28SC:admin#
```

## 4-7 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** – Specify to display the default method list for user login.

**method_list_name** - Specify the user-defined method list for user login.

**<string 15>** - Specify the user-defined method list for user login. The method list name can be up to 15 characters long.

**all** – Specify to display all method lists for user login.

### Restrictions

Only Administrator-level users can issue this command.

### Example

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

```
DGS-3620-28SC: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-3620-28SC:admin#
```

## 4-8 create authen_enable method_list_name

### Description

This command is used to create a user-defined method list of authentication methods for promoting a user's privilege to Admin level. The maximum supported number of the enable method lists is eight.

### Format

**create authen_enable method_list_name <string 15>**

### Parameters

**<string 15>** - Specify the user-defined method list name.

### Restrictions

Only Administrator-level users can issue this command.

### Example

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

```
DGS-3620-28SC:admin#create authen_enable method_list_name enable_list_1
Command: create authen_enable method_list_name enable_list_1

Success.

DGS-3620-28SC:admin#
```

## 4-9 config authen_enable

### Description

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

### 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** - Specify the default method list of authentication methods.

**method_list_name** - Specify the user-defined method list of authentication methods.
  **<string 15>** - Specify the user-defined method list of authentication methods. The method list name can be up to 15 characters long.

**method** - Choose the desired authentication method:
  **tacacs** - Specify authentication by the built-in server group TACACS.
  **xtacacs** - Specify authentication by the built-in server group XTACACS.
  **tacacs+** - Specify authentication by the built-in server group TACACS+.
  **radius** - Specify authentication by the built-in server group RADIUS.
  **server_group** - Specify authentication by the user-defined server group.
    **<string 15>** - Specify authentication by the user-defined server group. The server group value can be up to 15 characters long.
  **local_enable** - Specify authentication by local enable password in the device.
  **none** - Specify no authentication.

### Restrictions

Only Administrator-level users can issue this command.

### Example

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

```
DGS-3620-28SC: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-3620-28SC:admin#
```

## 4-10 delete authen_enable method_list_name

### Description

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

### Format

**delete authen_enable method_list_name <string 15>**

### Parameters

**<string 15>** - Specify the user-defined method list name.

### Restrictions

Only Administrator-level users can issue this command.

### Example

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

```
DGS-3620-28SC:admin#delete authen_enable method_list_name enable_list_1
Command: delete authen_enable method_list_name enable_list_1

Success.

DGS-3620-28SC:admin#
```

## 4-11 show authen_enable

### Description

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

### Format

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

### Parameters

**default** - Specify to display the default method list for promoting a user's privilege to Administrator level.

**method_list_name** - Specify the user-defined method list for promoting a user's privilege to Administrator level.

**<string 15>** - Specify the user-defined method list for a promoting a user's privilege to Administrator level . The method list name value can be up to 15 characters long.

**all** - Specify to display all method lists for promoting a user's privilege to Administrator level.

### Restrictions

Only Administrator-level users can issue this command.

### Example

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

```
DGS-3620-28SC:admin#show authen_enable all
Command: show authen_enable all

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

enable_list_2     1         tacacs+         Built-in Group
                  2         radius          Built-in Group

```

```
Total Entries : 3

DGS-3620-28SC:admin#
```

## 4-12 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** - Specify an application: console.
**telnet** - Specify an application: Telnet.
**ssh** - Specify an application: SSH.
**http** - Specify an application: Web.
**all** - Specify all applications: console, Telnet, SSH, and Web.

**login** - Specify the method list of authentication methods for user login.
**enable** - Specify the method list of authentication methods for promoting user privilege to Administrator level.

**default** - Specify the default method list.
**method_list_name** - Specify the user-defined method list name.
**<string 15>** - Specify the user-defined method list name. The method list name value can be up to 15 characters long.

### Restrictions

Only Administrator-level users can issue this command.

### Example

To configure the login method list for Telnet:

```
DGS-3620-28SC: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-3620-28SC:admin#
```

## 4-13 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 Administrator-level users can issue this command.

### Example

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

```
DGS-3620-28SC: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-3620-28SC:admin#
```

## 4-14 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 eight. Each group consists of eight server hosts as maximum.

### Format

**create authen server_group <string 15>**

### Parameters

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

### Restrictions

Only Administrator-level users can issue this command.

### Example

To create a user-defined authentication server group:

```
DGS-3620-28SC:admin#create authen server_group mix_1
Command: create authen server_group mix_1

Success.

DGS-3620-28SC:admin#
```

## 4-15 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+, and RADIUS accept the server host with the same protocol only, but user-defined server group can accept server hosts with different protocols. The server host must be created first by using the CLI command **create authen server_host**.

### Format

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

### Parameters

| |
|---|
| **tacacs** - Specify the built-in server group TACACS.<br>**xtacacs** - Specify the built-in server group XTACACS.<br>**tacacs+** - Specify the built-in server group TACACS+.<br>**radius** – Specify the built-in server group RADIUS.<br>**<string 15>** - Specify a user-defined server group. |
| **add** - Specify to add a server host to a server group.<br>**delete** - Specify to remove a server host from a server group. |
| **server_host** - Specify the server host’s IP address.<br>**<ipaddr>** - Specify the server host’s IP address. |
| **protocol** - Specify the server host’s type of authentication protocol.<br>**tacacs** - Specify the server host’s authentication protocol TACACS.<br>**xtacacs** - Specify  the server host’s authentication protocol XTACACS.<br>**tacacs+** - Specify the server host’s authentication protocol TACACS+.<br>**radius** - Specify the server host’s authentication protocol RADIUS. |

### Restrictions

Only Administrator-level users can issue this command.

### Example

To add an authentication server host to a server group:

```
DGS-3620-28SC: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-3620-28SC:admin#
```

## 4-16 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>** - Specify the user-defined server group name. |

### Restrictions

Only Administrator-level users can issue this command.

### Example

To delete a user-defined authentication server group:

```
DGS-3620-28SC:admin#delete authen server_group mix_1
Command: delete authen server_group mix_1

Success.

DGS-3620-28SC:admin#
```

## 4-17 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) Specify the built-in or user-defined server group name. |

### Restrictions

Only Administrator-level users can issue this command.

### Example

To display all authentication server groups:

```
DGS-3620-28SC:admin#show authen server_group
Command: show authen server_group

Group Name       IP Address       Protocol
---------------  ---------------  --------
mix_1            10.1.1.222       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-3620-28SC:admin#
```

## 4-18 create authen server_host

### Description

This command is used to create an authentication server host. When an authentication server host is created, the IP address and protocol are the index. That means more than one authentication protocol service 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] | timeout <int 1-255> | retransmit <int 1-20>}**

### Parameters

**<ipaddr>** - Specify the server host’s IP address.

**protocol** - Specify the server host’s type of authentication protocol.
**tacacs** - Specify  the server host’s authentication protocol TACACS.
**xtacacs** - Specify the server host’s authentication protocol XTACACS.
**tacacs+** - Specify the server host’s authentication protocol TACACS+.
**radius** - Specify the server host’s authentication protocol RADIUS.

**port** - (Optional) Specify the port number of the authentication protocol for the server host. The default value for TACACS/XTACACS/TACACS+ is 49. The default value for RADIUS is 1812.
**<int 1-65535>** - Specify the port number of the authentication protocol for the server host. The default value for TACACS/XTACACS/TACACS+ is 49. The default value for RADIUS is 1812. The port number must be between 1 and 65535.

**key** - (Optional) Specify the key for TACACS+ and RADIUS authentication.
**<key_string 254>** - Specify the key for TACACS+ and RADIUS authenticaiton. If the value is null, no encryption will apply. This value is meaningless for TACACS and XTACACS.
**none** - No encryption for TACACS+ and RADIUS authenticaiton. This value is meaningless for TACACS and XTACACS.

**timeout** - (Optional) Specify the time in seconds for waiting for a server reply. The default value is 5 seconds.
**<int 1-255>** - Specify the time in seconds for waiting for a server reply. The default value is 5 seconds. The timeout value must be between 1 and 255 seconds.

**retransmit** - (Optional) Specify the count for re-transmit. This value is meaningless for TACACS+. The default value is 2.
  **<int 1-20>** - Specify the count for re-transmit. This value is meaningless for TACACS+. The default value is 2. The re-transmit value must be between 1 and 20.

### Restrictions

Only Administrator-level users can issue this command.

### Example

To create a TACACS+ authentication server host with a listening port number of 15555 and a timeout value of 10 seconds:

```
DGS-3620-28SC:admin#create authen server_host 10.1.1.222 protocol tacacs+ port
15555 key "123" timeout 10
Command: create authen server_host 10.1.1.222 protocol tacacs+ port 15555 key
"123" timeout 10


Success.


DGS-3620-28SC:admin#
```

## 4-19 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] | timeout <int 1-255> | retransmit <int 1-20>}(1)**

### Parameters

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

**protocol** - Specify the server host's type of authentication protocol.
  **tacacs** - Specify the server host's authentication protocol TACACS.
  **xtacacs** - Specify the server host's authentication protocol XTACACS.
  **tacacs+** - Specify the server host's authentication protocol TACACS+.
  **radius** - Specify the server host's authentication protocol RADIUS.

**port** - Specify the port number of the authentication protocol for the server host. The default value for TACACS/XTACACS/TACACS+ is 49. The default value for RADIUS is 1812.
  **<int 1-65535>** - Specify the port number of the authentication protocol for the server host. The default value for TACACS/XTACACS/TACACS+ is 49. The default value for RADIUS is 1812. The port number must be between 1 and 65535.

**key** - Specify the key for TACACS+ and RADIUS authentication.
  **<key_string 254>** - Specify the key for TACACS+ and RADIUS authentication. If the value is null, no encryption will apply. This value is meaningless for TACACS and XTACACS.
  **none** - Specify no encryption for TACACS+ and RADIUS authentication. This value is meaningless for TACACS and XTACACS.

**timeout** - Specify the time in seconds for waiting for a server reply. The default value is 5 seconds.
  **<int 1-255>** - Specify the time in seconds for waiting for a server reply. The default value is 5

seconds. The timeout value must be between 1 and 255 seconds.

**retransmit** - Specify the count for re-transmit. This value is meaningless for TACACS+. The default value is 2.

**<int 1-20>** - Specify the count for re-transmit. This value is meaningless for TACACS+. The default value is 2. The re-transmit value must be between 1 and 20.

### Restrictions

Only Administrator-level users can issue this command.

### Example

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

```
DGS-3620-28SC:admin#config authen server_host 10.1.1.222 protocol tacacs+ key
"abc123"
Command: config authen server_host 10.1.1.222 protocol tacacs+ key "abc123"

Success.

DGS-3620-28SC:admin#
```

## 4-20 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>** - Specify the server host's IP address.

**protocol** - Specify the server host's type of authentication protocol.
**tacacs** - Specify  the server host's authentication protocol TACACS.
**xtacacs** - Specify the server host's authentication protocol XTACACS.
**tacacs+** - Specify the server host's authentication protocol TACACS+.
**radius** - Specify the server host's authentication protocol RADIUS.

### Restrictions

Only Administrator-level users can issue this command.

### Example

To delete an authentication server host:

```
DGS-3620-28SC:admin#delete authen server_host 10.1.1.222 protocol tacacs+
Command: delete authen server_host 10.1.1.222 protocol tacacs+

Success.
```

```
DGS-3620-28SC:admin#
```

## 4-21 show authen server_host

### Description

This command is used to display authentication server hosts.

### Format

**show authen server_host**

### Parameters

None.

### Restrictions

Only Administrator-level users can issue this command.

### Example

To display all authentication server hosts:

```
DGS-3620-28SC:admin#show authen server_host
Command: show authen server_host

IP Address       Protocol  Port   Timeout  Retransmit  Key
---------------  --------  -----  -------  ----------  -----------------------
10.1.1.222       TACACS+   15555  10       ------      123

Total Entries : 1

DGS-3620-28SC:admin#
```

## 4-22 config authen parameter response_timeout

### Description

This command is used to configure the amount of time waiting for user to input on console, Telnet, and SSH applications.

### Format

**config authen parameter response_timeout <int 0-255>**

### Parameters

**<int 0-255>** - Specify the amount of time for user input on console or Telnet or SSH. 0 means there is no time out. The default value is 30 seconds.

### Restrictions

Only Administrator-level users can issue this command.

### Example

To configure 60 seconds for user to input:

```
DGS-3620-28SC:admin#config authen parameter response_timeout 60
Command: config authen parameter response_timeout 60

Success.

DGS-3620-28SC:admin#
```

## 4-23 config authen parameter attempt

### Description

This command is used to configure the maximum attempts for users trying to login or promote the privilege on console, Telnet, or SSH applications. If the failure value is exceeded, connection or access will be locked.

### Format

**config authen parameter attempt <int 1-255>**

### Parameters

**<int 1-255>** - Specify the amount of attempts for users trying to login or promote the privilege on console, Telnet, or SSH. The default value is 3.

### Restrictions

Only Administrator-level users can issue this command.

### Example

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

```
DGS-3620-28SC:admin#config authen parameter attempt 9
Command: config authen parameter attempt 9

Success.

DGS-3620-28SC:admin#
```

## 4-24 show authen parameter

### Description

This command is used to display the authentication parameters.

### Format

**show authen parameter**

### Parameters

None.

### Restrictions

Only Administrator-level users can issue this command.

### Example

To display the authentication parameters:

```
DGS-3620-28SC:admin# show authen parameter
Command: show authen parameter

Response Timeout : 60 seconds
User Attempts    : 9

DGS-3620-28SC:admin#
```

## 4-25 enable admin

### Description

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

### Format

**enable admin**

### Parameters

None.

### Restrictions

None.

### Example

To enable administrator lever privilege:

```
DGS-3620-28SC:admin# enable admin
Password:********

DGS-3620-28SC:admin#
```

## 4-26 config admin local_enable

### Description

This command is used to configure the local enable password for the enable command. When the user chooses the local_enable method to promote the privilege level, the enable password of the local device is needed.

### Format

**config admin local_enable**

### Parameters

None.

### Restrictions

Only Administrator-level users can issue this command.

### Example

To configure the administrator password:

```
DGS-3620-28SC: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-3620-28SC:admin#
```

# Chapter 5 Access Control List (ACL) Commands

**create access_profile profile_id** <value 1-6> profile_name <name 1-32> [ethernet {vlan {<hex 0x0-0x0fff>} | source_mac <macmask 000000000000-ffffffffffff> | destination_mac <macmask 000000000000-ffffffffffff> | 802.1p | ethernet_type}(1) | 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>}]}(1) | packet_content_mask {offset_chunk_1 <value 0-31> <hex 0x0-0xffffffff> | offset_chunk_2 <value 0-31> <hex 0x0-0xffffffff> | offset_chunk_3 <value 0-31> <hex 0x0-0xffffffff> | offset_chunk_4 <value 0-31> <hex 0x0-0xffffffff>}(1) | ipv6 {class | flowlabel | source_ipv6_mask <ipv6mask> | destination_ipv6_mask <ipv6mask> | [tcp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | udp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | icmp {type | code}]}(1)]

**delete access_profile** [profile_id <value 1-6> | profile_name <name 1-32> | all]

**config access_profile** [profile_id <value 1-6> | profile_name <name 1-32>] [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>}(1) | 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>}}]}(1) | 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>}}(1) | 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 <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>}]}(1)] [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 time_range** <range_name 32> [hours start_time <time hh:mm:ss> end_time <time hh:mm:ss> weekdays <daylist> | delete]

**show time_range**

**show current_config access_profile**

**delete cpu access_profile** [profile_id <value 1-5> | all]

**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}(1) | 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>}]}(1) | 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>}(1) | ipv6 {class | flowlabel | source_ipv6_mask <ipv6mask> | destination_ipv6_mask <ipv6mask>}(1)]

**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>]

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

**enable cpu_interface_filtering**

**disable cpu_interface_filtering**

**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_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 <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>}}

## 5-1 create access_profile profile_id

### Description

This command is used to create access list profiles.

**Note:** Please see the "**Error! Reference source not found. Error! Reference source not found.**" section for a configuration example and further information.

### Format

**create access_profile profile_id <value 1-6> profile_name <name 1-32> [ethernet {vlan {<hex 0x0-0x0fff>} | source_mac <macmask 000000000000-ffffffffffff> | destination_mac <macmask 000000000000-ffffffffffff> | 802.1p | ethernet_type}(1) | 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>}]}(1) | packet_content_mask {offset_chunk_1 <value 0-31> <hex 0x0-0xffffffff> | offset_chunk_2 <value 0-31> <hex 0x0-0xffffffff> | offset_chunk_3 <value 0-31> <hex 0x0-0xffffffff> | offset_chunk_4 <value 0-31> <hex 0x0-0xffffffff>}(1) | ipv6 {class | flowlabel | source_ipv6_mask <ipv6mask> | destination_ipv6_mask <ipv6mask> | [tcp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | udp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | icmp {type | code}]}(1)]**

## Parameters

**<value 1-6>** - Specify the profile ID between 1 and 6. The lower the profile ID, the higher the priority.
**profile_name** - Specify a profile name.
**<name 1-32>** - The maximum length is 32 characters.

**ethernet** - Specify an Ethernet access control list rule.
**vlan** - Specify a VLAN mask. Only the last 12 bits of the mask will be considered.
**<hex 0x0-0x0fff>** - (Optional) Specify a VLAN mask.
**source_mac** - Specify the source MAC mask.
**<macmask 000000000000-ffffffffffff>** - Specify the source MAC mask.
**destination_mac** - Specify the destination MAC mask.
**<macmask 000000000000-ffffffffffff>** - Specify the destination MAC mask.
**802.1p** - Speciy the 802.1p priority tag mask.
**ethernet_type** - Specify the Ethernet type.

**ip** - Specify an IP access control list rule.
**vlan** - Specify a VLAN mask. Only the last 12 bits of the mask will be considered.
**<hex 0x0-0x0fff>** - (Optional) Specify a VLAN mask.
**source_ip_mask** - Specify an IP source submask.
**<netmask>** - Specify an IP source submask.
**destination_ip_mask** - Specify an IP destination submask.
**<netmask>** - Specify an IP destination submask.
**dscp** - Specify the DSCP mask.
**icmp** - Specify that the rule applies to ICMP traffic.
**type** - (Optional) Specify the ICMP packet type.
**code** - (Optional) Specify the ICMP code.
**igmp** - Specify that the rule applies to IGMP traffic.
**type** - (Optional) Specify the IGMP packet type.
**tcp** - Specify that the rule applies to TCP traffic.
**src_port_mask** - (Optional) Specify the TCP source port mask.
**<hex 0x0-0xffff>** - Specify the TCP source port mask.
**dst_port_mask** - (Optional) Specify the TCP destination port mask.
**<hex 0x0-0xffff>** - Specify the TCP destination port mask.
**flag_mask** - (Optional) Specify the TCP flag field mask.
**all** – Specify to check all paramenters below.
**urg** - (Optional) Specify Urgent Pointer field significant.
**ack** - (Optional) Specify Acknowledgment field significant.
**psh** - (Optional) Specify Push Function.
**rst** - (Optional) Specify to reset the connection.
**syn** - (Optional) Specify to synchronize sequence numbers.
**fin** - (Optional) No more data from sender.
**udp** - Specify that the rule applies to UDP traffic.
**src_port_mask** - (Optional) Specify the TCP source port mask.
**<hex 0x0-0xffff>** - Specify the TCP source port mask.
**dst_port_mask** - (Optional) Specify the TCP destination port mask.
**<hex 0x0-0xffff>** - Specify the TCP destination port mask.
**protocol_id_mask** - Specify that the rule applies to the IP protocol ID traffic.
**<hex 0x0-0xff>** - Specify that the rule applies to the IP protocol ID traffic.
**user_define_mask** - (Optional) Specify the L4 part mask.
**<hex 0x0-0xffffffff>** - Specify the L4 part mask.

**packet_content_mask** - A maximum of six offsets can be specified. Each offset defines one byte of data which is identified as a single UDF field. The offset reference is also configurable. It can be defined to start at the end of the tag, the end of the Ethernet type, or the end of the IP header.

**offset_chunk_1** - Specifies the offset chunk 1 that allows users to examine the specified offset_chunks within a packet at one time and specifies the frame content offset and mask.

**<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 value here.

**offset_chunk_2** - Specifies the offset chunk 2 that allows users to examine the specified offset_chunks within a packet at one time and specifies the frame content offset and mask.

**<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 value here.

**offset_chunk_3** - Specifies the offset chunk 3 that allows users to examine the specified offset_chunks within a packet at one time and specifies the frame content offset and mask.

**<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 value here.

**offset_chunk_4** - Specifies the offset chunk 4 that allows users to examine the specified offset_chunks within a packet at one time and specifies the frame content offset and mask.

**<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 value here.

**ipv6** - Specify the IPv6 filtering mask.

**class** - Specify the IPv6 class mask.

**flowlabel** - Specify the IPv6 flow label mask.

**source_ipv6_mask** - Specify the IPv6 source IP mask.

**<ipv6mask>** - Specify the IPv6 source IP mask.

**destination_ipv6_mask** - Specify the IPv6 destination IP mask.

**<ipv6mask>** - Specify the IPv6 destination IP mask.

**tcp** - Specify that the rule applies to TCP traffic.

**src_port_mask** - (Optional) Specify the TCP source port mask.

**<hex 0x0-0xffff>** - Specify the TCP source port mask.

**dst_port_mask** - (Optional) Specify the TCP destination port mask.

**<hex 0x0-0xffff>** - Specify the TCP destination port mask.

**udp** - Specify that the rule applies to UDP traffic.

**src_port_mask** - (Optional) Specify the TCP source port mask.

**<hex 0x0-0xffff>** - Specify the TCP source port mask.

**dst_port_mask** - (Optional) Specify the TCP destination port mask.

**<hex 0x0-0xffff>** - Specify the TCP destination port mask.

**icmp** - Specify that the rule applies to ICMP traffic.

**type** - (Optional) Specify the ICMP packet type.

**code** - (Optional) Specify the ICMP code.

## Restrictions

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

## Example

To create access list profiles:

```
DGS-3620-28SC:admin#create access_profile profile_id 1 profile_name 1 ethernet
vlan source_mac FF-FF-FF-FF-FF-FF destination_mac 00-00-00-FF-FF-FF 802.1p
ethernet_type
Command: create access_profile profile_id 1 profile_name 1 ethernet vlan
source_mac FF-FF-FF-FF-FF-FF destination_mac 00-00-00-FF-FF-FF 802.1p
ethernet_type


Success.
```

```
DGS-3620-28SC:admin#

DGS-3620-28SC:admin#create access_profile profile_id 2 profile_name 2 ip vlan
source_ip_mask 255.255.255.255 destination_ip_mask 255.255.255.0 dscp icmp
Command: create access_profile profile_id 2 profile_name 2 ip vlan
source_ip_mask 255.255.255.255 destination_ip_mask 255.255.255.0 dscp icmp

Success.

DGS-3620-28SC:admin#
```

## 5-2 delete access_profile

### Description

This command is used to delete access list profiles.

### Format

**delete access_profile [profile_id <value 1-6> | profile_name <name 1-32> | all]**

### Parameters

**profile_id** - Specify the index of the access list profile.
**<value 1-6>** - Specify the index of the access list profile. Enter a value between 1 and 6.

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

**all** - Specify the whole access list profile to delete.

### Restrictions

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

### Example

To delete access list profiles:

```
DGS-3620-28SC:admin#delete access_profile profile_id 1
Command: delete access_profile profile_id 1

Success.

DGS-3620-28SC:admin#
```

## 5-3 config access_profile

### Description

This command is used to configure access list entries.

**Note:** Please see the "**Error! Reference source not found. Error! Reference source not found.**" section for a configuration example and further information.

## Format

**config access_profile [profile_id <value 1-6> | profile_name <name 1-32>] [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>}(1) | 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>}}]}(1) | 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>}}(1) | 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 <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>}]}(1)] [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.<br>**<value 1-6>** - Specify the value between 1 and 6. |
| **profile_name** - Specify the profile name.<br>**<name 1-32>** - Specify the profile name. The maximum length is 32 characters. |
| **add access_id** - Specify the index of the access list entry. The lower the access ID, the higher the priority.<br>**auto_assign** - Specify to automatically assign the access ID.<br>**<value 1-256>** - Specify a value between 1 and 256. |
| **ethernet** - Specify an Ethernet access control list rule.<br>**vlan** - Specify the VLAN name.<br>**<vlan_name 32>** -Specify the VLAN name. The maximum length is 32 characters.<br>**vlanid** - Specify the VLAN ID.<br>**<vlanid 1-4094>** - Specify the VLAN ID between 1 and 4094.<br>**mask** - (Optional) Specify the mask.<br>**<hex 0x0-0x0fff>** - Specify the mask.<br>**source_mac** - Specify the source MAC address.<br>**<macaddr>** - Specify the source MAC address.<br>**mask** - (Optional) Specify the mask.<br>**<macmask>** - Specify the mask.<br>**destination_mac** - Specify the destination MAC address.<br>**<macaddr>** - Specify the destination MAC address.<br>**mask** - (Optional) Specify the mask.<br>**<macmask>** - Specify the mask.<br>**802.1p** - Specify the value of the 802.1p priority tag.<br>**<value 0-7>** - Specify the value of the 802.1p priority tag. The priority tag ranges from 1 to 7.<br>**ethernet_type** - Specify the Ethernet type.<br>**<hex 0x0-0xffff>** - Specify the Ethernet type. |

**ip** - Specify an IP access control list rule.

**vlan** - Specify the VLAN name.

**<vlan_name 32>** -Specify the VLAN name. The maximum length is 32 characters.

**vlanid** - Specify the VLAN ID.

**<vlanid 1-4094>** - Specify the VLAN ID between 1 and 4094.

**mask** - (Optional)Specify the mask.

**<hex 0x0-0x0fff>** - Specify the mask.

**source_ip** - Specify an IP source address.

**<ipaddr>** - Specify an IP source address.

**mask** - (Optional) Specify the mask.

**<netmask>** - Specify the mask.

**destination_ip** - Specify an IP destination address.

**<ipaddr>** - Specify an IP destination address.

**mask** - (Optional) Specify the mask.

**<netmask>** - Specify the mask.

**dscp** - Specify the value of DSCP.

**<value 0-63>** - Specify the value of DSCP. The DSCP value ranges from 0 to 63.

**icmp** - Specify the ICMP.

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

**<value 0-255>** - Specify the value between 0 and 255.

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

**<value 0-255>** - Specify the value between 0 and 255.

**igmp** - Specify the IGMP.

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

**<value 0-255>** - Specify the value between 0 and 255.

**tcp** - Specify TCP.

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

**<value 0-65535>** - Specify the value between 0 and 65535.

**mask** - (Optional) Specify the mask.

**<hex 0x0-0xffff>** - Specify the mask.

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

**<value 0-65535>** - Specify the value between 0 and 65535.

**mask** - (Optional) Specify the mask.

**<hex 0x0-0xffff>** - Specify the mask.

**flag** - Specify the TCP flag field value.

**all** – Specify to check all paramenters below.

**urg** - (Optional) Specify Urgent Pointer field significant.

**ack** - (Optional) Specify Acknowledgment field significant.

**psh** - (Optional) Specify Push Function.

**rst** - (Optional) Specify to reset the connection.

**syn** - (Optional) Specify to synchronize sequence numbers.

**fin** - (Optional) No more data from sender.

**udp** - Specify UDP.

**src_port** - (Optional) Specify the UDP source port range.

**<value 0-65535>** - Specify the value between 0 and 65535.

**mask** - (Optional) Specify the mask.

**<hex 0x0-0xffff>** - Specify the mask.

**dst_port** - (Optional) Specify the UDP destination port range.

**<value 0-65535>** - Specify the value between 0 and 65535.

**mask** - (Optional) Specify the mask.

**<hex 0x0-0xffff>** - Specify the mask.

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

**<value 0-255>** - Specify the value 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 4 bytes.

**<hex 0x0-0xffffffff> -** 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 4 bytes.

**mask** - (Optional) Specify the mask.

**<hex 0x0-0xffffffff>** - Specify the mask.

**packet_content -** Specify the packet content for the user defined mask.

**offset_chunk_1** - Specifies the contents of the offset trunk 1 to be monitored.
**<hex 0x0-0xffffffff>** - Enter the contents of the offset trunk 1 to be monitored here.
**mask** - Specifies an additional mask for each field.
**<hex 0x0-0xffffffff>** - Enter the additional mask value used here.
**offset_chunk_2** - Specifies the contents of the offset trunk 2 to be monitored.
**<hex 0x0-0xffffffff>** - Enter the contents of the offset trunk 2 to be monitored here.
**mask** - Specifies an additional mask for each field.
**<hex 0x0-0xffffffff>** - Enter the additional mask value used here.
**offset_chunk_3** - Specifies the contents of the offset trunk 3 to be monitored.
**<hex 0x0-0xffffffff>** - Enter the contents of the offset trunk 3 to be monitored here.
**mask** - Specifies an additional mask for each field.
**<hex 0x0-0xffffffff>** - Enter the additional mask value used here.
**offset_chunk_4** - Specifies the contents of the offset trunk 4 to be monitored.
**<hex 0x0-0xffffffff>** - Enter the contents of the offset trunk 4 to be monitored here.
**mask** - Specifies an additional mask for each field.
**<hex 0x0-0xffffffff>** - Enter the additional mask value used here.

**ipv6** - Specify that the rule applies to IPv6 fields.
**class** - Specify the value of the IPv6 class.
**<value 0-255>** - Specify the value between 0 and 255.
**flowlabel** - Specify the value of the IPv6 flow label.
**<hex 0x0-0xfffff>** - Specify the value of the IPv6 flow label.
**source_ipv6** - Specify the value of the IPv6 source address.
**<ipv6addr>** - Specify the value of the IPv6 source address.
**mask** - (Optional) Specify the mask.
**<ipv6mask>** - Specify the mask.
**destination_ipv6** - Specify the value of the IPv6 destination address.
**<ipv6addr>** - Specify the value of the IPv6 destination address.
**mask** - (Optional) Specify the mask.
**<ipv6mask>** - Specify the mask.
**tcp** - Specify TCP.
**src_port** - (Optional) Specify the TCP source port range.
**<value 0-65535>** - Specify the value between 0 and 65535.
**mask** - (Optional) Specify the mask.
**<hex 0x0-0xffff>** - Specify the mask.
**dst_port** - (Optional) Specify the TCP destination port range.
**<value 0-65535>** - Specify the value between 0 and 65535.
**mask** - (Optional) Specify the mask.
**<hex 0x0-0xffff>** - Specify the mask.
**udp** - Specify UDP.
**src_port** - (Optional) Specify the UDP source port range.
**<value 0-65535>** - Specify the value between 0 and 65535.
**mask** - (Optional) Specify the mask.
**<hex 0x0-0xffff>** - Specify the mask.
**dst_port** - (Optional) Specify the UDP destination port range.
**<value 0-65535>** - Specify the value between 0 and 65535.
**mask** - Specify the mask.
**<hex 0x0-0xffff>** - Specify the mask.
**icmp** - Specifies that the rule applies to the value of ICMP traffic.
**type** - Specifies that the rule applies to the value of ICMP type traffic.
**<value 0-255>** - Enter the ICMP type value used here. This value must be between 0 and 255.
**code** - Specifies that the rule applies to the value of ICMP code traffic.
**<value 0-255>** - Enter the ICMP code value used here. This value must be between 0 and 255.

**port** - The access profile rule may be defined for each port on the switch. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon.
**<portlist>** - Specify a list of ports.
**all** - Specify that the access rule will apply to all ports.

**vlan_based** - Specify the VLAN-based ACL rule. There are two conditions: this rule will apply to

all ports and packets must belong to the configured VLAN. It can be specified by VLAN name or VLAN ID.
**vlan** - Specify the VLAN name.
**<vlan_name 32>** - Specify the VLAN name. The maximum length is 32 characters.
**vlan_id** - Specify the VLAN ID.
**<vlanid 1-4094>** - Specify the VLAN ID between 1 and 4094.

**permit** - Specify the packets that match the access profile are permit by the switch.

**priority** - (Optional) Specify the packets that match the access profile are remap the 802.1p priority tag field by the switch.
**<value 0-7>** - Specify the value between 0 and 7.

**replace_priority** - (Optional) Specify the packets that match the access profile remarking the 802.1p priority tag field by the switch.
**replace_dscp_with** - (Optional) Specify the DSCP of the packets that match the access profile are modified according to the value.
**<value 0-63>** - Specify the value 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>** - Specify the value between 0 and 7.

**counter** - (Optional) Specifies whether the ACL counter feature will be enabled or disabled.
**enable** - Specify whether the ACL counter feature is enabled. 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.
**disable** - Specify whether the ACL counter feature is disabled. The default option is disabled.

**mirror** - Specify that packets matching the access profile are copied to the mirror port.

**group_id** - Specifies the group ID used.
**<value 1-4>** - Enter the group ID used here. This value must be between 1 and 4.

**deny** - Specify the packets that match the access profile are filtered by the switch.

**time_range** - (Optional) Specify the name of this time range entry.
**<range_name 32>** - Specify the name of this time range entry. The maximum length is 32 characters.

**delete access_id** - Specify to delete the access ID.
**<value 1-256>** - Specify the value between 1 and 256.

## Restrictions

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

## Example

To configure an access list entry:

```
DGS-3620-28SC:admin#config 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 port 1 permit
Command: config 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 port 1 permit


Success.


DGS-3620-28SC:admin#
```

## 5-4 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.<br>**<value 1-6>** - Specify the profile ID between 1 and 6. | |
| **profile_name** - (Optional) Specify the name of the access list profile.<br>**<name 1-32>** - Specify the profile name between 1 and 32. | |

### Restrictions

None.

### Example

To display the current access list table:

```
DGS-3620-28SC:admin#show access_profile
Command: show access_profile

Access Profile Table

Total User Set Rule Entries : 3
Total Used HW Entries       : 19
Total Available HW Entries  : 1005
===============================================================================
=
Profile ID: 1      Profile Name: 1                     Type: Ethernet
Mask on
    VLAN ID   : 0xFF
    Source MAC: FF-FF-FF-FF-FF-00
    802.1p
Available HW Entries: 254
-------------------------------------------------------------------------------
--
Rule ID : 1       Ports: 1-10
Match on:
   VLAN ID    : 2    Mask : 0xFFF
   Source MAC : 00-01-02-03-04-00
Action:
   Permit
   Replaced Priority to 2
   Replace DSCP to 33

Matched Count: 0 packets
-------------------------------------------------------------------------------
```

```
--
Rule ID : 256 (auto assign) Ports: -
Match on:
   VLAN ID    : 8
   Source MAC : 00-01-02-03-04-00
   802.1p
Action:
   Deny
===============================================================================
====
Profile ID: 3      Profile Name: 3                     Type: IPv4
Mask on
    Source IP : 255.255.255.0
    TCP
    Source Port : 0x00FF
Available HW Entries: 254
-------------------------------------------------------------------------------
--
Rule ID : 4      Ports: 1-28
Match on:
   Source IP : 192.168.1.0
   TCP
Source Port: 210   Mask : 0x0FFF
Action:
   Mirror
===============================================================================
====
Profile ID: 2  Profile Name: IMPBv4

Mask
   Source MAC : FF-FF-FF-FF-FF-FF
   Source IP : 255.255.255.255
Consumed HW Entries: 2
-------------------------------------------------------------------------------
---
Rule ID : 1      Ports: 1
 Match on
    Source MAC : 00-05-04-03-02-01    Mask : FF-FF-FF-FF-FF-FF
    Source Ip : 10.10.10.1            Mask : 255.255.255.255
 Action:
    Permit
-------------------------------------------------------------------------------
----
Rule ID : 2    Ports: 1
Match on
   Any
Action:
   Deny

===============================================================================
===
Profile ID: 3    Profile Name: VLAN Counter
Consumed HW Entries: 9
```

```
Profile ID: 4    Profile Name: System
Consumed HW Entries: 4

DGS-3620-28SC:admin#
```

**Note:** “Total User Set Entries” indicates the total number of ACL rules created by the user. “Total Used HW Entries” indicates the total number of hardware entries used in the device. “Available HW Entries” indicates the total number of available hardware entries in the device.

To display an access profile that supports an entry mask for each rule:

```
DGS-3620-28SC: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-3620-28SC:admin#
```

To display the packet content mask profile for the profile with an ID of 5:

```
DGS-3620-28SC:admin#show access_profile profile_id 5
Command: show access_profile profile_id 5

Access Profile Table

=============================================================================
Profile ID: 5     Profile name: 5  Type: User Defined

MASK on
    offset_chunk_1 : 0      value : 0x0000FFFF

Available HW Entries : 256
=============================================================================

DGS-3620-28SC:admin#
```

## 5-5 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 SNTP time or configured time. If this time is not available, then the time range will not be met.

### Format

**config time_range <range_name 32> [ hours start_time < hh:mm:ss> end_time< hh:mm:ss> weekdays <daylist> | delete]**

### Parameters

**<range_name 32>** - Specify the name of the time range settings.

**hours start_time** - Specify the starting time in a day. (24-hr time). For example, 19:00 means 7PM. 19 is also acceptable. The start_time must be smaller than the end_time.
**< hh:mm:ss>** - Specify the time.

**end_time** - Specify the ending time in a day. (24-hr time)
**< hh:mm:ss>** - Specify the time.

**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. For example, mon-fri (Monday to Friday)
sun, mon, fri (Sunday, Monday, and Friday)
**<daylist>** - Specify a list of days.

**delete** - Delete a time range profile. When a time range profile has been associated with ACL entries, the deletion of this time range profile will fail.

### Restrictions

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

### Example

To configure the range of time to activate a function on the switch:

```
DGS-3620-28SC:admin#config time_range testdaily hours start_time 12:0:0
end_time 13:0:0 weekdays mon,fri
Command: config time_range testdaily hours start_time 12:0:0 end_time 13:0:0
weekdays mon,fri


Success.


DGS-3620-28SC:admin#
```

## 5-6 show time_range

### Description

This command is used to display current time range settings.

### Format

**show time_range**

### Parameters

None.

### Restrictions

None.

### Example

To display current time range setting:

```
DGS-3620-28SC:admin#show time_range
Command: show time_range

Time Range Information
-------------------------
Range Name   :  testdaily
Weekdays     :  Mon,Fri
Start Time   :  12:00:00
End Time     :  13:00:00

Total Entries :1

DGS-3620-28SC:admin#
```

## 5-7 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-3620-28SC: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 profile_id 2
config access_profile profile_id 2 add access_id 1 ip source_ip 10.10.10.10
port 2 deny

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

DGS-3620-28SC:admin#
```

## 5-8 delete cpu access_profile

### Description

This command is used to delete CPU access list profiles.

### Format

**delete cpu access_profile [profile_id <value 1-5> | all]**

### Parameters

| |
|---|
| **profile_id** - Specify the index of the access list profile.<br>**<value 1-5>** - Specify the value between 1 and 5. |
| **all** - Specify to delete all the access list profiles. |

### Restrictions

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

### Example

To delete access list rules:

```
DGS-3620-28SC:admin#delete cpu access_profile profile_id 3
Command: delete cpu access_profile profile_id 3

Success.

DGS-3620-28SC:admin#
```

## 5-9 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}(1) | 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>}]}(1) | 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>}(1) | ipv6 {class | flowlabel | source_ipv6_mask <ipv6mask> | destination_ipv6_mask <ipv6mask>}(1)]**

### Parameters

**<value 1-5>** - Specify a value between 1 and 5.

**ethernet** - Specify an Ethernet CPU access control list rule.
- **vlan** - Specify a VLAN mask.
- **source_mac** - Specify the source MAC mask.
  - **<macmask000000000000-ffffffffffff>** - Specify the source MAC mask.
- **destination_mac** - Specify the destination MAC mask.
  - **<macmask 000000000000-ffffffffffff>** - Specify the destination MAC mask.
- **802.1p** - Specify the 802.1p priority tag mask.
- **ethernet_type** - Specify the Ethernet type mask.

**ip** - Specify an IP CPU access control list rule.
- **vlan** - Specify a VLAN mask.
- **source_ip_mask** - Specify an IP source submask.
  - **<netmask>** - Specify an IP source submask.
- **destination_ip_mask** - Specify an IP destination submask.
  - **<netmask>** - Specify an IP destination submask.
- **dscp** - Specify the DSCP mask.
- **icmp** - Specify that the rule applies to ICMP traffic.
  - **type** - (Optional) Specify the ICMP packet type.
  - **code** - (Optional) Specify the ICMP code.
- **igmp** - Specify that the rule applies to IGMP traffic.
  - **type** - (Optional) Specify the IGMP packet type.
- **tcp** - Specify that the rule applies to TCP traffic.
  - **src_port_mask** - (Optional) Specify the TCP source port mask.
    - **<hex 0x0-0xffff>** - Specify the TCP source port mask.
  - **dst_port_mask** - (Optional) Specify the TCP destination port mask.
    - **<hex 0x0-0xffff>** - Specify the TCP destination port mask.
- **flag_mask** - (Optional) Specify the TCP flag field mask.
  - **all** – Specify to check all paramenters below.
  - **urg** - (Optional) Specify Urgent Pointer field significant.
  - **ack** - (Optional) Specify Acknowledgment field significant.
  - **psh** - (Optional) Specify Push Function.
  - **rst** - (Optional) Specify to reset the connection.

**syn** - (Optional) Specify to synchronize sequence numbers.
**fin** - (Optional) No more data from sender.
**udp** - Specify that the rule applies to UDP traffic.
**src_port_mask** - (Optional) Specify the UDP source port mask.
**<hex 0x0-0xffff>** - Specify the UDP source port mask.
**dst_port_mask** - (Optional) Specify the UDP destination port mask.
**<hex 0x0-0xffff>** - Specify the UDP destination port mask.
**protocol_id_mask** - Specify that the rule applies to the IP protocol ID traffic.
**<hex 0x0-0xff>** - Specify that the rule applies to the IP protocol ID traffic.
**user_define_mask** - (Optional) Specify the L4 part mask
**<hex 0x0-0xffffffff>** - Specify the L4 part mask

**packet_content_mask** - Specify the packet content mask.
**offset_0-15** - Specify the mask for packet bytes 0-15.
**<hex 0x0-0xffffffff>** - Specify the mask for packet bytes 0-3.
**<hex 0x0-0xffffffff>** - Specify the mask for packet bytes 4-7.
**<hex 0x0-0xffffffff>** - Specify the mask for packet bytes 8-11.
**<hex 0x0-0xffffffff>** - Specify the mask for packet bytes 12-15.
**offset_16-31** - Specify the mask for packet bytes 16-31.
**<hex 0x0-0xffffffff>** - Specify the mask for packet bytes 16-19.
**<hex 0x0-0xffffffff>** - Specify the mask for packet bytes 20-23.
**<hex 0x0-0xffffffff>** - Specify the mask for packet bytes 24-27.
**<hex 0x0-0xffffffff>** - Specify the mask for packet bytes 28-31.
**offset_32-47** - Specify the mask for packet bytes 32-47
**<hex 0x0-0xffffffff>** - Specify the mask for packet bytes 32-35.
**<hex 0x0-0xffffffff>** - Specify the mask for packet bytes 36-39.
**<hex 0x0-0xffffffff>** - Specify the mask for packet bytes 40-43.
**<hex 0x0-0xffffffff>** - Specify the mask for packet bytes 44-47.
**offset_48-63** - Specify the mask for packet bytes 48-63.
**<hex 0x0-0xffffffff>** - Specify the mask for packet bytes 48-51.
**<hex 0x0-0xffffffff>** - Specify the mask for packet bytes 52-55.
**<hex 0x0-0xffffffff>** - Specify the mask for packet bytes 56-59.
**<hex 0x0-0xffffffff>** - Specify the mask for packet bytes 60-63.
**offset_64-79** - Specify the mask for packet bytes 64-79.
**<hex 0x0-0xffffffff>** - Specify the mask for packet bytes 64-67.
**<hex 0x0-0xffffffff>** - Specify the mask for packet bytes 68-71.
**<hex 0x0-0xffffffff>** - Specify the mask for packet bytes 72-75.
**<hex 0x0-0xffffffff>** - Specify the mask for packet bytes 76-79.

**ipv6** - Specify the IPv6 mask.
**class** - Specify the IPv6 class mask.
**flowlabel** - Specify the IPv6 flow label mask.
**source_ipv6_mask** - Specify the IPv6 source IP mask.
**<ipv6mask>** - Specify the IPv6 source IP mask.
**destination_ipv6_mask** - Specify the IPv6 destination IP mask.
**<ipv6mask>** - Specify the IPv6 destination IP mask.

## Restrictions

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

## Example

To create CPU access list profiles:

```
DGS-3620-28SC:admin#create cpu access_profile profile_id 1 ethernet vlan
Command: create cpu access_profile profile_id 1 ethernet vlan

Success.
```

```
DGS-3620-28SC:admin#create cpu access_profile profile_id 2 ip source_ip_mask
255.255.255.255
Command: create cpu access_profile profile_id 2 ip source_ip_mask
255.255.255.25
5

Success.

DGS-3620-28SC:admin#
```

## 5-10 config cpu access_profile profile_id

### Description

This command is used to configure CPU access list entries.

### 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>** - Specify the index of the CPU access list profile.

**add access_id** - Specify the index of an access list entry to add. The range of this value is 1 to 100.
- **auto_assign** - Specify to automatically assign the access ID.
- **<value 1-100>** - Specify an access ID between 1 and 100.

**ethernet** - Specify an Ethernet CPU access control list rule.
- **vlan** - Specify the VLAN name.
  - **<vlan_name 32>** -Specify the VLAN name. The maximum length is 32 characters.
- **vlanid** - Specify the VLAN ID.
  - **<vlanid 1-4094>** - Specify the VLAN ID between 1 and 4094.
- **source_mac** - Specify the source MAC address.
  - **<macaddr>** - Specify the source MAC address.
- **destination_mac** - Specify the destination MAC address.
  - **<macaddr>** - Specify the destination MAC address.
- **802.1p** - Specify the value of the 802.1p priority tag.
  - **<value 0-7>** - Specify the value of the 802.1p priority tag. The priority tag ranges from 1 to 7.

**ethernet_type** - Specify the Ethernet type.

**<hex 0x0-0xffff>** - Specify the Ethernet type.

**ip** - Specify an IP access control list rule.

**vlan** - Specify the VLAN name.

**<vlan_name 32>** -Specify the VLAN name. The maximum length is 32 characters.

**vlanid** - Specify the VLAN ID.

**<vlanid 1-4094>** - Specify the VLAN ID between 1 and 4094.

**source_ip** - Specify an IP source address.

**<ipaddr>** - Specify an IP source address.

**destination_ip** - Specify an IP destination address.

**<ipaddr>** - Specify an IP destination address.

**dscp** - Specify the value of DSCP.

**<value 0-63>** - Specify the value of DSCP. The DSCP value ranges from 0 to 63.

**icmp** - Specify the ICMP.

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

**<value 0-255>** - Specify the value between 0 and 255.

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

**<value 0-255>** - Specify the value between 0 and 255.

**igmp** - Specify the IGMP.

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

**<value 0-255>** - Specify the value between 0 and 255.

**tcp** - Specify TCP.

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

**<value 0-65535>** - Specify the value between 0 and 65535.

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

**<value 0-65535>** - Specify the value between 0 and 65535.

**flag** - Specify the TCP flag field value.

**all** – Specify to check all paramenters below.

**urg** - (Optional) Specify Urgent Pointer field significant.

**ack** - (Optional) Specify Acknowledgment field significant.

**psh** - (Optional) Specify Push Function.

**rst** - (Optional) Specify to reset the connection.

**syn** - (Optional) Specify to synchronize sequence numbers.

**fin** - (Optional) No more data from sender.

**udp** - Specify UDP.

**src_port** - (Optional) Specify the UDP source port range.

**<value 0-65535>** - Specify the value between 0 and 65535.

**dst_port** - (Optional) Specify the UDP destination port range.

**<value 0-65535>** - Specify the value between 0 and 65535.

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

**<value 0-255>** - Specify the value 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 4 bytes.

**<hex 0x0-0xffffffff>** - 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 4 bytes.

**packet_content** - Specifies that the access control list rule will be set to packet content.

**offset_0-15** - Specify the mask for packet bytes 0-15.

**<hex 0x0-0xffffffff>** - Specify the mask for packet bytes 0-3.

**<hex 0x0-0xffffffff>** - Specify the mask for packet bytes 4-7.

**<hex 0x0-0xffffffff>** - Specify the mask for packet bytes 8-11.

**<hex 0x0-0xffffffff>** - Specify the mask for packet bytes 12-15.

**offset_16-31** - Specify the mask for packet bytes 16-31.

**<hex 0x0-0xffffffff>** - Specify the mask for packet bytes 16-19.

**<hex 0x0-0xffffffff>** - Specify the mask for packet bytes 20-23.

**<hex 0x0-0xffffffff>** - Specify the mask for packet bytes 24-27.

**<hex 0x0-0xffffffff>** - Specify the mask for packet bytes 28-31.

**offset_32-47** - Specify the mask for packet bytes 32-47

**<hex 0x0-0xffffffff>** - Specify the mask for packet bytes 32-35.

**<hex 0x0-0xffffffff>** - Specify the mask for packet bytes 36-39.

**<hex 0x0-0xffffffff>** - Specify the mask for packet bytes 40-43.

**<hex 0x0-0xffffffff>** - Specify the mask for packet bytes 44-47.
**offset_48-63** - Specify the mask for packet bytes 48-63.
**<hex 0x0-0xffffffff>** - Specify the mask for packet bytes 48-51.
**<hex 0x0-0xffffffff>** - Specify the mask for packet bytes 52-55.
**<hex 0x0-0xffffffff>** - Specify the mask for packet bytes 56-59.
**<hex 0x0-0xffffffff>** - Specify the mask for packet bytes 60-63.
**offset_64-79** - Specify the mask for packet bytes 64-79.
**<hex 0x0-0xffffffff>** - Specify the mask for packet bytes 64-67.
**<hex 0x0-0xffffffff>** - Specify the mask for packet bytes 68-71.
**<hex 0x0-0xffffffff>** - Specify the mask for packet bytes 72-75.
**<hex 0x0-0xffffffff>** - Specify the mask for packet bytes 76-79.

**ipv6** - Specify that the rule applies to IPv6 fields.
**class** - Specify the value of the IPv6 class.
**<value 0-255>** - Specify the value between 0 and 255.
**flowlabel** - Specify the value of the IPv6 flow label.
**<hex 0x0-0xfffff>** - Specify the value of the IPv6 flow label.
**source_ipv6** - Specify the value of the IPv6 source address.
**<ipv6addr>** - Specify the value of the IPv6 source address.
**destination_ipv6** - Specify the value of the IPv6 destination address.
**<ipv6addr>** - Specify the value of the IPv6 destination address.

**port** - Specify the port number to configure.
**<portlist>** - Specify a list of ports.
**all** - Specify to configure all ports.

**permit** - Specify the packets that match the access profile are permitted by the switch.
**deny** - Specify the packets that match the access profile are filtered by the switch.

**time_range** - (Optional) Specify the name of this time range entry.
**<range_name 32>** - Specify the name of this time range entry. The maximum length is 32 characters.

**delete access_id** - Specify to delete the access ID.
**<value 1-100>** - Specify the value between 1 and 100.

### Restrictions

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

### Example

To configure access list entry:

```
DGS-3620-28SC:admin#config cpu access_profile profile_id 1 add access_id 1
ethernet vlan default port 1-3 deny
Command: config cpu access_profile profile_id 1 add access_id 1 ethernet vlan
default port 1-3 deny


Success.


DGS-3620-28SC:admin#
```

## 5-11 show cpu access_profile

### Description

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

### Format

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

## Parameters

**profile_id** - (Optional) Specify the index of an access list profile.
**<value 1-5>** - Specify value between 1 and 5.

## Restrictions

None.

## Example

To display the current CPU access list table:

```
DGS-3620-28SC:admin#show cpu access_profile
Command: show cpu access_profile

CPU Interface Filtering State: Disabled

CPU Interface Access Profile Table

Total Unused Rule Entries : 93
Total Used Rule Entries   : 7

===============================================================================
=
Profile ID: 1     Type: IPv4

MASK on
    Dest IP     : 255.255.255.255
    IGMP

Unused Rule Entries: 93
-------------------------------------------------------------------------------
-
Rule ID : 1       Ports: 2

Match on
    IGMP

Action:
    Deny
===============================================================================
=

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

MASK on
    Dest IP     : 255.255.0.0

Unused Rule Entries: 93
-------------------------------------------------------------------------------
```

```
-
Rule ID : 1       Ports: 1-28
Time Range: ben

Match on
    Dest IP     : 10.90.90.12      Mask : 255.255.255.255

Action:
    Deny
===============================================================================
=

===============================================================================
=
Profile ID: 4     Type: IPv6

MASK on
    UDP
    Source Port      : 0xFFFF

Unused Rule Entries: 93
-------------------------------------------------------------------------------
-
Rule ID : 99   (auto assign)    Ports: 1

Match on
    UDP
    Source Port : 1234

Action:
    Permit
-------------------------------------------------------------------------------
-
Rule ID : 100  (auto assign)    Ports: 1

Match on
    UDP
    Source Port : 0      Mask : 0x0

Action:
    Permit
===============================================================================
=

===============================================================================
=
Profile ID: 5     Type: IPv6

MASK on
    Class
    Flow Label
    Source IPv6 Addr : FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
    Dest IPv6 Addr   : FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
    TCP
    Source Port      : 0xFFFF
    Dest Port        : 0xFFFF

Unused Rule Entries: 93
-------------------------------------------------------------------------------
-
Rule ID : 1       Ports: 1

Match on
    Class       : 123
    Flow Label  : 0x12345
    Source IPv6 : 2001::
           Mask : FFFF::
    Dest IPv6   : 2002::
         Mask   : FFFF::
    TCP
    Source Port : 1024
    Dest Port   : 0      Mask : 0x0

Action:
    Permit
-------------------------------------------------------------------------------
-
Rule ID : 100  (auto assign)    Ports: 1

Match on
    Class       : 127
    Flow Label  : 0x67890

Action:
    Deny
===============================================================================
=

===============================================================================
=
Profile ID: 6     Type: User Defined

MASK on
    Offset  0-15 : 0xFFFFFFFF 0xFFFFFFFF 0xFFFFFFFF 0xFFFFFFFF

Unused Rule Entries: 93
-------------------------------------------------------------------------------
-
Rule ID : 1       Ports: 1

Match on
    Offset  0-15 : 0x12345678 0x12345678 0x12345678 0x12345678

Action:
    Permit
===============================================================================
=
DGS-3620-28SC:admin#
```

## 5-12 enable cpu_interface_filtering

### Description

This command is used to enable CPU interface filtering.

### Format

**enable cpu_interface_filtering**

### Parameters

None.

### Restrictions

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

### Example

To enable CPU interface filtering:

```
DGS-3620-28SC:admin#enable cpu_interface_filtering
Command: enable cpu_interface_filtering

Success.

DGS-3620-28SC:admin#
```

## 5-13 disable cpu_interface_filtering

### Description

This command is used to disable CPU interface filtering.

### Format

**disable cpu_interface_filtering**

### Parameters

None.

### Restrictions

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

### Example

To disable CPU interface filtering:

```
DGS-3620-28SC:admin#disable cpu_interface_filtering
Command: disable cpu_interface_filtering

Success.

DGS-3620-28SC:admin#
```

## 5-14 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 remarked DSCP, 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. 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. The color mapping for both “single rate three color” and “two rate three color” mode follow RFC 2697 and RFC 2698 in the color-blind situation.

### 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_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 <value 0-63>} | drop] {counter [enable | disable]} | delete]**

### Parameters

| |
|---|
| **profile_id** - Specify the index of the access list profile.<br>**<value 1-6>** - Specify the value between 1 and 6. |
| **profile_name** - Specify the name of the profile.<br>**<name 1-32>** - Specify the name of the profile. The maximum length is 32 characters. |
| **access_id** - Specify the index of the access list entry.<br>**<value 1-256>** - Specify the value between 1 and 256. |

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

**<value 0-1048576>**- Specify the value between 0 and 1048576.

**burst_size** - (Optional) Specify the burst size for the single rate two color mode. The unit is Kbyte.

**<value 0-131072>** - Specify the value between 0 and 131072.

**rate_exceed** - Specify the action for packets that exceed the committed rate in single rate two color mode. The action can be specified as one of the following:

**drop_packet** - Drop the packet immediately.

**remark_dscp** - Mark the packet with a specified DSCP. The packet is set to drop for packets with a high precedence.

**<value 0-63>** - Specify the value between 0 and 63.

**tr_tcm** - Specify the “two-rate three-color mode.”

**cir** -Specify the Committed Information Rate. The unit is Kbps. CIR should always be equal or less than PIR.

**<value 0-1048576>** - Specify the value between 0 and 1048576.

**cbs** - (Optional) Specify the Committed Burst Size. The unit is Kbyte.

**<value 0-131072>** - Specify the value between 0 and 131072.

**pir** - Specify the Peak information Rate. The unit is Kbps. PIR should always be equal to or greater than CIR.

**<value 0-1048576>** - Specify the value between 0 and 1048576.

**pbs** - (Optional) Specify the Peak Burst Size. The unit is Kbyte.

**<value 0-131072>** - Specify the value between 0 and 131072.

**color_blind** - Specifies the meter mode as color-blind. The default is color-blind mode.

**color_aware** - Specifies the meter mode as color-aware. The final color of the packet is determined by the initial color of the packet and the metering result.

**conform** - (Optional) This field denotes the green packet flow. Green packet flows may have their DSCP field rewritten to a value stated in this field. Users may also choose to count green packets by using counter parameter.

**permit** - Enter this parameter to allow packet flows that are in the green flow.

**replace_dscp** - Packets that are in the green flow may have their DSCP field rewritten using this parameter and entering the DSCP value to replace.

**<value 0-63>** - Specify the value between 0 and 63.

**counter** - (Optional) Use this parameter to enable or disable the packet counter for the specified ACL entry in the green flow.

**enable** - Enable the packet counter for the specified ACL entry in the green flow.

**disable** - Disable the packet counter for the specified ACL entry in the green flow.

**exceed** - This field denotes the yellow packet flow. Yellow packet flows may have excess packets permitted through or dropped. Users may replace the DSCP field of these packets by checking its radio button and entering a new DSCP value in the allotted field.

**permit** - Enter this parameter to allow packet flows that are in the yellow flow.

**replace_dscp** - Specifies to change the DSCP of the packet.

**<value 0-63>** - Enter the replacement DSCP of the packet here. This value must be between 0 and 63.

**drop** - Enter this parameter to drop packets that are in the yellow flow.

**counter** - (Optional) Use this parameter to enable or disable the packet counter for the specified ACL entry in the green flow.

**enable** - Enable the packet counter for the specified ACL entry in the green flow.

**disable** - Disable the packet counter for the specified ACL entry in the green flow.

**violate** - This field denotes the red packet flow. Red packet flows may have excess packets permitted through or dropped. Users may replace the DSCP field of these packets by checking its radio button and entering a new DSCP value in the allotted field.

**permit** - Enter this parameter to allow packet flows that are in the red flow.

**replace_dscp** - Specifies to change the DSCP of the packet.

**<value 0-63>** - Enter the replacement DSCP of the packet here. This value must be between 0 and 63.

**drop** - Enter this parameter to drop packets that are in the red flow.

**counter** - (Optional) Use this parameter to enable or disable the packet counter for the specified ACL entry in the green flow.

**enable** - Enable the packet counter for the specified ACL entry in the green flow.

| |
|---|
| **disable** - Disable the packet counter for the specified ACL entry in the green flow. |
| **sr_tcm** - Specify the "single-rate three-color mode".<br>**cir** -Specify the Committed Information Rate. The unit is in Kbps.<br>**<value 0-1048576>** - Specify the value between 0 and 1048576.<br>**cbs** - Specify the Committed Burst Size. The unit is in Kbyte.<br>**<value 0-131072>** - Specify the value between 0 and 131072.<br>**ebs** - Specify the Excess Burst Size. The unit is Kbyte.<br>**<value 0-131072>** - Specify the value between 0 and 131072. |
| **color_blind** - Specifies the meter mode as color-blind. The default is color-blind mode.<br>**color_aware** - Specifies the meter mode as color-aware. The final color of the packet is determined by the initial color of the packet and the metering result. |
| **conform** - (Optional) This field denotes the green packet flow. Green packet flows may have their DSCP field rewritten to a value stated in this field. Users may also choose to count green packets by using counter parameter.<br>**permit** - Enter this parameter to allow packet flows that are in the green flow.<br>**replace_dscp** - Packets that are in the green flow may have their DSCP field rewritten using this parameter and entering the DSCP value to replace.<br>**<value 0-63>** - Specify the value between 0 and 63.<br>**counter** - (Optional) Use this parameter to enable or disable the packet counter for the specified ACL entry in the green flow.<br>**enable** - Enable the packet counter for the specified ACL entry in the green flow.<br>**disable** - Disable the packet counter for the specified ACL entry in the green flow. |
| **exceed** - This field denotes the yellow packet flow. Yellow packet flows may have excess packets permitted through or dropped. Users may replace the DSCP field of these packets by checking its radio button and entering a new DSCP value in the allotted field.<br>**permit** - Enter this parameter to allow packet flows that are in the yellow flow.<br>**replace_dscp** - Specifies to change the DSCP of the packet.<br>**<value 0-63>** - Enter the replacement DSCP of the packet here. This value must be between 0 and 63.<br>**drop** - Enter this parameter to drop packets that are in the yellow flow.<br>**counter** - (Optional) Use this parameter to enable or disable the packet counter for the specified ACL entry in the green flow.<br>**enable** - Enable the packet counter for the specified ACL entry in the green flow.<br>**disable** - Disable the packet counter for the specified ACL entry in the green flow. |
| **violate** - This field denotes the red packet flow. Red packet flows may have excess packets permitted through or dropped. Users may replace the DSCP field of these packets by checking its radio button and entering a new DSCP value in the allotted field.<br>**permit** - Enter this parameter to allow packet flows that are in the red flow.<br>**replace_dscp** - Specifies to change the DSCP of the packet.<br>**<value 0-63>** - Enter the replacement DSCP of the packet here. This value must be between 0 and 63.<br>**drop** - Enter this parameter to drop packets that are in the red flow.<br>**counter** - (Optional) Use this parameter to enable or disable the packet counter for the specified ACL entry in the green flow.<br>**enable** - Enable the packet counter for the specified ACL entry in the green flow.<br>**disable** - Disable the packet counter for the specified ACL entry in the green flow.<br>**delete** - Use this parameter to delete the specified flow meter. |

## Restrictions

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

## Example

To configure a two rate, three color flow meter:

```
DGS-3620-28SC:admin#config flow_meter profile_id 1 access_id 1 tr_tcm cir 1000
cbs 200 pir 2000 pbs 200 conform replace_dscp 21 exceed drop violate permit
Command: config flow_meter profile_id 1 access_id 1 tr_tcm cir 1000 cbs 200 pir
```

```
2000 pbs 200 conform replace_dscp 21 exceed drop violate permit

Success.

DGS-3620-28SC:admin#
```

To replace DSCP action changed to perform on conform (green) and unconform (yellow and red) packets:

```
DGS-3620-28SC:admin# config flow_meter profile_id 1 access_id 1 tr_tcm cir 1000
cbs 200 pir 2000 pbs 200 exceed permit replace_dscp 21 violate permit
replace_dscp 21
Command: config flow_meter profile_id 1 access_id 1 tr_tcm cir 1000 cbs 200 pir
2000 pbs 200 exceed permit replace_dscp 21 violate permit replace_dscp 21

Success.

DGS-3620-28SC:admin#
```

## 5-15 show flow_meter

### Description

This command is used to display the flow meter table.

### 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>** - Specify the profile ID. Enter a value between 1 and 6.

**profile_name** - (Optional) Specify the name of the profile.
**<name 1-32>** - Specify the name of the profile. The maximum length is 32 characters.

**access_id** - (Optional) Specify the access ID.
**<value 1-256>** - Specify the access ID. Enter a value between 1 and 256.

### Restrictions

None.

### Example

To display the flow meter configuration:

```
DGS-3620-28SC: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):200      PIR(Kbps):2000     PBS(Kbyte):200
Action:
      Conform : Permit                        Counter: Disabled
       Exceed : Permit     Replace DSCP: 21   Counter: Disabled
      Violate : Permit     Replace DSCP: 21   Counter: Disabled
------------------------------------------------------------------------------

Total Entries: 1

DGS-3620-28SC:admin#
```

# Chapter 6 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}]}]

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

**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>]

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

**show current_config egress_access_profile**

**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 <value 0-63>} | drop] {counter [enable | disable]} | delete]

**show egress_flow_meter** {[profile_id <value 1-4> | profile_name <name 1-32>] {access_id <value1-128>}}

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

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

| |
|---|
| **delete port_group** [id <value 1-64> \| name <name 16>] |
| **show port_group** {id <value 1-64> \| name <name 16>} |

## 6-1 create egress_access_profile

### 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

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

**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** - Specifies this is an Ethernet mask.
**vlan** - (Optional) Specifies a VLAN mask.
**<hex 0x0-0x0fff>** - Enter the VLAN mask used here.
**source_mac** - (Optional) Specifies the source MAC mask.
**<macmask 000000000000-ffffffffffff>** - Enter the source MAC mask used here.
**destination_mac** - (Optional) Specifies the destination MAC mask.
**<macmask 000000000000-ffffffffffff>** - Enter the destination MAC mask used here.
**802.1p** - (Optional) Specifies 802.1p priority tag mask.
**ethernet_type** - (Optional) Specifies the Ethernet type mask.

**ip** - Specifies this is an IPv4 mask.
**vlan** - (Optional) Specifies a VLAN mask.
**<hex 0x0-0x0fff>** - Enter the VLAN mask used here.
**source_ip_mask** - (Optional) Specifies a source IP address mask.
**<netmask>** - Enter the source network mask used here.
**destination_ip_mask** - (Optional) Specifies a destination IP address mask.
**<netmask>** - Enter the destination network mask used here.
**dscp** - (Optional) Specifies the DSCP mask.
**icmp** - (Optional) Specifies that the rule applies to ICMP traffic.
**type** - Specifies the type of ICMP traffic.
**code** - Specifies the code of ICMP traffic.
**igmp** - (Optional) Specifies that the rule applies to IGMP traffic.
**type** - Specifies the type of IGMP traffic.
**tcp** - (Optional) Specifies that the rule applies to TCP traffic.

**src_port_mask** - Specifies the TCP source port mask.
**<hex 0x0-0xffff>** - Enter the TCP source port mask value here.
**dst_port_mask** - Specifies the TCP destination port mask.
**<hex 0x0-0xffff>** - Enter the TCP source port mask value here.
**flag_mask** - (Optional) Specifies the TCP flag field mask.
**all** - Specifies that the TCP flag field mask will be set to 'all'.
**urg** - Specifies that the TCP flag field mask will be set to 'urg'.
**ack** - Specifies that the TCP flag field mask will be set to 'ack'.
**psh** - Specifies that the TCP flag field mask will be set to 'psh'.
**rst** - Specifies that the TCP flag field mask will be set to 'rst'.
**syn** - Specifies that the TCP flag field mask will be set to 'syn'.
**fin** - Specifies that the TCP flag field mask will be set to 'fin'.
**udp** - (Optional) Specifies that the rule applies to UDP traffic.
**src_port_mask** - Specifies the UDP source port mask.
**<hex 0x0-0xffff>** - Enter the UDP source port mask value here.
**dst_port_mask** - Specifies the UDP destination port mask.
**<hex 0x0-0xffff>** - Enter the UDP destination port mask value here.
**protocod_id_mask** - (Optional) Specifies that the rule applies to IP protocol ID traffic.
**<hex 0x0-0xff>** - Enter the protocol ID mask value here.
**user_define_mask** - (Optional) Specifies that the rule applies to the IP protocol ID, and that the mask option behind the IP header length is 20 bytes.
**<hex 0x0-0xffffffff>** - Enter the user-defined mask value here.

**ipv6** - (Optional) Specifies this is an IPv6 mask.
**class** - (Optional) Specifies the IPv6 class.
**source_ipv6_mask** - (Optional) Specifies an IPv6 source sub-mask.
**<ipv6mask>** - Enter the IPv6 source sub-mask value here.
**destination_ipv6_mask** - Specifies an IPv6 destination sub-mask.
**<ipv6mask>** - Enter the IPv6 destination sub-mask value here.
**tcp** - (Optional) Specifies that the following parameter are application to the TCP configuration.
**src_port_mask** - Specifies an IPv6 Layer 4 TCP source port mask.
**<hex 0x0-0xffff>** - Enter the Ipv6 TCP source port mask value here.
**dst_port_mask** - Specifies an IPv6 Layer 4 TCP destination port mask.
**<hex 0x0-0xffff>** - Enter the Ipv6 TCP destination port mask value here.
**udp** - (Optional) Specifies that the following parameter are application to the UDP configuration.
**src_port_mask** - Specifies an IPv6 Layer 4 UDP source port mask.
**<hex 0x0-0xffff>** - Enter the Ipv6 UDP source port mask value here.
**dst_port_mask** - Specifies an IPv6 Layer 4 UDP destination port mask.
**<hex 0x0-0xffff>** - Enter the Ipv6 UDP destination port mask value here.
**icmp** - (Optional) Specifies that the rule applies to ICMP traffic.
**type** - Specifies the type of ICMP traffic.
**code** - Specifies the code of ICMP traffic.

## Restrictions

Only Administrator, Operator and Power-User level 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-3620-28SC: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-3620-28SC:admin#
```

## 6-2 delete egress_access_profile

### Description

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

### Restrictions

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

### Example

To delete egress access list profile ID 1:

```
DGS-3620-28SC:admin#  delete egress_access_profile profile_id 1
Command: delete egress_access_profile profile_id 1

Success.

DGS-3620-28SC:admin#
```

## 6-3 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** - Specifies the index of the egress access list profile.<br>**<value 1-4>** - Enter the profile ID used here. This value must be between 1 and 4. |
| **profile_name** - Specifies the name of the profile.<br>**<name 1-32>** - Enter the profile name here. This name can be up to 32 characters long. |
| **add** - Specifies to add a profile or rule. |
| **access_id** - Specifies the index of the access list entry. If the auto_assign option is selected, the access ID is automatically assigned. The lower the access ID, the higher the priority.<br>**auto assign** - Specifies that the access ID will be configured automatically.<br>**<value 1-128>** - Enter the access ID used here. This value must be between 1 and 128. |
| **ethernet** - Specifies an Ethernet egress ACL rule.<br>**vlan** - (Optional) Specifies the VLAN name.<br>**<vlan_name 32>** - Enter the VLAN name used for this configuration here. This name can be up to 32 characters long.<br>**vlanid** - Specifies a VLAN ID.<br>**<vlanid 1-4094>** - Enter the VLAN ID used for this congfiguration here. This value must be between 1 and 4094.<br>**mask** - (Optional) Specifies the mask used.<br>**<hex 0x0-x0fff>** - Enter the mask value used here.<br>**source_mac** - (Optional) Specifies the source MAC address.<br>**<macaddr>** - Enter the source MAC address used here.<br>**mask** - Specifies that source MAC mask used.<br>**<macmask>** - Enter the source MAC mask value here.<br>**destination_mac** - Specifies the destination MAC address.<br>**<macaddr>** - Enter the destination MAC address used here.<br>**mask** - Specifies that destination MAC mask used.<br>**<macmask>** - Enter the destination MAC mask value here.<br>**802.1p** - (Optional) Specifies the value of the 802.1p priority tag. The priority tag ranges from 1 to 7.<br>**<value 0-7>** - Enter the 802.1p priority tag used here.<br>**ethernet_type** - (Optional) Specifies the Ethernet type.<br>**<hex 0x0-0xffff>** - Enter the Ethernet type mask used here. |
| **ip** - Specifies an IP egress ACL rule.<br>**vlan** - (Optional) Specifies the VLAN name.<br>**<vlan_name 32>** - Enter the VLAN name used for this configuration here. This name can be up to 32 characters long.<br>**vlanid** - Specifies a VLAN ID.<br>**<vlanid 1-4094>** - Enter the VLAN ID used for this congfiguration here. This value must be between 1 and 4094.<br>**mask** - (Optional) Specifies the mask used.<br>**<hex 0x0-x0fff>** - Enter the mask value used here.<br>**source_ip** - (Optional) Specifies an IP source address.<br>**<ipaddr>** - Enter the source IP address used here.<br>**mask** - Specifies the source IP address used here.<br>**<netmask>** - Enter the source network mask here.<br>**destination_ip** - (Optional) Specifies an IP destination address.<br>**<ipaddr>** - Enter the destination IP address used here. |

| |
|---|
| **mask** - Specifies the destination IP address used here.<br>**<netmask>** - Enter the destination network mask here.<br>**dscp** - (Optional) Specifies the value of DSCP. The DSCP value ranges from 0 to 63.<br>**<value 0-63>** - Enter the DSCP value used here. This value must be between 0 and 63.<br>**icmp** - (Optional) Specifies that the following parameters configured will apply to the ICMP configuration.<br>**type** - Specifies that the rule will apply to the ICMP type traffic value.<br>**<value 0-255>** - Enter the ICMP traffic type value here. This value must be between 0 and 255.<br>**code** - Specifies that the rule will apply to the ICMP code traffic value.<br>**<value 0-255>** - Enter the ICMP code traffic value here. This value must be between 0 and 255.<br>**igmp** - (Optional) Specifies that the following parameters configured will apply to the IGMP configuration.<br>**type** - Specifies that the rule will apply to the IGMP type traffic value.<br>**<value 0-255>** - Enter the IGMP type traffic value here. This value must be between 0 and 255.<br>**tcp** - (Optional) Specifies that the following parameters configured will apply to the TCP configuration.<br>**src_port** - Specifies that the rule will apply to a range of TCP source ports.<br>**<value 0-65535>** - Enter the source port value here. This value must be between 0 and 65535.<br>**mask** - Specifies the TCP source port mask here.<br>**<hex 0x0-0xffff>** - Enter the TCP source port mask value here.<br>**dst_port** - Specifies that the rule will apply to a range of TCP destination ports.<br>**<value 0-65535>** - Enter the destination port value here. This value must be between 0 and 65535.<br>**mask** - Specifies the TCP destination port mask here.<br>**<hex 0x0-0xffff>** - Enter the TCP destination port mask value here.<br>**flag** - (Optional) Specifies the TCP flag fields.<br>**all** - Specifies that the TCP flag field will be set to 'all'.<br>**urg** - Specifies that the TCP flag field will be set to 'urg'.<br>**ack** - Specifies that the TCP flag field will be set to 'ack'.<br>**psh** - Specifies that the TCP flag field will be set to 'psh'.<br>**rst** - Specifies that the TCP flag field will be set to 'rst'.<br>**syn** - Specifies that the TCP flag field will be set to 'syn'.<br>**fin** - Specifies that the TCP flag field will be set to 'fin'.<br>**udp** - (Optional) Specifies that the following parameters configured will apply to the UDP configuration.<br>**src_port** - Specifies the UDP source port range.<br>**<value 0-65535>** - Enter the UDP source port range value here.<br>**mask** - Specifies the UDP source port mask here.<br>**<hex 0x0-0xffff>** - Enter the UDP source port mask value here.<br>**dst_port** - Specifies the UDP destination port range.<br>**<value 0-65535>** - Enter the UDP destination port range value here.<br>**mask** - Specifies the UDP destination port mask here.<br>**<hex 0x0-0xffff>** - Enter the UDP destination port mask value here.<br>**protocol_id** - (Optional) Specifies that the rule will apply to the value of IP protocol ID traffic.<br>**<value 0-255>** - Enter the protocol ID used here. This value must be between 0 and 255.<br>**user_define** - (Optional) Specifies 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.<br>**<hex 0x0-0xffffffff>** - Enter the user-defined mask value here.<br>**mask** - Specifies the user-defined mask here.<br>**<hex 0x0-0xffffffff>** - Enter the user-defined mask value here. |
| **ipv6** - Specifies the rule applies to IPv6 fields.<br>**class** - (Optional) Specifies the value of IPv6 class.<br>**<value 0-255>** - Enter the IPv6 class value here. This value must be between 0 and 255.<br>**source_ipv6** - (Optional) Specifies the value of IPv6 source address.<br>**<ipv6addr>** - Enter the source IPv6 source address here.<br>**mask** - Specifies the IPv6 source address mask here. |

**<ipv6mask>** - Enter the IPv6 source address mask value here.
**destination_ipv6** - (Optional) Specifies the value of IPv6 destination address.
**<ipv6addr>** - Enter the source IPv6 destination address here.
**mask** - Specifies the IPv6 destination address mask here.
**<ipv6mask>** - Enter the IPv6 destination address mask value here.
**tcp** - (Optional) Specifies the TCP protocol
**src_port** - Specifies 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** - Specifies the IPv6 TCP source port mask here.
**<hex 0x0-0xffff>** - Enter the IPv6 TCP source port mask value here.
**dst_port** - Specifies 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** - Specifies the IPv6 TCP destination port mask here.
**<hex 0x0-0xffff>** - Enter the IPv6 TCP destination port mask value here.
**udp** - (Optional) Specifies the UDP protocol.
**src_port** - Specifies 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** - Specifies the IPv6 UDP source port mask here.
**<hex 0x0-0xffff>** - Enter the IPv6 UDP source port mask value here.
**dst_port** - Specifies 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** - Specifies the IPv6 UDP destination port mask here.
**<hex 0x0-0xffff>** - Enter the IPv6 UDP destination port mask value here.
**icmp** - (Optional) Specifies that the following parameters configured will apply to the ICMP configuration.
**type** - Specifies 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** - Specifies that the rule will apply to the ICMP code traffic value.
**<value 0-255>** - Enter the ICMP code traffic value here. This value must be between 0 and 255.
**vlan_based** - The rule applies on the specified VLAN.
**vlan** - Specifies 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** - Specifies 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** - Specifies the port group value here.
**id** - Specifies 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** - Specifies the name of the port group which the rule applies.
**<name 16>** - Enter the port group name here. This name can be up to 16 characters long.

**port** - Specifies the port in the port group used.
**<port>** - Enter the port number used here.

**permit** - Specifies that packets matching the egress access rule are permitted by the switch.

**replace_priority_with** - (Optional) Specifies 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) Specifies 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) Specifies whether the ACL counter feature is enabled or disabled. This parameter is optional. The default option is disabled. If the rule is not bound with the flow_meter, all matching packets are counted. If the rule is bound with the flow_meter, then

the “counter” is overridden.
**enable** - Specifies that the ACL counter feature will be enabled.
**disable** - Specifies that the ACL counter feature will be disabled.

**deny** - Specifies the packets that match the egress access rule are filtered by the switch.

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

**delete** - Specifies to delete a profile or rule.

**access_id** - Specifies 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.

### Restrictions

Only Administrator, Operator and Power-User level 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-3620-28SC: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-3620-28SC: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-3620-28SC: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-3620-28SC:admin#
```

## 6-4 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) Specifies the index of the egress access list profile.
**<value 1-4>** - Enter the profile ID here. This value must be between 1 and 4.

**profile_name** - (Optional) Specifies 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-3620-28SC:admin# show egress_access_profile
Command: show access_profile

Egress Access Profile Table

Total User Set Rule Entries       : 3
Total Used Hardware Entries       : 3
Total Available Hardware Entries : 253

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

Mask on
    Source MAC      : FF-FF-FF-FF-FF-FF

Available Hardware Entries : 127
-------------------------------------------------------------------------------
-
Rule ID : 1       Port group: -

Match on
    VLAN ID         : 1
    Source MAC      : 00-00-00-00-00-01

Action:
    Permit

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



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

Mask on
    Source IP           : 255.255.255.255
    Destination IP     : 255.255.255.255
    DSCP

Available Hardware Entries : 126
-------------------------------------------------------------------------------
-
Rule ID : 1    (auto assign)    Port group: 1

Match on
    Source IP           : 10.0.0.2
    Destination IP     : 10.90.90.90
    DSCP                : 25

Action:
    Permit

-------------------------------------------------------------------------------
-
Rule ID : 2    (auto assign)    Port group: 1

Match on
    Source IP           : 10.0.0.1
    Destination IP     : 10.90.90.90
    DSCP                 : 25

Action:
    Permit

Matched Count : 0 packets
===============================================================================
=

DGS-3620-28SC:admin#
```

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

```
DGS-3620-28SC: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: 1  Type: Ethernet

Mask on
    Source MAC      : FF-FF-FF-FF-FF-FF

Available Hardware Entries : 127
-------------------------------------------------------------------------------
-
Rule ID : 1       Port group: -

Match on
    VLAN ID         : 1
    Source MAC      : 00-00-00-00-00-01

Action:
    Permit

===============================================================================
=
DGS-3620-28SC:admin#
```

## 6-5 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-3620-28SC: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
-00-00-00-00-01 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-3620-28SC:admin#
```

## 6-6 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 <value 0-63>} | drop] {counter [enable | disable]} | delete]**

### Parameters

| |
|---|
| **profile_id** - Specifies the profile ID. |

**<value 1-4>** - Enter the profile ID used here. This value must be between 1 and 4.

**profile_name** - Specifies 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** - Specifies the access ID.
**<value 1-128>** - Enter the access ID used here. This value must be between 1 and 128.

**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 exceed the committed rate in single rate “two color” mode. The action can be specified as one of the following:
**drop_packet** - Drop the packet immediately.
**remark_dscp** - Mark the packet with a specified DSCP. The packet is set to have the higher 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** - Specifies the two rate three color mode used.
**<value 0-1048576>** - Enter the two rate three color mode value here. This value must be between 0 and 1048576.
**cbs** - (Optional) Specifies the “Committed Burst Size”. The unit is Kbytes. That is to say, 1 means 1Kbytes. This parameter is an optional parameter. The default value is 4*1024.
**<value 0-131072>** - Enter the comitted burst size value here. This value must be between 0 and 131072.
**pir** - Specifies 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) Specifies the “Peak Burst Size”. The unit is in Kbytes.
**<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 to be color-blind. The default is color-blind mode.
**color_aware** - (Optional) Specify the meter mode to be color-aware. When this code is specified, user could set the “in-coming packet color” by using command “config color_aware”. The final color of packet is determined by the initial color of packet and the metering result.

**conform** - (Optional) Specify the action when packet is in “green color”.
**permit** - Permit the packet.
**replace_dscp** - Changes the DSCP of the packet.
**<value 0-63>** - Enter the replace DSCP value here. This value must be between 0 and 63.
**counter** - (Optional) Specifies the ACL counter. This is optional. The default is “disable”. The resource may be limited so that a counter cannot be turned on. Counters will be cleared when the function is disabled.
**enable** - Specifies that the ACL counter parameter will be enabled.
**disable** - Specifies that the ACL counter parameter will be disabled.

**exceed** - Specify the action when packet is in “yellow color”.
**permit** - (Optional) Permit the packet.
**replace_dscp** - Changes the DSCP of the packet.
**<value 0-63>** - Enter the DSCP replace value here. This value must be between 0 and 63.
**drop** - Drops the packet.
**counter** - (Optional) Specifies the ACL counter. This is optional. The default is “disable”. The resource may be limited so that a counter cannot be turned on. Counters will be cleared when the function is disabled.
**enable** - Specifies that the ACL counter parameter will be enabled.
**disable** - Specifies that the ACL counter parameter will be disabled.

**violate** - Specify the action when packet is in “red color”.

**permit** - Permit the packet.

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

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

**drop** - Drops the packet.

**counter** - (Optional) Specifies the ACL counter. This is optional. The default is “disable”. The resource may be limited so that a counter cannot be turned on. Counters will be cleared when the function is disabled.

**enable** - Specifies that the ACL counter parameter will be enabled.

**disable** - Specifies that the ACL counter parameter will be disabled.

**sr_tcm** - Specify the “single rate three color mode”.

**cir** - Specifies the single rate three color mode used.

**<value 0-1048576>** - Enter the single rate three color mode 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 committed 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 to be color-blind. The default is color-blind mode.

**color_aware** - (Optional) Specify the meter mode to be color-aware. When this code is specified, user could set the “in-coming packet color” by using command “config color_aware”. The final color of packet is determined by the initial color of packet and the metering result.

**conform** - (Optional) Specify the action when packet is in “green color”.

**permit** - (Optional) Permit the packet.

**replace_dscp** - Changes the DSCP of the packet.

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

**counter** - (Optional) Specifies the ACL counter. This is optional. The default is “disable”. The resource may be limited so that a counter cannot be turned on. Counters will be cleared when the function is disabled.

**enable** - Specifies that the ACL counter parameter will be enabled.

**disable** - Specifies that the ACL counter parameter will be disabled.

**exceed** - Specify the action when packet is in “yellow color”.

**permit** - Permit the packet.

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

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

**drop** - Drops the packet.

**counter** - (Optional) Specifies the ACL counter. This is optional. The default is “disable”. The resource may be limited so that a counter cannot be turned on. Counters will be cleared when the function is disabled.

**enable** - Specifies that the ACL counter parameter will be enabled.

**disable** - Specifies that the ACL counter parameter will be disabled.

**violate** - Specify the action when packet is in “red color”.

**permit** - Permit the packet.

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

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

**drop** - Drops the packet.

**counter** - (Optional) Specifies the ACL counter. This is optional. The default is “disable”. The resource may be limited so that a counter cannot be turned on. Counters will be cleared when the function is disabled.

**enable** - Specifies that the ACL counter parameter will be enabled.

**disable** - Specifies that the ACL counter parameter will be disabled.

**delete** - Delete the specified “flow_meter”.

## Restrictions

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

### Example

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

```
DGS-3620-28SC:admin#  config egress_flow_meter profile_id 1 access_id 1 tr_tcm
cir 1000 cbs 200 pir 2000 pbs 200 exceed 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 replace_dscp 21 violate drop


Success.


DGS-3620-28SC:admin#
```

## 6-7 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 <value1-128>}}**

### Parameters

**profile_id** - (Optional) Specifies the index of access list profile.
**<value 1-4>** - Enter the profile ID used here. This value must be between 1 and 4.

**profile_name** - (Optional) Specifies 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) Specifies the access ID.
**<value 1-128>** - Enter the access ID used here. This value must be between 1 and 128.

### Restrictions

None.

### Example

To display current egress flow meter table:

```
DGS-3620-28SC:admin# show egress_flow_meter
Command: show egress_flow_meter

Flow Meter Information:
------------------------
Profile ID : 1     Access ID : 1      Mode : trTcm / color-blind
CIR:1000(Kbps)   CBS:2000(Kbyte)   PIR:2000(Kbps)   PBS:2000(Kbyte)
Actions:
Conform : Permit    Replace DSCP : 11     Counter : enable
Exceed  : Permit    Replace DSCP : 22     Counter : enable
Violate : Drop

Profile ID : 1     Access ID : 1      Mode : srTcm / color-blind
CIR:2500(Kbps)   CBS:2000(Kbyte)    EBS:3500(Kbyte)
Actions:
Conform : Permit                              Counter : enable
Exceed  : Permit     Replace DSCP: 33      Counter : enable
Violate : Drop

Total Entries: 2

DGS-3620-28SC:admin#
```

## 6-8 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

| | |
|---|---|
| **id** - Specifies the port group ID.<br>**<value 1-64>** - Enter the port group ID here. This value must be between 1 and 64. | |
| **name** - Specifies the port group name.<br>**<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-3620-28SC:admin#  create port_group id 2 name group2
Command: create port_group id 2 name group2

Success.

DGS-3620-28SC:admin#
```

## 6-9 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** - Specifies the port group ID.<br>**<value 1-64>** - Enter the port group ID used here. This value must be between 1 and 64. |
| **name** - Specifies the port group name.<br>**<name 16> -** Enter the port group name here. This name can be up to 16 characters long. |
| **add** - Add a port list to this port group.<br>**delete** - Delete a port list from this port group. |
| **<portlist>** - Enter a list of ports used for the configuration here.<br>**all** - Specifies that all the ports will be used for this configuration. |

### Restrictions

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

### Example

Add port list “1-3” to the port group which ID is “2”:

```
DGS-3620-28SC:admin#  config port_group id 2 add 1-3
Command: config port_group id 2 add 1-3

Success.

DGS-3620-28SC:admin#
```

## 6-10 delete port_group

### Description

This command is used to delete port group.

### Format

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

### Parameters

**id** - Specifies the port group ID.
    **<value 1-64>** - Enter the port group ID used here. This value must be between 1 and 64.

**name** - Specifies 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 the port group which ID is “2”:

```
DGS-3620-28SC:admin# delete port_group id 2
Command: delete port_group id 2

Success.

DGS-3620-28SC:admin#
```

## 6-11 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) Specifies the port group ID.
    **<value 1-64>** - Enter the port group ID used here. This value must be between 1 and 64.

**name** - (Optional) Specifies the port group name.
    **<name 16>** - Enter the port group name here. This name can be up to 16 characters long.

If not specified parameter, will show all the port group.

### Restrictions

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

### Example

To show all the port group information:

```
DGS-3620-28SC:admin# show port_group
Command: show port_group

Port Group Table
Group ID     Group Name                     Ports
1              group1                         1-2,5
2              group2                         4,5,7,9,11,13
                                               15,17,19-25
4              group3                         5-7

Total Entries :3

DGS-3620-28SC:admin#
```

# Chapter 7 ARP Commands

**create arpentry** <ipaddr> <macaddr>

**delete arpentry** [<ipaddr> | all]

**config arpentry** <ipaddr> <macaddr>

**config arp_aging time** <min 0-65535>

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

**clear arptable**

**show ipfdb** {[ip_address <ipaddr> | interface <ipif_name 12> | port <port>]}

## 7-1 create arpentry

### Description

This command is used to enter an IP address and the corresponding MAC address into the switch's ARP table.

### Format

**create arpentry <ipaddr> <macaddr>**

### Parameters

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

**<macaddr>** - The MAC address corresponding to the IP address above.

### Restrictions

Only Administrator, Operator and Power-User level 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-3620-28SC: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-3620-28SC:admin#
```

## 7-2 delete arpentry

### Description

This command is used to delete a static ARP entry, made using the **create arpentry** command above, by specifying either the IP address of the entry or all. Specifying **all** deletes the switch's ARP table.

### Format

**delete arpentry [<ipaddr> | all]**

### Parameters

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

**all** - Delete all ARP entries

### Restrictions

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

### Example

To delete an entry of IP address 10.48.74.121 from the ARP table:

```
DGS-3620-28SC:admin#delete arpentry 10.48.74.121
Command: delete arpentry 10.48.74.121

Success.

DGS-3620-28SC:admin#
```

## 7-3 config arpentry

### Description

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

### Format

**config arpentry <ipaddr> <macaddr>**

### Parameters

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

**<macaddr>** - The MAC address corresponding to the IP address above.

### Restrictions

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

### Example

To configure a static ARP entry for the IP address 10.48.74.121 and MAC address 00:50:BA:00:07:36:

```
DGS-3620-28SC:admin#config arpentry 10.48.74.121 00-50-BA-00-07-36
Command: config arpentry 10.48.74.121 00-50-BA-00-07-36

Success.
```

```
DGS-3620-28SC:admin#
```

## 7-4 config arp_aging time

### Description

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

### Format

**config arp_aging time <min 0-65535>**

### Parameters

**<min 0-65535>** - The ARP age-out time, in minutes. The default is 20 minutes. The range is 0 to 65535 minutes.

### Restrictions

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

### Example

To configure the ARP aging time:

```
DGS-3620-28SC:admin#config arp_aging time 30
Command: config arp_aging time 30

Success.

DGS-3620-28SC:admin#
```

## 7-5 show arpentry

### Description

This command is used to display the Address Resolution Protocol (ARP) table. Filter the display by IP address, interface name, static entries or mac_address.

### Format

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

### Parameters

**ipif** - The name of the IP interface the end node or station for which the ARP table entry was made, resides on.
**<ipif_name 12>** - Specify the IP interface name. The maximum length is 12 characters.

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

**static** - Displays the static entries to the ARP table.

**mac_address** - Displays the ARP entry by MAC address.
  **<macaddr>** - Specify the MAC address.

**Note:** If no parameter is specified, all ARP entries will be displayed.

### Restrictions

None.

### Example

To display the ARP table:

```
DGS-3620-28SC: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         10.90.90.90      00-01-02-03-04-00  Local
System         10.255.255.255   FF-FF-FF-FF-FF-FF  Local/Broadcast

Total Entries: 3

DGS-3620-28SC:admin#
```

## 7-6 clear arptable

### Description

This command is used to remove dynamic entries from the ARP table. Static ARP entries are not affected.

### Format

**clear arptable**

### Parameters

None.

### Restrictions

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

### Example

To remove the dynamic entries from the ARP table:

```
DGS-3620-28SC:admin#clear arptable
Command: clear arptable

Success.

DGS-3620-28SC:admin#
```

## 7-7 show ipfdb

### Description

This command is used to display the IP address forwarding table on the Switch.

### Format

**show ipfdb {[ip_address <ipaddr> | interface <ipif_name 12> | port <port>]}**

### Parameters

**ip_address** - (Optional) Specifies the IP address of the forwarding table.
    **<ipaddr>** - Enter the IP address to be displayed.

**interface** - (Optional) Specifies the interface name of the forwarding table.
    **<ipif_name 12>** - Enter the interface name here. This name can be up to 12 characters long.

**port** - (Optional) Specifies the port to be displayed.
    **<port>** - Enter the port number to be displayed.

### Restrictions

None.

### Example

To display the IP address forwarding table on the Switch:

```
DGS-3620-28SC:admin# show ipfdb
Command: show ipfdb

Interface     IP Address       Port      Learned
------------  ---------------- --------- ---------

Total Entries: 0

DGS-3620-28SC:admin#
```

# Chapter 8 ARP Spoofing Prevention Commands

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

## 8-1 config arp_spoofing_prevention

### Description

The user can 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 either its sender MAC field or 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 gateway_ip** - Specify a gateway IP to be added.<br>**<ipaddr>** - Specify the IP address.<br>**gateway_mac** - Specify a gateway MAC to be configured.<br>**<macaddr>** - Specify the MAC address.<br>**ports** – Specify the ports.<br>**<portlist>** - Specify a range of ports to be configured.<br>**all** - Specify all ports to be configured. |
| **delete gateway_ip** - Specify a gateway IP to be deleted.<br>**<ipaddr>** - Specify the IP address. |

### Restrictions

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

### Example

To configure the prevent IP spoofing attack:

```
DGS-3620-28SC:admin#config arp_spoofing_prevention add gateway_ip
10.254.254.251 gateway_mac 00-00-00-11-11-11 ports 1-2
Command: config arp_spoofing_prevention add gateway_ip 10.254.254.251
gateway_mac 00-00-00-11-11-11 ports 1-2


Success.


DGS-3620-28SC:admin#
```

## 8-2 show arp_spoofing_prevention

### Description

This command is used to display the ARP spoofing prevention status.

### Format

**show arp_spoofing_prevention**

### Parameters

None.

### Restrictions

None.

### Example

To display the ARP spoofing prevention status:

```
DGS-3620-28SC:admin#show arp_spoofing_prevention
Command: show arp_spoofing_prevention

Gateway IP         Gateway MAC         Ports
------------------ -------------------  --------------------
192.168.0.1        00-00-00-00-00-01    1-28

 Total Entries: 1

DGS-3620-28SC:admin#
```

# Chapter 9 Asymmetric VLAN Commands

**enable asymmetric_vlan**
**disable asymmetric_vlan**
**show asymmetric_vlan**

## 9-1 enable asymmetric_vlan

### Description

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

### Format

**enable asymmetric_vlan**

### Parameters

None.

### Restrictions

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

### Example

To enable asymmetric VLAN setting:

```
DGS-3620-28SC:admin# enable asymmetric_vlan
Command: enable asymmetric_vlan

Success.

DGS-3620-28SC:admin#
```

## 9-2 disable asymmetric_vlan

### Description

This command is used to disable the asymmetric VLAN function.

### Format

**disable asymmetric_vlan**

### Parameters

None.

### Restrictions

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

### Example

To disable asymmetric VLAN setting:

```
DGS-3620-28SC:admin# disable asymmetric_vlan
Command: disable asymmetric_vlan

Success.

DGS-3620-28SC:admin#
```

## 9-3 show asymmetric_vlan

### Description

This command is used to display the asymmetric VLAN function.

### Format

**show asymmetric_vlan**

### Parameters

None.

### Restrictions

None.

### Example

To display asymmetric VLAN:

```
DGS-3620-28SC:admin# show asymmetric_vlan
Command: show asymmetric_vlan

Asymmetric Vlan : Disabled

DGS-3620-28SC:admin#
```

# Chapter 10 Auto Configuration Commands

**show autoconfig**

**enable autoconfig**

**disable autoconfig**

## 10-1 show autoconfig

### Description

This command is used to display the status of automatically getting configuration from a TFTP server.

### Format

**show autoconfig**

### Parameters

None.

### Restrictions

None.

### Example

To display the DHCP auto configuration status:

```
DGS-3620-28SC:admin#show autoconfig
Command: show autoconfig

Autoconfig State: Disabled

DGS-3620-28SC:admin#
```

## 10-2 enable autoconfig

### Description

This command is used to enable automatically to get configuration from a TFTP server according to the options in the DHCP reply packet. To employ this method, the DHCP server must be set up to deliver the TFTP server IP address and configuration file name information first.

### Format

**enable autoconfig**

### Parameters

None.

### Restrictions

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

### Example

To enable DHCP auto configuration status:

```
DGS-3620-28SC:admin#enable autoconfig
Command: enable autoconfig

Success.

DGS-3620-28SC:admin#
```

## 10-3 disable autoconfig

### Description

This command is used to disable automatically to get configuration from a TFTP server.

### Format

**disable autoconfig**

### Parameters

None.

### Restrictions

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

### Example

To disable the DHCP auto configuration status:

```
DGS-3620-28SC:admin#disable autoconfig
Command: disable autoconfig

Success.
```

```

DGS-3620-28SC:admin#
```

# Chapter 11 Basic IP Commands

| |
|---|
| **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 <ipv6networkaddr> \| state [enable \| disable]] \| ip_mtu <value 512-1712> \| ipv4 state [enable \| disable] \| dhcpv6_client [enable \| disable] \| ip_directed_broadcast [enable \| disable]] |
| **create ipif** <ipif_name 12> {<network_address>} <vlan_name 32> {secondary \| state [enable \| disable] \| proxy_arp [enable \| disable] {local [enable \| disable]}} |
| **delete ipif** [<ipif_name 12> {ipv6address <ipv6networkaddr>} \| all] |
| **enable ipif** [<ipif_name 12> \| all] |
| **disable ipif** [<ipif_name 12> \| all] |
| **show ipif** {<ipif_name 12>} |
| **config out_band_ipif** {ipaddress <network_address> \| state [enable \| disable] \| gateway <ipaddr>} |
| **show out_band_ipif** |
| **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>} |

## 11-1 config ipif

### Description

Configure the parameters for an L3 interface. For IPv4, only the system interface can be specified for the way to get the IP address. If the mode is set to BOOTP or DHCP, then the IPv4 address will be obtained through the operation of protocols. The manual configuration of the IP address will be of no use. If the mode is configured to BOOTP or DHCP first, and then the user configures IP address later, the mode will be changed to manual configured mode. For IPv6, multiple addresses can be defined on the same L3 interface. For IPv4, multi-netting must be done by creation of a secondary interface. Note that an IPv6 address is not allowed to be configured on a secondary 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<ipv6networkaddr> | state [enable | disable]] | ip_mtu <value 512-1712> | ipv4 state [enable | disable] | dhcpv6_client [enable | disable] | ip_directed_broadcast [enable | disable]]**

### Parameters

| |
|---|
| **ipif** - Specifies the IP interface configured.<br>**<ipif_name 12>** - Enter the name of the IP interface used here. This name can be up to 12 characters long. The default interface is 'System'. |
| **ipaddress** - (Optional) The IP address and netmask of the IP interface to be created.<br>**<network_address>** - Specify the address and mask information using the traditional format (for example, 10.1.2.3/255.0.0.0 or in CIDR format, 10.1.2.3/8). |
| **vlan** - (Optional) The name of the VLAN corresponding to the IP interface.<br>**<vlan_name 32>** - Specify the VLAN name. The maximum length is 32 characters. |

**state** - Enable or disable the IP interface.
- **enable** - Enable the IP interface.
- **disable** - Disable the IP interface.

**proxy_arp** - (Optional) Enable or disable the proxy ARP. This is for the IPv4 function. The default is disabled.
- **enable** - Enable the proxy ARP.
- **disable** - Disable the proxy ARP.

**local** - (Optional) This setting controls whether the system provides the proxy reply for the ARP packets destined for IP addresses 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 addresses located on a different interface. For ARP packets destined for IP address located on the same interface, the system will check this setting to determine whether to reply. The default is disabled.
- **enable** - Enable the local proxy ARP function.
- **disable** - Disable the local proxy ARP function.

**bootp** - Allows the selection of the BOOTP protocol for the assignment of an IP address to the switch's System IP interface.

**dhcp** - Allows the selection of the DHCP protocol for the assignment of an IP address to the switch's System.

**ipv6** - The following are IPv6-related parameters.
- **ipv6address** - The IPv6 address and subnet prefix of the IPV6 address to be created.
  - **<ipv6networkaddr>** - The IPv6 address and subnet prefix of the IPV6 address to be created.
- **state** - Enable or disable the IPv6 state of the IP interface.
  - **enable** - Enable the IPv6 state of the IP interface.
  - **disable** - Disable the IPv6 state of the IP interface.

**ip_mtu** - Specifies the IP Layer MTU value used.
- **<value 512-1712>** - Enter the IP Layer MTU value used here. The value must be between 512 and 1712.

**ipv4 state** - The state of the IPv4 interface.
- **enable** - Enable the IPv4 state of the IP interface.
- **disable** - Disable the IPv4 state of the IP interface.

**dhcpv6_client** - Specifies the DHCPv6 client state of the interface.
- **enable** - Specifies that the DHCPv6 client state of the interface will be enabled.
- **disable** - Specifies that the DHCPv6 client state of the interface will be disabled.

**ip_directed_broadcast** - Specifies the IP directed-broadcast state of the interface.
- **enable** - Specifies that the IP directed-broadcast state of the interface will be enabled.
- **disable** - Specifies that the IP directed-broadcast state of the interface will be disabled.

## Restrictions

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

## Example

To configure the System IP interface:

```
DGS-3620-28SC:admin#config ipif System vlan v1
Command: config ipif System vlan v1

Success.

DGS-3620-28SC:admin#
```

## 11-2 create ipif

### Description

This command is used to create an L3 interface. This interface can be configured with IPv4 or IPv6 addresses. Currently, it has a restriction: an interface can have only one IPv4 address defined. But it can have multiple IPv6 addresses defined. Thus, the multinetting configuration of IPv4 must be done through creation of a secondary interface on the same VLAN, instead of directly configuring multiple IPv4 addresses on the same interface. Configuration of IPv6 addresses must be done through the command **config ipif**.

### 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>** - Specify the name of the interface.

**<network_address>** - (Optional) Specify a host address and length of network mask.

**<vlan_name 32>** - Specify the name of the VLAN corresponding to the IP interface. The maximum length is 32 characters.

**secondary** - The IPv4 secondary interface to be created.

**state** - The state of the IP interface.
- **enable** - Enable the state setting.
- **disable** - Disable the state setting.

**proxy_arp** - Enable or disable the proxy ARP function. It is for IPv4 function. The default is disabled.
- **enable** - Enable the proxy ARP function.
- **disable** - Disable the proxy ARP function.

**local** - (Optional) This setting controls whether the system provides the proxy reply for the ARP packets destined for IP address located on 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 an IP address located on a different interface. For ARP packets destined for an IP address located on the same interface, the system will check this setting to determine whether to reply. The default is disabled.
- **enable** - Enable the local setting.
- **disable** - Disable the local setting.

### Restrictions

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

### Example

To create an IP interface petrovic1:

```
DGS-3620-28SC:admin#create ipif petrovic1 100.1.1.2/16 VLAN598
Command: create ipif petrovic1 100.1.1.2/16 VLAN598

Success.

DGS-3620-28SC:admin#
```

## 11-3 delete ipif

### Description

This command is used to delete an interface or an IPv6 address.

### Format

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

### Parameters

**<ipif_name 12>** - The name of the interface.

- **ipv6address** - (Optional) The IPv6 network address to be deleted.
  - **<ipv6networkaddr>** - The IPv6 network address to be deleted.

**all** - All IP interfaces except the System IP interface will be deleted.

### Restrictions

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

### Example

To delete interface petrovic1:

```
DGS-3620-28SC:admin#delete ipif petrovic1
Command: delete ipif petrovic1

Success.

DGS-3620-28SC:admin#
```

## 11-4 enable ipif

### Description

This command is used to enable the state for an IPIF. When the state is enabled, the IPv4 processing will be started when an IPv4 address is configured on the IPIF. The IPv6 processing will be started when an IPv6 address is explicitly configured on the IPIF.

### Format

**enable ipif [<ipif_name 12> | all]**

### Parameters

**<ipif_name 12>** - The name of the interface.

**all** - All of the IP interfaces.

### Restrictions

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

### Example

To enable the state for interface petrovic1:

```
DGS-3620-28SC:admin#enable ipif petrovic1
Command: enable ipif petrovic1

Success.

DGS-3620-28SC:admin#
```

## 11-5 disable ipif

### Description

This command is used to disable the state of an interface.

### Format

**disable ipif [<ipif_name 12> | all]**

### Parameters

| |
|---|
| **<ipif_name 12>** - The name of the interface. |
| **all** - All of the IP interfaces. |

### Restrictions

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

### Example

To disable the state for an interface:

```
DGS-3620-28SC:admin#disable ipif petrovic1
Command: disable ipif petrovic1

Success.

DGS-3620-28SC:admin#
```

## 11-6 show ipif

### Description

This command is used to display IP interface settings.

### Format

**show ipif {<ipif_name 12>}**

### Parameters

**<ipif_name 12>** - (Optional) The name of the interface.

### Restrictions

None.

### Example

To display IP interface settings:

```
DGS-3620-28SC:admin#show ipif
Command: show ipif

IP Interface                : System
VLAN Name                   : default
Interface Admin State       : Enabled
DHCPv6 Client State         : Disabled
IPv4 Address                : 10.90.90.90/8 (Manual)  Primary
Proxy ARP                   : Disabled   (Local : Disabled)
IP Directed Broadcast       : Disabled
IPv4 State                  : Enabled
IPv6 State                  : Enabled
IP MTU                      : 1500

IP Interface                : mgmt_ipif
Status                      : Enabled
IP Address                  : 192.168.0.1
Subnet Mask                 : 255.255.255.0
Gateway                     : 0.0.0.0
Link Status                 : Link Down

Total Entries: 2

DGS-3620-28SC:admin#
```

## 11-7 config out_band_ipif

### Description

This command is used to configure the out of band management port settings.

### Format

**config out_band_ipif {ipaddress <network_address> | state [enable | disable] | gateway <ipaddr>} (1)**

### Parameters

**ipaddress** - Specify the IP address of the interface. The parameter must include the mask.
**<network_address>** - Specify the IP address of the interface. The parameter must include the mask.

**state** – Specify the interface status.
    **enable** - Specify to enable the interface.
    **disable** - Specify to disable the interface.

**gateway** - Specify the gateway IP address of the out-of-band management network.
    **<ipaddr>** - Specify the gateway IP address.

### Restrictions

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

### Example

To disable the out-of-band management state:

```
DGS-3620-28SC:admin#config out_band_ipif state disable
Command: config out_band_ipif state disable

Success.

DGS-3620-28SC:admin#
```

## 11-8 show out_band_ipif

### Description

This command is used to display the current configurations of special out-of-band management interfaces.

### Format

**show out_band_ipif**

### Parameters

None.

### Restrictions

None.

### Example

To display the configuration of out-of-band management interfaces:

```
DGS-3620-28SC:admin#show out_band_ipif
Command: show out_band_ipif

Status              : Enable
IP Address          : 192.168.0.1
Subnet Mask         : 255.255.255.0
Gateway             : 0.0.0.0
Link Status         : LinkDown
```

```
DGS-3620-28SC:admin#
```

## 11-9 enable ipif_ipv6_link_local_auto

### Description

This command is used to enable the auto configuration of link local address when there are no IPv6 addresses explicitly configured. When an IPv6 address is explicitly configured, the link local address will be automatically configured, and the IPv6 processing will be started. When there is no IPv6 address explicitly configured, by default, link local address is not configured and the IPv6 processing will be disabled. By enabling this automatic configuration, the link local address will be automatically configured and IPv6 processing will be started.

### Format

**enable ipif_ipv6_link_local_auto [<ipif_name 12> | all]**

### Parameters

**<ipif_name 12>** - The name of the interface.

**all** - All of the IP interfaces.

### Restrictions

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

### Example

To enable the automatic configuration of link local address for an interface:

```
DGS-3620-28SC:admin#enable ipif_ipv6_link_local_auto interface1
Command: enable ipif_ipv6_link_local_auto interface1

Success.

DGS-3620-28SC:admin#
```

## 11-10 disable ipif_ipv6_link_local_auto

### Description

This command is used to disable the auto configuration of link local address when no IPv6 address is explicitly configured.

### Format

**disable ipif_ipv6_link_local_auto [<ipif_name 12> | all]**

### Parameters

**<ipif_name 12>** - The name of the interface.

**all** - All of the IP interfaces.

### Restrictions

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

### Example

To disable the automatic configuration of link local address for an interface:

```
DGS-3620-28SC:admin#disable ipif_ipv6_link_local_auto interface1
Command: disable ipif_ipv6_link_local_auto interface1

Success.

DGS-3620-28SC:admin#
```

## 11-11 show ipif_ipv6_link_local_auto

### Description

This command is used to display the link local address automatic configuration state.

### Format

**show ipif_ipv6_link_local_auto {<ipif_name 12>}**

### Parameters

**<ipif_name 12>** - (Optional) The name of the interface.

### Restrictions

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

### Example

To display the link local address automatic configuration state:

```
DGS-3620-28SC:admin#show ipif_ipv6_link_local_auto
Command: show ipif_ipv6_link_local_auto

 IPIF: System          Automatic Link Local Address: Disabled

DGS-3620-28SC:admin#
```

# Chapter 12 Border Gateway Protocol (BGP) Command List

```
enable bgp
disable bgp
create bgp <as_number 1-65535>
delete bgp <as_number 1-65535>
config bgp router_id <ipaddr>
config bgp synchronization [enable | disable]
config bgp enforce_first_as [enable | disable]
create bgp aggregate_address <network_address> {summary_only | as_set}
delete bgp aggregate_address [<network_address> | all]
show bgp aggregate_address {<network_address>}
create bgp network <network_address> {route_map <map_name 16>}
config bgp network <network_address> [route_map <map_name 16> | clear_routemap]
delete bgp network [<network_address> | all]
show bgp network {<network_address>}
config bgp timer holdtime <sec 0-65535> keepalive <sec 0-65535>
config bgp {always_compare_med [disable | enable] | deterministic_med [disable | enable] |
        default_local_preference <uint 0-4294967295> | bestpath {as_path_ignore [disable | enable] |
        compare_routerid [disable | enable] | med_confed [disable | enable] | med_missing_as_worst
        [disable | enable] | compare_confed_aspath [disable | enable]}(1)}(1)
config bgp dampening [route_map <map_name 16> | clear_routemap | {state [enable | disable] |
        half_life <value 1-45> | reuse <value 1-20000> | suppress <value 1-20000> |
        max_suppress_time <value 1-255> | un_reachability_half_life <value 1-45>}(1)]
show bgp dampening
config bgp peer_group <peer_group_name 16> [remote_as <as_number 0-65535> | [add |
        delete] <ipaddr>]
create bgp neighbor [<ipaddr> [remote_as <as_number 1-65535> | peer_group
        <peer_group_name 16>] | peer_group <peer_group_name 16>]
delete bgp neighbor [<ipaddr> | peer_group <peer_group_name 16> | all]
config bgp neighbor [<ipaddr> | peer_group <peer_group_name 16>] [description <desc 80> |
        clear_description | password <password 25> | clear_password]
config bgp neighbor session [<ipaddr> | peer_group <peer_group_name 16>] [activity | state]
        [enable | disable]
config bgp neighbor general [<ipaddr> | peer_group <peer_group_name 16>] {ebgp_multihop
        <value 1-255> | weight [<value 0-65535> | default] | update_source [add | delete] ipif
        <ipif_name 12> | send_community [standard | none] | next_hop_self [enable | disable] |
        soft_reconfiguration_inbound [enable | disable] | remove_private_as [enable | disable] |
        allowas_in [enable {<value 1-10>} | disable] | default_originate [enable {route_map
        <map_name 16>} | disable]}(1)
config bgp neighbor timer [<ipaddr> | peer_group <peer_group_name 16>]
        {advertisement_interval [<sec 0-600> | default] | [keepalive <sec 0-65535> holdtime <sec 0-
        65535> | default_keepalive_holdtime] | as_origination_interval [<sec 1-600> | default] |
        connect [<sec 1-65535> | default]}(1)
config bgp neighbor route_reflector_client [<ipaddr> | peer_group <peer_group_name 16>]
        state [enable | disable]
config bgp neighbor map [<ipaddr> | peer_group <peer_group_name 16>]  {unsuppress_map
        [add | delete] <map_name 16> | route_map [in | out] [add | delete] <map_name 16>}(1)
config bgp neighbor filter [<ipaddr> | peer_group <peer_group_name 16>] {filter_list [in | out]
```

| |
|---|
| [add \| delete] <list_name 16> \| prefix_list [in \| out] [add \| delete] <list_name 16> \| capability_orf_prefix_list [receive \| send \| both \| none]}(1) |
| **show bgp peer_group** {<peer_group_name 16>} |
| **config bgp route_reflector cluster_id** <ipaddr> |
| **config bgp client_to_client_reflection** [enable \| disable] |
| **config bgp confederation identifier** <as_number 0-65535> |
| **config bgp confederation peers** [add \| delete] <aspath_list> |
| **clear bgp** [all \| ipaddr <ipaddr> \| as <as_number 1-65535> \| peer_group <peer_group_name 16> \| external] {soft {[in {prefix_filter} \| out]}} |
| **clear bgp dampening {[<ipaddr> \| <network_address>]}** |
| **create bgp as_path access_list** <list_name 16> |
| **config bgp as_path access_list** <list_name 16> [add \| delete] <regexp_str 80> [deny \| permit] |
| **delete bgp as_path access_list** [list_name <list_name 16> \| all] |
| **show bgp as_path access_list** {<list_name 16>} |
| **create bgp community_list** [standard \| expanded] <list_name 16> |
| **config bgp community_list** [standard <list_name 16> [add \| delete] {internet \| local_as \| no_advertise \| no_export \| community_set <community_set 80>}(1) [deny \| permit] \| expanded <list_name 16> [add \| delete] <regexp_str 80> [deny \| permit]] |
| **delete bgp community_list** [list_name <list_name 16> \| all] |
| **show bgp community_list** {<list_name 16>} |
| **show bgp route** {[regexp <desc 80> \| inconsistent_as \| cidr_only \| filter_list <list_name 16> \| route_map <map_name 16> \| community {community_set <community_set 80> \| local_as \| no_advertise \| no_export \| internet} {exact_match} \| community_list <list_name 16> {exact_match} \| ipaddress <ipaddr> \| network <network_address> {longer_prefixes} \| prefix_list <list_name 16>]} |
| **show bgp neighbors** {<ipaddr> {[advertised_routes \| received_routes \| routes \| received_prefix_filter \| statistics]}} |
| **show bgp dampened_routes** |
| **show bgp flap_statistics** |
| **show bgp** {summary} |
| **show bgp reflection** |
| **show bgp confederation** |
| **config bgp trap** [peer_established \| peer_idle \| all] [enable \| disable] |
| **show bgp trap_state** |
| **config bgp scan_timer** [<sec 5-60> \| default] |
| **config bgp aggregate_next_hop_check** [enable \| disable] |
| **config bgp fast_external_fallover** [enable \| disable] |
| **config bgp neighbor maximum_prefix** [<ipaddr> \| peer_group <peer_group_name 16>] <value 1-12000> {<value 1-100>} {warning_only} |
| **clear bgp flap_statistics {[<ipaddr> \| <network_address>]}** |

## 12-1 enable bgp

### Description

This command is used to enable the BGP protocol. By enabling the BGP protocol, all the previous configurations will be applied to the protocol kernel and start. By default, BGP is disabled.

### Format

**enable bgp**

### Parameters

None.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

To enable BGP protocol:

```
DGS-3620-28SC:admin# enable bgp
Command: enable bgp

Success.

DGS-3620-28SC:admin#
```

## 12-2 disable bgp

### Description

This command is used to disable the BGP protocol. By disabling the BGP protocol, all peers will be disconnected and dynamic routes will be deleted. All the static configurations however will be reserved. If BGP enables again, the previous configurations can be re-applied.

### Format

**disable bgp**

### Parameters

None.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

To disable BGP protocol:

```
DGS-3620-28SC:admin# disable bgp
Command: disable bgp

Success.

DGS-3620-28SC:admin#
```

## 12-3 create bgp

### Description

This command is used to create a BGP process. It's AS number must be set. When BGP protocol starts, it must belong to a single AS. The user must set the AS number before configuring any of the other attributes.

### Format

**create bgp <as_number 1-65535>**

### Parameters

**<as_number 1-65535>** - Specifies the BGP AS number. This value must be between 1 and 65535.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

To create a BGP process:

```
DGS-3620-28SC:admin# create bgp 100
Command: create bgp 100

Success.

DGS-3620-28SC:admin#
```

## 12-4 delete bgp

### Description

This command is used to delete the BGP process. The AS number must be specified. When the BGP process is deleted, all peer and route information from BGP will be deleted. Route entries redistributed from BGP must also be canceled.

### Format

**delete bgp <as_number 1-65535>**

### Parameters

**<as_number 1-65535>** - Specifies the BGP AS number. This value must be between 1 and 65535.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

To create a BGP process:

```
DGS-3620-28SC:admin# delete bgp 100
Command: delete bgp 100

Success.

DGS-3620-28SC:admin#
```

## 12-5 config bgp router_id

### Description

This command is used to configure the BGP process's router ID. The address of a loopback interface is preferred to as an IP address on a physical interface because the loopback interface is more effective than a fixed interface as an identifier because there is no physical link to go down.

The user must specify a unique router ID within the network. This command will reset all active BGP peering sessions.

When a router ID is not configured, the router ID is selected by the following rules:

1. If a loopback interface is configured, the router ID is set to the IP address of the loopback.
2. If multiple loopback interfaces are configured, the loopback with the highest IP address is used.
3. If no loopback interface is configured, the router ID is set to the highest IP address on a physical interface.

**Note:** One newly created interface whose address may be preferred to be the router ID according to the rules above, but, it will not be chosen to be router ID immediately. Only when the router ID is set to zero or when recreating a BGP instance, the new interface may be selected as the BGP router ID.

### Format

**config bgp router_id <ipaddr>**

### Parameters

**<ipaddr>** - An ID to identify a BGP router. If it is set to zero the router ID will be automatically determined. The default value is the highest IP address on a physical interface.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

To configure the BGP process's router ID:

```
DGS-3620-28SC:admin#  config bgp router_id 10.10.10.1
Command: config bgp router_id 10.10.10.1

Success

DGS-3620-28SC:admin#
```

## 12-6 config bgp synchronization

### Description

This command is used to configure the BGP synchronization ability. Usually, a BGP speaker does not advertise a route to an external neighbor unless that route is local or exists in the IGP. By default, synchronization between BGP and the IGP is turned off to allow the BGP to advertise a network route without waiting for route validation from the IGP. This feature allows routers and access servers within an Autonomous System to have the route before BGP makes it available to other autonomous systems.

### Format

**config bgp synchronization [enable | disable]**

### Parameters

**enable** - Specifies to enable synchronization.
**disable** - Specifies to disable synchronization. By default, this setting is disabled.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

To enable the BGP process' synchronization ability:

```
DGS-3620-28SC:admin#  config bgp synchronization enable
Command: config bgp synchronization enable

Success

DGS-3620-28SC:admin#
```

## 12-7 config bgp enforce_first_as

### Description

This command is used to enforce the neighbor's AS as the first AS in the AS list.

When the setting is enabled, any updates received from an external neighbor, that does not have the neighbor’s configured Autonomous System (AS) at the beginning of the AS_PATH in the received update, will be denied. Enabling this feature adds to the security of the BGP network by not allowing traffic from unauthorized systems.

### Format

**config bgp enforce_first_as [enable | disable]**

### Parameters

**enable** - Enables the enforce first AS setting.
**disable** - Disables the enforce first AS setting. The default setting is disabled.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

To enable the BGP process’s enforce_first_as ability:

```
DGS-3620-28SC:admin#  config bgp enforce_first_as enable
Command: config bgp enforce_first_as enable

Success

DGS-3620-28SC:admin#
```

## 12-8 create bgp aggregate_address

### Description

This command is used to create an aggregate entry in the Border Gateway Protocol (BGP) database.

Using the aggregate_address command with no keywords will create an aggregate entry in the BGP routing table, if any more specific BGP routes are available that fall within the specified range. The aggregate route will be advertised as coming from your Autonomous System and will have the atomic aggregate attribute set to indicate that information might be missing. That is, the original AS path associated with more specific routes will be lost. The atomic aggregate attribute is set unless you specify the as_set keyword.

Using the as_set keyword will create an aggregate entry, but the path advertised for this route will include an AS set consisting of all AS that are contained in all paths that are being summarized. Do not use continually withdrawn and updated as autonomous system path reachability information for the summarized routes changes.

Using the summary_only keyword will create an aggregate route but suppresses advertisements of more specific routes to all neighbors. If you want to suppress only advertisements to certain neighbors, you may use the neighbor prefix_list command.

### Format

**create bgp aggregate_address <network_address> {summary_only | as_set}**

### Parameters

**<network_address>** - Specifies the IP network address aggregated.

**summary_only** - (Optional) Specifies that more specific routes will not be advertised.

**as_set** - (Optional) Generates an Autonomous System set path information.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

To create an aggregate route of which the network address is 10.0.0.0/8, suppress more-specific routes:

```
DGS-3620-28SC:admin#  create bgp aggregate_address 10.0.0.0/8 summary_only
Command: create bgp aggregate_address 10.0.0.0/8 summary_only

Success.

DGS-3620-28SC:admin#
```

## 12-9 delete bgp aggregate_address

### Description

This command is used to delete an aggregate entry in a Border Gateway Protocol (BGP) database.

### Format

**delete bgp aggregate_address [<network_address> | all]**

### Parameters

**<network_address>** - Specifies the IP aggregated network to be deleted.

**all** - Delete all IP aggregated networks.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

To delete an aggregate_route of which the network address is 10.0.0.0/8:

```
DGS-3620-28SC:admin#  delete bgp aggregate_address 10.0.0.0/8
Command: delete bgp aggregate_address 10.0.0.0/8

Success.

DGS-3620-28SC:admin#
```

## 12-10 show bgp aggregate_address

### Description

This command is used to show the aggregate entries in the Border Gateway Protocol (BGP) database.

### Format

**show bgp aggregate_address {<network_address>}**

### Parameters

**<network_address>** - Specifies the IP aggregated network address.
If specific network address is not specified, all aggregated address will be displayed.

### Restrictions

None. (EI Mode Only Command)

### Example

To display an aggregate route of 10.0.0.0/8:

```
DGS-3620-28SC:admin#  show bgp aggregate_address 10.0.0.0/8
Command: show bgp aggregate_address 10.0.0.0/8
Network Address         Options
------------------    ----------------------
10.0.0.0/8              summary_only, as_set

Total Aggregate Address Number: 1.

DGS-3620-28SC:admin#
```

## 12-11 create bgp network

### Description

This command is used to specify the network advertised by the Border Gateway Protocol (BGP). BGP networks can be learned from connected routes, from dynamic routing, and from static route sources.

### Format

**create bgp network <network_address> {route_map <map_name 16>}**

### Parameters

**<network_address>** - Represents the local network that BGP will advertise.

**route_map** - (Optional) Specifies the route map to be applied to the advertised networks. If not specified, all networks are advertised.
**<map_name 16>** - Enter the route map name here. This name can be up to 16 characters long.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

Setup network 10.108.0.0/16 to be included in the BGP updates:

```
DGS-3620-28SC:admin#  create bgp network 10.108.0.0/16
Command: create bgp network 10.108.0.0/16

Success.

DGS-3620-28SC:admin#
```

## 12-12 config bgp network

### Description

This command is used to configure the attribute associated with the network advertised by the Border Gateway Protocol (BGP).

### Format

**config bgp network <network_address> [route_map <map_name 16> | clear_routemap]**

### Parameters

**<network_address>** - Represents the local network that BGP will advertise.

**route_map** - Specifies the route map applied to the advertised networks.
**<map_name 16>** - Enter the route map name here. This name can be up to 16 characters long.

**clear_routemap** - Removes the route map applied to the network.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

Change the network 10.108.0.0/16 to clear a route map:

```
DGS-3620-28SC:admin#  config bgp network 10.108.0.0/16 clear_routemap
Command: config bgp network 10.108.0.0/16 clear_routemap

Success.

DGS-3620-28SC:admin#
```

## 12-13 delete bgp network

### Description

This command is used to delete the networks advertised by the Border Gateway Protocol (BGP).

### Format

**delete bgp network [<network_address> | all]**

### Parameters

| |
|---|
| **<network_address>** - Represents the local network that BGP will advertise. |
| **all** - Deletes all BGP networks. |

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

To delete network 10.108.0.0/16 to be advertised in the BGP updates:

```
DGS-3620-28SC:admin#  delete bgp network 10.108.0.0/16
Command: delete bgp network 10.108.0.0/16

Success.

DGS-3620-28SC:admin#
```

## 12-14 show bgp network

### Description

This command is used to show the networks advertised by the Border Gateway Protocol (BGP).

### Format

**show bgp network {<network_address>}**

### Parameters

| |
|---|
| **<network_address> -** (Optional) Represents the local network that BGP will advertise. |
| If a specific network address is not specified, all network addresses will be displayed. |

### Restrictions

None. (EI Mode Only Command)

### Example

To show network 10.108.0.0/16 advertised in the BGP updates:

```
DGS-3620-28SC:admin#  show bgp network 10.108.0.0/16
Command: show bgp network 10.108.0.0/16

Network Address       Route Map
-----------------     -------------
10.108.0.0/16          -

Total Network Number:  1

DGS-3620-28SC:admin#
```

## 12-15 config bgp timer

### Description

This command is used to configure the BGP protocol timer. The hold time needs to be at least three times that of the keepalive time. If the timer is specified for specific neighbors, then the neighbor specific timer will take effect.

### Format

**config bgp timer holdtime <sec 0-65535> keepalive <sec 0-65535>**

### Parameters

**holdtime** - The system will declare a peer as dead if a keepalive message is received that is more than the hold time. The default value is 180 seconds. If the holdtime is set to zero, then the holdtime will never expire. If the two routers that build a BGP connection have a different hold time, then the smaller hold time will be used. If the timer is specified for specific neighbors, then the neighbor specific timer will take effect. The hold time needs to be at least three times that of the keepalive timer.
**<sec 0-65535>** - Enter the hold time value used here. This value must be between 0 and 65535.

**keepalive** - This specifies the interval at which keepalive messages are sent to its peer. If the keepalive value is set to zero, then the keepalive message will not be sent out. The default value is 60 seconds. If the two routers that build a BGP connection have a different keepalive timer, then the smaller keepalive timer will be used. If the timer is specified for specific neighbors, then the neighbor specific timer will take effect.
**<sec 0-65535>** - Enter the keep-alive time value used here. This value must be between 0 and 65535.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

This command is used to configure the BGP hold and keepalive timer:

```
DGS-3620-28SC:admin#  config bgp timer holdtime 360 keepalive 120
Command: config bgp timer holdtime 360 keepalive 120

Success.

DGS-3620-28SC:admin#
```

## 12-16 config bgp

### Description

This command is used to configure the BGP best path selection related setting. MED is a metric assigned to tell the external router how to choose a route. By default, MED is used to determine the route that is advertised by the same AS.

The BGP deterministic med command can be configured to enforce a deterministic comparison of the MED values between all the paths received from within the same Autonomous System

Default local preference:

By default, a BGP router will send the default local preference with the routes. It can be overwritten if the local preference is set by the route map. For the received route, the local preference received with the route will be used in the best path selection. This local preference will be overwrite if the local preference is ingress set by the route map.

For the local routes, the default local preference will be used for them in the best path selection

Best path selection process:

The following is the steps that the BGP will use to select the best path among BGP routes:

1. Prefer the path that has the largest weight.
2. If the routes have the same weight, use the route with the highest local preference.
3. If the routes have the same local preference, prefer the route that was originated by BGP on this router. Originated from network command > from redistribute command> from aggregate command.
4. If no route was originated, prefer the route with the shortest AS path.
5. If all paths are of the same AS length, prefer the route with lowest origin code (IGP < EGP < INCOMPLETE).
6. If the origin codes are the same, prefer the path with the lowest Multi Exit Discriminator.
7. If the MEDs are the same, prefer external paths over internal paths. EBGP >Confederation>IBGP.
8. Prefer the path through the closest IGP neighbor.
9. Prefer the path that was received first (the oldest one).
10. Prefer the path with the lowest BGP Router ID.
11. Prefer to the routes advertised by the BGP speaker with a lower BGP identifier value.
12. Prefer to the routes advertised by the BGP speaker with lower peer address.

## Format

```
config bgp {always_compare_med [disable | enable] | deterministic_med [disable | enable] |
default_local_preference <uint 0-4294967295> | bestpath {as_path_ignore [disable | enable]
| compare_routerid [disable | enable] | med_confed [disable | enable] |
med_missing_as_worst [disable | enable] | compare_confed_aspath [disable | enable]}(1)}(1)
```

## Parameters

**always_compare_med** - (Optional) Enable or disable the comparison of the Multi Exit Discriminator (MED) for paths from the neighbors in different Autonomous Systems. By default this setting is disabled.
**enable** - Specifies that the 'always compare MED' option will be enabled.
**disable** - Specifies that the 'always compare MED' option will be disabled.

**deterministic_med** - (Optional) Enable or disable to enforce the deterministic comparison of the Multi Exit Discriminator (MED) for paths received from the neighbors within the same Autonomous System. By default this setting is disabled.
**enable** - Specifies that the 'deterministic MED' option will be enabled.
**disable** - Specifies that the 'deterministic MED' option will be disabled.

**default_local_preference** - (Optional) Specifies the default local preference value. The default value is 100.
**<uint 0-4294967295>** - Enter the default local preference value here. This value must be between 0 and 4294967295.

**bestpath** - (Optional) Specifies the best path value to be used.

**as_path_ignore** - (Optional) If enabled, the BGP process will ignore the AS path in the path selection process. By default this value is disabled.
**enable** - Specifies that the 'AS path ignore' option will be enabled.
**disable** - Specifies that the 'AS path ignore' option will be disabled.

**compare_routerid** - (Optional) If enabled, the BGP process will include the router ID in the path selection process. Similar routes are compared and the route with the lowest router ID is selected. By default this value is disabled.
**enable** - Specifies that the 'compare router ID' option will be enabled.
**disable** - Specifies that the 'compare router ID' option will be disabled.

**med_confed** - (Optional) If enabled, the BGP process will compare the MED for the routes that are received from confederation peers. For routes that have an external AS in the path, the comparison does not occur. By default this value is disabled.
**enable** - Specifies that the 'MED confed' option will be enabled.
**disable** - Specifies that the 'MED confed' option will be disabled.

**med_missing_as_worst** - (Optional) If enabled, the BGP process will assign a value of infinity to routes that are missing the Multi Exit Discriminator (MED) attribute. If disabled, the BGP process will assign a value of zero to routes that are missing the Multi Exit Discriminator (MED) attribute, causing this route to be choosed as the best path. By default this value is disabled.
**enable** - Specifies that the 'MED missing AS worst' option will be enabled.
**disable** - Specifies that the 'MED missing AS worst' option will be disabled.

**compare_confed_aspath** - (Optional) If enabled, the BGP process will compare the confederation AS path length of the routes received. The shorter the confederation AS path length, the better the route is. By default this value is disabled.
**enable** - Specifies that the 'compare confed AS path' option will be enabled.
**disable** - Specifies that the 'compare confed AS path' option will be disabled.

## Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

This command shows how to disable the comparison of the Multi Exit Discriminator (MED):

```
DGS-3620-28SC:admin# config bgp always_compare_med disable
Command: config bgp always_compare_med disable

Success.

DGS-3620-28SC:admin#
```

## 12-17 config bgp dampening

### Description

The purpose of this command is to eliminate the dampening of routes and thus to avoid unstable networks caused by flapping routes. The following describes the way how it is achieved.

If a prefix is removed or is added, BGP will add a penalty on the route of 1000; if an attribute of received route changes, BGP will add a penalty on the route of 500.

Suppose that the half-life is configured to be 15min, the re-use value will be 800, and the suppress value will be 1500.

1. When a route flaps (from up to down), add the penalty by 1000.Since the penalty is smaller than the suppress value, BGP will work normally. It will send a withdraw message (an update message) to the neighbors.
2. The penalty of the route will decrease as time elapses. Here we assume that it pass 7.5 minutes, then the penalty of the route is 1000-500*7.5/15=750.
3. If another flap occurs (the route change from down to up) then the penalty of the route will be 1750 which is larger than the suppress value, and the route will be dampened. BGP will not send an update message for this status change.
4. When the penalty of the route decreases and become smaller than the re-use value (800), the route will not be dampened and the update message will be sent again.

**Note:** If the dampening ability is enabled and there are one or more dampened routes, the dampened routes will be released to be the normal state immediately after we disable the dampening function.

### Format

**config bgp dampening [route_map <map_name 16> | clear_routemap | {state [enable | disable] | half_life <value 1-45> | reuse <value 1-20000> | suppress <value 1-20000> | max_suppress_time <value 1-255> | un_reachability_half_life <value 1-45>}(1)]**

### Parameters

**route_map** - The route_map here is to set the dampening to be criterial.
**<map_name 16>** - Enter the route map name here. This name can be up to 16 characters long.

**clear_routemap** - This option will withdraw the route_map configuration.

**state** - (Optional) Specifies the BGP dampening function’s state.
**enable** - Specifies that the BGP dampening function's state will be enabled.

**disable** - Specifies that the BGP dampening function's state will be disabled.

**half_life** - (Optional) Specifies the time (in minute) after which the penalty of the reachable routes will be down, by half. The default setting is 15 minutes.

**<value 1-45>** - Enter the half life value here. This value must be between 1 and 45 minutes.

**reuse** - (Optional) If the penalty for a flapping route decreases enough to fall below this value, the route is unsuppressed. The default setting is 750.

**<value 1-20000>** - Enter the re-use value used here. This value must be between 1 and 20000.

**suppress** - (Optional) A route is suppressed when its penalty exceeds this limit. The default setting is 2000.

**<value 1-20000>** - Enter the surpress value used here. This value must be between 1 and 20000.

**max_suppress_time** - (Optional) Maximum time (in minutes) a route can be suppressed. The default setting is 45 minutes.

**<min 1-255>** - Enter the maximum suppress time value here. This value must be between 1 and 255 minutes.

**un_reachablity_half_life** - (Optional) Specifies the time (in minute) after which the penalty of the unreachable routes will be down, by half. The default setting is 15 minutes.

**<value 1-45>** - Enter the the time after which the penalty of the unreachable routes will be down, by half here. This value must be between 1 and 45 minutes.

## Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

## Example

This command shows how to disable the dampening function:

```
DGS-3620-28SC:admin#  config bgp dampening state disable
Command: config bgp dampening state disable

Success.

DGS-3620-28SC:admin# show bgp dampening
Command: show bgp dampening

BGP Dampening State             :Enabled

BGP Dampening Route_Map         :dmp1
Half-life Time                  :15 mins
Reuse Value                     :500
Suppress Value                  :900
MAX Suppress Time               :60 mins
Unreachable route's Half-life   :15 mins

DGS-3620-28SC:admin# show bgp route
Command: show bgp route

 BGP Local Router ID is 20.90.90.90
 Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
 Origin codes: i - IGP, e - EGP, ? - incomplete
```

```
IP Address/Netmask        Gateway         Metric       LocPrf   Weight  Path

*>   20.0.0.0/8           0.0.0.0         0                     32768   i
*>   221.221.2.0/24       0.0.0.0         0                     32768   i
*d   221.221.252.0/24     1.1.1.2                                       1 40 i
*d   221.221.253.0/24     1.1.1.2                                       1 40 i

Total Entries: 4

DGS-3620-28SC:admin# config bgp dampening state disable
Command: config bgp dampening state disable

Success.

DGS-3620-28SC:admin# show bgp route
Command: show bgp route

 BGP Local Router ID is 20.90.90.90
 Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
 Origin codes: i - IGP, e - EGP, ? - incomplete

IP Address/Netmask        Gateway         Metric        LocPrf   Weight  Path

*>   20.0.0.0/8           0.0.0.0         0                      32768   i
*>   221.221.2.0/24       0.0.0.0         0                      32768   i
*    221.221.252.0/24     1.1.1.2                                        1 40 i
*    221.221.253.0/24     1.1.1.2                                        1 40 i

 Total Entries: 4

DGS-3620-28SC:admin#
```

## 12-18 show bgp dampening

### Description

This command is used to show the BGP dampening configurations.

### Format

**show bgp dampening**

### Parameters

None.

### Restrictions

None. (EI Mode Only Command)

### Example

Following example shows how to get the BGP dampening configurations:

```
DGS-3620-28SC:admin#  show bgp dampening
Command: show bgp dampening

BGP Dampening State              :Enabled

BGP Dampening Route_Map          :dmp1
Half Life Time                   :15 minutes
Reuse Value                      :750
Suppress Value                   :2000
MAX Suppress Time                :45 minutes
Unreachable route's Half-life    :15 mins



DGS-3620-28SC:admin#
```

## 12-19 config bgp peer_group

### Description

This command is used to configure the BGP peer group. The purpose of the neighbor peer group is to simplify the BGP neighbor configuration. The command is used to add an IP or to delete an IP from a BGP peer group. The peer group must be created using the "create neighbor peer group" command. The members must all be internal or external. If all the members of the BGP peer group are external, they are allowed to have different AS numbers. There are two kinds of the peer groups.

For the first kind or peer group, the remote AS is not set; members must be created as neighbors before it can be added to the peer group. When we configure the peer group's remote AS behind this, the member's remote AS will not change. For the second kind of peer group, the peer group has set a remote AS number. A member can be added to the peer group even if the member didn't have an AS number before. In this situation, the system will create a neighbor for the peer group's remote AS automatically. The member's remote AS will change to the configured peer group's remote AS, but the others' will not change, which is created as a neighbor before added to the peer group.

If a BGP peer belongs to a peer group, some attributes or actions can only be configured from the peer group. The following is a list of them: local_as, capability_orf_prefix_list, next_hop_self, route_reflector_client, send_community, soft_reconfiguration_inbound, remove_private_as, allowas_in, holdtime, keepalive, unsuppress_map, default_originate, filter_list for out direction, route_map for out direction, prefix_list for out direction.

On the contrary, some attributes or actions are allowed to be configured from both the peer group and the member. If they are configured from the member, the setting will overwrite the setting configured from the peer group.

Other attribute that can be set from an individual peer are as follows: description, filter_list for in direction, route_map for in direction, prefix_list for in direction, ebgp_multihop, session state, session activity, weight.

As for the above attributes, setting the attribute of a peer group will automatically affect the setting for individual peers in the peer group.

For session state, if the peer group is configure to disable, all the members can't set to enable. For session activity, can't set the peer group to disable.

As for the description attribute, setting the peer group will not affect the setting for an individual peer.

After this command is executed, all peers belonging to this peer group, which are generated with no indicated AS number, will change their AS number to the same value as the peer group's, stop and restarted values. If the peer group remote AS has a value of zero, it means "no remote_as", and members that are generated with no indicated AS number will be deleted.

### Format

**config bgp peer_group <peer_group_name 16> [remote_as <as_number 0-65535> | [add | delete] <ipaddr>]**

### Parameters

**<peer_group_name 16>** - This is the name of the BGP peer group. This name can be up to 16 characters long.

**remote_as** - The number of autonomous systems to which the peer group belongs to.
**<as_number 0-65535>** - Enter the remote AS value here. This value must be between 0 and 65535.

**add** - Specifies to add an IP address.
**delete** - Specifies to delete an IP address.

**<ipaddr>** - Enter the IP address to be added or deleted here.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

To delete a member from the peer group named local:

```
DGS-3620-28SC:admin#  config bgp peer_group local delete 10.2.2.2
Command: config bgp peer_group local delete 10.2.2.2

Success.

DGS-3620-28SC:admin#
```

To set a peer group named local remote_as to 50:

```
DGS-3620-28SC:admin#  config bgp peer_group local remote_as 50
Command: config bgp peer_group local remote_as 50

Success.

DGS-3620-28SC:admin#
```

## 12-20 create bgp neighbor

### Description

The command is used to create a BGP neighbor. Either a single router or a peer group can be created as neighbor.

If the created neighbor has a single IP address, the remote AS must be specified. A peer group must be specified of which this BGP speaking neighbor belongs to, and in this condition, a remote AS must be specified to the peer group first.

If the created neighbor is a peer group, then the remote AS cannot be specified here. The remote AS must specified by using the “config peer_group remote_as” command.

### Format

**create bgp neighbor [<ipaddr> [remote_as <as_number 1-65535> | peer_group <peer_group_name 16>] | peer_group <peer_group_name 16>]**

### Parameters

**<ipaddr>** - Enter the IP address of the BGP speaking neighbor here.

**remote_as** - The number of Autonomous Systems to which the neighbor belongs.
  **<as_number 1-65535>** - Enter the remote AS number here. This value must be between 1 and 65535.

**peer_group** - Specifies the peer group to be created and added as a neighbor.
  **<peer_group_name 16>** - Enter the peer group name here. This name can be up to 16 characters long.

**peer_group** - Specifies the peer group to be created and added as a neighbor.
  **<peer_group_name 16>** - Enter the peer group name here. This name can be up to 16 characters long.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

To create a neighbor peer whose address is 10.10.10.2:

```
DGS-3620-28SC:admin#  create bgp neighbor 10.10.10.2 remote_as 10
Command: create bgp neighbor 10.10.10.2 remote_as 10

Success.

DGS-3620-28SC:admin#
```

## 12-21 delete bgp neighbor

### Description

This command is used to delete the BGP neighbor.

### Format

**delete bgp neighbor [<ipaddr> | peer_group <peer_group_name 16> | all]**

### Parameters

**<ipaddr>** - Specifies the IP address of the neighbor that will be deleted.

**peer_group** - Specifies the peer group that will be deleted as a neighbor.
**<peer_group_name 16>** - Enter the peer group name here. This name can be up to 16 characters long.

**all** - Delete all BGP neighbors, including individual peers and peer groups.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

To delete a neighbor whose address is 10.10.10.2:

```
DGS-3620-28SC:admin#  delete bgp neighbor 10.10.10.2
Command: delete bgp neighbor 10.10.10.2

Success.

DGS-3620-28SC:admin#
```

## 12-22 config bgp neighbor

### Description

This command is used to configure the BGP neighbor’s description or password attribute.

### Format

**config bgp neighbor [<ipaddr> | peer_group <peer_group_name 16>] [description <desc 80> | clear_description | password <password 25> | clear_password]**

### Parameters

**<ipaddr>** - Specifies the IP address of the neighbor to be configured.

**peer_group** - Specifies the peer group to be configured.
**<peer_group_name 16>** - Enter the peer group name here. This name can be up to 16 characters long.

**description** - Associate a description with a neighbor. By default, the description is not specified.
**<desc 80>** - Enter the description value used here. This value can be up to 80 characters long.

**clear_description** - Removes the neighbor’s description.

**password** - Specifies to set the MD5 authentication password when a TCP connection between BGP neighbors are established. When BGP neighbors are created, password aren’t set by default.
**<password 25>** - Enter the password used here. This password can be up to 25 characters long.

**clear_password** - Specifies to clear the MD5 authentication password when a TCP connection between BGP neighbors are established.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

To configure a neighbor's description:

```
DGS-3620-28SC:admin#  config bgp neighbor 10.10.10.2 description EBGP-neighbor
Command: config bgp neighbor 10.10.10.2 description EBGP-neighbor

Success.

DGS-3620-28SC:admin#
```

## 12-23 config bgp neighbor session

### Description

The command is used to configure the state or neighbor's session activity for a BGP neighbor. If a neighbor is specified to be in the disabled state, it is equivalent to the case that the neighbor is deleted except when the neighbor configuration is kept.

### Format

**config bgp neighbor session [<ipaddr> | peer_group <peer_group_name 16>] [activity | state] [enable | disable]**

### Parameters

**<ipaddr>** - Specifies the IP address of the neighbor to be configured.

**peer_group** - Specifies the peer group to be configured.
**<peer_group_name 16>** - Enter the peer group name here. This name can be up to 16 characters long.

**state** - If state is changed from enabled to disabled, the session with the neighbor peer will be terminated.
**activity** - Specify the state for individual address family. By default, the setting is enabled for IPv4 address family.

**enable** - Specifies that the neighbor session state or the for individual address family state will be enabled.
**disable** - Specifies that the neighbor session state or the for individual address family state will be disabled.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

This example will shut down all the neighbors that are contained in the peer group “Campus”:

```
DGS-3620-28SC:admin# config bgp neighbor session peer_group Campus state
disable
Command: config bgp neighbor session peer_group Campus state disable

Success.

DGS-3620-28SC:admin#
```

This example shuts down the activity state of the neighbor 10.90.90.90:

```
DGS-3620-28SC:admin#  config bgp neighbor session 10.90.90.90 activity disable
Command: config bgp neighbor session 10.90.90.90 activity disable

Success.

DGS-3620-28SC:admin#
```

## 12-24 config bgp neighbor general

### Description

This command is used to configure the BGP neighbor’s general setting.

**ebgp_multihop:** This specifies the TTL of the BGP packet sent to the neighbor. If it is specified as 1, it will have a restriction that the neighbor must be directly connected to it.

**weight:** This specifies the weight that will be associated to the routes learned from the specified neighbor. The route with highest weight will be chosen as the preferred route. If the route map sets weight to a route, then this route map specified weight will override the weight specified by the BGP neighbor’s command. Weight is an attribute which is specified in the ingress direction, and is not an attribute to be advertised with the route. It is used to specify preference to routes received from a neighbor over another neighbor.

**soft_reconfiguration_inbound:** If the setting is enabled, the route updates sent from the specified neighbor will be stored. This storage is required for inbound soft reconfiguration. When a soft reset is requested for inbound sessions, the session will not be torn down, but the inbound routing table will be cleared. It needs to be rebuilt. If the soft reconfiguration inbound is enabled, then the routing table can be rebuilt based on the stored route update information. If the soft reconfiguration inbound is disabled, then the local router will send the route refresh requests to the neighbor to ask for the route refresh.

**next_hop_self:** If the next_hop_self option is enabled, the router will set the next_hop to itself when it advertises the routes to the specific neighbor. If the next_hop_self option is disabled, the next_hop attributes will not be changed. The behavior described here will be overridden by the set next hop statement if route map is applied to the neighbor in the out direction.

**remove_private_as:** The private Autonomous System numbers are from 64512 to 65535. If this setting is set to enable, the private AS number in AS path attribute of the BGP update packets will be dropped.

**allowas_in:** The BGP router will do AS path loop checks for the received BGP update packet. If the BGP router’s self AS appears in the AS path, it is identified as a loop and the packet will be discarded. If the allow-as setting is enabled, the BGP router’s self AS is allowed in the AS path list.

**default_originate:** If this setting is enabled, it will allow a BGP speaker (the local router) to send the default route 0.0.0.0/0 to a neighbor to use as the default route. If route map is specified, the default route will be injected if the route map contains a match IP address statement. If this setting is disabled, no default route will be sent to the neighbor. The default setting is disabled.

## Format

**config bgp neighbor general [<ipaddr> | peer_group <peer_group_name 16>] {ebgp_multihop <value 1-255> | weight [<value 0-65535> | default] | update_source [add | delete] ipif <ipif_name 12> | send_community [standard | none] | next_hop_self [enable | disable] | soft_reconfiguration_inbound [enable | disable] | remove_private_as [enable | disable] | allowas_in [enable {<value 1-10>} | disable] | default_originate [enable {route_map <map_name 16>} | disable]}(1)**

## Parameters

**<ipaddr>** - Specifies the IP address of the neighbor to be configured.

**peer_group** - Specifies the peer group to be configured.
**<peer_group_name 16>** - Enter the peer group name here. This name can be up to 16 characters long.

**ebgp_multihop** - (Optional) Specifies the TTL of BGP packet sent to the neighbor. For an EBGP neighbor the default setting is 1. This means only direct connected neighbors are allowed.
**<value 1-255>** - Enter the EBGP multi-hop value used here. This value must be between 1 and 255.

**weight** - (Optional) The valid range is from 0 to 65535. If this is not specified, the routes learned through another BGP peer will have a default weight of 0. Routes sourced by the local router have a weight of 32768. It cannot be changed.
**value <0-65535>** - Enter the weight value used here. This value must be between 0 and 65535.
**default** - Specifies that the default weight value will be used.

**update_source** - (Optional) Specifies an interface to be used by BGP sessions for the TCP connection. By default, this parameter is not set.
**add** - Specifies to add an interface.
**delete** - Specifies to delete an interface.

**ipif** - (Optional) Specifies the IP interface name used.
**<ipif_name 12>** - Enter the IP interface name used here. This name can be up to 12 characters long.

**send_community** - (Optional) This specifies the communities attribute to be sent to the BGP neighbor.
**standard** - Only standard communities will be sent.
**none** - No communities will be sent. The default value is none.

**next_hop_self** - (Optional) Enable or disable the next hop self attribute. By default, this setting is disabled.
**enable** - Specifies that the next-hop-self attribute will be enabled.
**disable** - Specifies that the next-hop-self attribute will be disabled.

**soft_reconfiguration_inbound** - (Optional) Specifies to enable or disable the inbound soft reconfiguration function. By default, this setting is disabled.
**enable** - Specifies that the soft re-configuration inbound option will be enabled.
**disable** - Specifies that the soft re-configuration inbound option will be disabled.

**remove_private_as** - (Optional) If this setting is set to enable, the private AS number in the AS path attribute of the BGP update packets will be dropped. By default, the setting is disabled.
**enable** - Specifies that the 'remove private AS' option will be enabled.
**disable** - Specifies that the 'remove private AS' option will be disabled.

**allowas_in** - (Optional) If the allow_as setting is enabled, the BGP router's self AS is allowed in the AS path list. By default, the allow_as setting is disabled. If no number is supplied, the default value of 3 times is used.

**enable** - Specifies that the allow AS-in option will be enabled.
**<value 1-10>** - Enter the allow AS-in value used here. This value must be between 1 and 10.
**disable** - Specifies that the allow AS-in option will be disabled.

**default_originate** - (Optional) Specifies to enable or disable the default originate function. By default, this setting is disabled.
**enable** - Specifies that the default originate function will be enabled.
**route_map** - Specifies the route map name.
**<map_name 16>** - Enter the route map name here. This name can be up to 16 characters long.
**disable** - Specifies that the default originate function will be disabled.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

This example shows how to configure the EBGP multi-hop to 2:

```
DGS-3620-28SC:admin#  config bgp neighbor general 10.100.200.1 ebgp_multihop 2
Command: config bgp neighbor general 10.100.200.1 ebgp_multihop 2

Success.

DGS-3620-28SC:admin#
```

## 12-25 config bgp neighbor timer

### Description

This command is used to configure the BGP neighbor’s timer attribute.

**advertisement_interval:** If an advertised route is flapping, this usually occurs when an interface is unstable, a lot of UPDATE and WITHDRAWN messages will be sent. One method to control the flooding of these messages is to set a minimum advertisement interval.

### Format

**config bgp neighbor timer [<ipaddr> | peer_group <peer_group_name 16>] {advertisement_interval [<sec 0-600> | default] | [keepalive <sec 0-65535> holdtime <sec 0-65535> | default_keepalive_holdtime] | as_origination_interval [<sec 1-600> | default] | connect [<sec 1-65535> | default]}(1)**

### Parameters

**<ipaddr>** - Specifies the IP address of the neighbor to be configured.

**peer_group** - Specifies the peer group to be configured.
**<peer_group_name 16>** - Enter the peer group name here. This name can be up to 16 characters long.

**advertisement_interval** - (Optional) It specifies the interval at which the BGP process sends update messages to its peer. If this value is set to zero, the update or withdrawn message will be sent immediately. The default value for IBGP peers is 5 seconds and for EBGP peers it is 30 seconds. When it is specified to default, the neighbor specific advertisement interval setting will be returned to the default setting.

**<sec 0-600>** - Enter the advertisement interval value here. This value must be between 0 and 600 seconds.
**default** - Specifies that the advertisement interval will be set to default.

**keepalive** - (Optional) This specifies the interval at which a keepalive message is sent to its peers. If the two routers, that build BGP connection, have different keepalive timers, the smaller keepalive timer will be used. If the keepalive is set to zero, then the keepalive message will not be sent out. By default, the timer is not specified. This neighbor specific setting will follow the global setting.
**<sec 0-65535>** - Enter the keep alive value here. This value must be between 0 and 65535.

**holdtime** - (Optional) The system will declare a peer as dead if not receiving a keepalive message until the hold time. If two routers, that builded a BGP connection, have different hold times, the smaller hold time will be used. If the holdtime is zero, then the holdtime will never expire. It is recommended that the holdtime value is 3 times that of keepalive timer. By default, the timer is not specified. This neighbor specific setting will follow the global setting.
**<sec 0-65535>** - Enter the hold time value here. This value must be between 0 and 65535.

**default_keepalive_holdtime** - (Optional) Clear the specification of the neighbor specific holdtime and keepalive setting.

**as_origination_interval** - (Optional) Minimum interval between the sending AS origination routing updates. The valid value is from 1 to 600. The default setting is 15 seconds.
**<sec 1-600>** - Enter the AS original interval value here. This value must be between 1 and 600.
**default** - Specifies that the default AS original interval value will be used.

**connect** - (Optional) Minimum interval BGP sends TCP connect requests to the peer after a TCP connection fail happens. The default setting is 120 seconds.
**<sec 1-65535>** - Enter the minimum interval BGP sends TCP connect requests to the peer after a TCP connection fail happens value here. This value must be between 1 and 65535.
**default** - Specifies that the default connect value will be used.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

This example shows how to configure the advertisement interval to 20 seconds:

```
DGS-3620-28SC:admin#  config bgp neighbor timer peer_group Campus
advertisement_interval 20
Command: config bgp neighbor timer peer_group Campus  advertisement_interval 20

Success.

DGS-3620-28SC:admin#
```

## 12-26 config bgp neighbor route_reflector_client

### Description

This command is used to configure the BGP's neighbor of the route reflector client. When the route reflector client is defined and the router reflection is enabled, the BGP router will act as the route reflector. The reflector and its client form a cluster. In a cluster, all the members must be iBGP connections with the reflector and vice versa. The reflector is the representative of the cluster. For the reflector, the iBGP connection is established by the "create bgp neighbor" command and the corresponding neighbor must be specified as the client by this command. For the client, the iBGP connection is established by the "create bgp neighbor" command.

When the router is in reflection mode, the router will exchange information with client neighbors in the reflection way and with the remaining neighbor in the ordinary way.

When the router is in non-reflection mode, the router will exchange information with all the neighbors in the non-reflection way.

An AS can have multiple clusters, and a cluster can have more than one reflector for redundancy purposes.

### Format

**config bgp neighbor route_reflector_client [<ipaddr> | peer_group <peer_group_name 16>] state [enable | disable]**

### Parameters

**<ipaddr>** - Specifies the IP address of the neighbor to be configured.

**peer_group** - Specifies the peer group to be configured.
**<peer_group_name 16>** - Enter the peer group name here. This name can be up to 16 characters long.

**state** - The specified neighbor will become the router reflector client. By default, this state is disabled.
**enable** - Specifies that the neighbor will become the router reflector client.
**disable** - Specifies that the neighbor will not become the router reflector client.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

This example shows how to add a neighbor as the route reflector client:

```
DGS-3620-28SC:admin#  config bgp neighbor route_reflector_client  10.10.10.2
state enable
Command: config bgp neighbor route_reflector_client  10.10.10.2 state enable


Success.


DGS-3620-28SC:admin#
```

## 12-27 config bgp neighbor map

### Description

The command is used to configure the route map related setting for a BGP neighbor. When a route map is applied by the route_map command, it enforces the route policy. When it is applied by the unsuppress_map command, the suppressed route which matches the permit rule will be unsuppressed. It provides a manipulation of routers per neighbor. If a route map is configured relating to a BGP neighbor but the route map doesn’t exist, it means deny any. If the route map exists but has no filter entry defined, it will permit all.

### Format

**config bgp neighbor map [<ipaddr> | peer_group <peer_group_name 16>] {unsuppress_map [add | delete] <map_name 16> | route_map [in | out] [add | delete] <map_name 16>}(1)**

### Parameters

**<ipaddr>** - Specifies the IP address of the neighbor to be configured.

**peer_group** - Specifies the peer group to be configured.
  **<peer_group_name 16>** - Enter the peer group name here. This name can be up to 16 characters long.

**unsuppress_map** - (Optional) Name of a route map used to selectively advertise routers previously suppressed by the aggregate_address command.
  **add** - Specifies that a route map will be added.
  **delete** - Specifies that a route map will be deleted.
  **<map_name 16>** - Enter the unsurpress map name here. This name can be up to 16 characters long.

**route_map** - (Optional) Specify the route map to be applied to the incoming or outgoing routes.
  **in** - Specifies the incoming routes from the neighbor.
  **out** - Specifies the outgoing routes sent to the peer.
  **add** - Specifies that a route map will be added.
  **delete** - Specifies that a route map will be deleted.
  **<map_name 16>** - Enter the unsurpress map name here. This name can be up to 16 characters long.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

This example shows how to configure the unsuppress map of peer group “Campus” to Profile1:

```
DGS-3620-28SC:admin#  config bgp neighbor map peer_group Campus  unsuppress_map
add Profile1
Command: config bgp neighbor map peer_group Campus  unsuppress_map add Profile1


Success.


DGS-3620-28SC:admin#
```

## 12-28 config bgp neighbor filter

### Description

The command is used to configure the filter related setting for a BGP neighbor.

**filter_list:** If the filter_list doesn’t exist or does exist but have no filter entry, it means deny any.

**prefix_list:** If the prefix_list doesn’t exist, it means deny any. If the prefix_list does exist but have no filter entry defined, it will permit all.

**capability_orf_prefix_list:** BGP Outbound Route Filter Capability allows one BGP router to install its configured inbound prefix_list filter on to the remote BGP router. This is used for reducing the amount of unwanted routing updates from the remote peer.

## Format

**config bgp neighbor filter [<ipaddr> | peer_group <peer_group_name 16>] {filter_list [in | out] [add | delete] <list_name 16> | prefix_list [in | out] [add | delete] <list_name 16> | capability_orf_prefix_list [receive | send | both | none]}(1)**

## Parameters

**<ipaddr>** - Specifies the IP address of the neighbor to be configured.

**peer_group**- Specifies the peer group to be configured.
**<peer_group_name 16>** - Enter the peer group name here. This name can be up to 16 characters long.

**filter_list** - (Optional) Specifies the name of an as_path access_list to be applied as a filter. The filtering can be applied to incoming routes or outgoing routes.
**in** - Specifies that the filter specified will be used for incoming traffic.
**out** - Specifies that the filter specified will be used for outgoing traffic.
**add** - Specifies that a filter list will be added.
**delete** - Specifies that a filter list will be deleted.
**<list_name 16>** - Enter the filter list name here. This name can be up to 16 characters long.

**prefix_list** - (Optional) Specifies the name of a prefix_list to be applied as a filter. The filtering can be applied to incoming routes or outgoing routes.
**in** - Specifies that the filter specified will be used for incoming traffic.
**out** - Specifies that the filter specified will be used for outgoing traffic.
**add** - Specifies that a filter list will be added.
**delete** - Specifies that a filter list will be deleted.
**<list_name 16>** - Enter the prefic list name here. This name can be up to 16 characters long.

**capability_orf_prefix_list** - (Optional) Used to configure an outbound route filter prefix list capability. It can be sent with the following values:
**receive** - Enables the ORF prefix list capability in the receiving direction. The local router will install the prefix filter list notified by the remote router.
**send** - Enables the ORF prefix list capability in the sending direction. The local router will notify the remote router for the ORF prefix list capability.
**both** - Enables the ORF prefix list capability in both received and send directions.
**none** - Disable the ORF prefix list capability in both received and send directions.

## Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

## Example

This example shows how to configure the BGP neighbor ingress filter list for the peer group "Campus" to List1:

```
DGS-3620-28SC:admin#  config bgp neighbor filter peer_group Campus  filter_list
in add List1
Command: config bgp neighbor filter peer_group Campus  filter_list in add List1


Success.


DGS-3620-28SC:admin#
```

## 12-29 show bgp peer_group

### Description

The command is used to show the information of the BGP peer group.

### Format

**show bgp peer_group {<peer_group_name 16>}**

### Parameters

| |
|---|
| **peer_group** - (Optional) Name of the BGP peer group. The length is up to 16 bytes.<br>**<peer_group_name 16>** - Enter the BGP peer group name here. This name can be up to 16 characters long. |
| It means to display all the BGP peer groups' information that doesn't specify the peer group name. |

### Restrictions

None. (EI Mode Only Command)

### Example

Show the information of the BGP peer group local1:

```
DGS-3620-28SC:admin# create bgp neighbor peer_group local1
Command: create bgp neighbor peer_group local1

Success.

DGS-3620-28SC:admin# create bgp neighbor 10.2.2.2 remote_as 10
Command: create  bgp neighbor 10.2.2.2 remote_as 10

Success.

DGS-3620-28SC:admin# config bgp peer_group local1 add 10.2.2.2
Command: config bgp peer_group local1 add 10.2.2.2

Success.

DGS-3620-28SC:admin# show bgp peer_group local1
Command: show bgp peer_group local1

BGP Peer Group :local1
-----------------------------------------------------------------------
Description                   :
Session                       : Enabled
Session Activity              : Enabled
Members                       : 10.2.2.2
Remote AS                     : Not Set
Advertisement Interval        : 30 seconds
```

```
Keepalive Interval            : 60 seconds
Holdtime Interval             : 180 seconds
AS Origination Interval       : 15 seconds
Connect Retry Interval        : 120 seconds
EBGP Multihop                 : 1
Weight                        : 0
Next Hop Self                 : Disabled
Route Reflector Client        : Disabled
Send Community                : None
Remove Private As             : Disabled
AllowAS In                    : Disabled
Soft Reconfiguration Inbound  : Disabled
Default Originate             : Disabled
Outbound Route Filter (ORF) type (64) Prefix list:
        Send Mode         : Disabled
        Receive Mode      : Disabled
Prefix Max Count              : 12000
Prefix Warning Threshold      : 75
Prefix Warning Only           : Disabled

Total peer_group number : 1

DGS-3620-28SC:admin#
```

## 12-30 config bgp route_reflector cluster_id

### Description

This command is used to configure the BGP process's global attribute. The route reflector and its clients together form a cluster. When a single route reflector is deployed in a cluster, the cluster is identified by the router ID of the route reflector.

When the cluster ID is 0.0.0.0, the cluster is identified by the router ID. Otherwise, the cluster is identified by the cluster ID.

The BGP cluster_id command is used to assign a cluster ID to a route reflector when the cluster has one or more route reflectors. Multiple route reflectors are deployed in a cluster to increase redundancy and to avoid a single point of failure. When multiple route reflectors are configured in a cluster, they must be configured with the same cluster ID. This allows all route reflectors in the cluster to recognize updates from peers in the same cluster and reduces the number of updates that needs to be stored in BGP routing tables.

This command is only required for the reflector and not the client.

### Format

**config bgp route_reflector cluster_id <ipaddr>**

### Parameters

**cluster_id** - Specifies the IP address of the cluster ID. Setting the cluster ID to 0.0.0.0 will remove specifications of the cluster ID. The default value is 0.0.0.0.
**<ipaddr>** - Enter the cluster ID's IP address here.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

This example shows how to configure the cluster ID:

```
DGS-3620-28SC:admin#  config bgp route_reflector cluster_id 10.100.200.1
Command: config bgp route_reflector cluster_id 10.100.200.1

Success.

DGS-3620-28SC:admin#
```

## 12-31 config bgp client_to_client_reflection

### Description

This command is used to configure the BGP client to client reflection setting. If the reflection is disabled, then the router will not reflect routes from the route reflect client to other route reflect clients, but it will still send routes received from a non-reflecting client to a reflecting client.

### Format

**config bgp client_to_client_reflection [enable | disable]**

### Parameters

**enable** - The reflector will operate in reflector mode.
**disable** - The reflector will operate in non-reflector mode.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

This example shows how to disable the client to client reflection:

```
DGS-3620-28SC:admin#  config bgp client_to_client_reflection disable
Command: config bgp client_to_client_reflection disable

Success.

DGS-3620-28SC:admin#
```

## 12-32 config bgp confederation identifier

### Description

This command is used to configure the BGP confederation. A confederation, which is represented by an AS, is a group of the sub AS.

A confederation can be used to reduce the internal BGP (iBGP) mesh by dividing a large single AS into multihop sub AS. External peers interact with the confederation as if it is a single AS.

Each sub AS is fully meshed within itself and it has connections to other sub AS within the confederation. The next hop, Multi Exit Discriminator (MED), and local preference information is preserved throughout the confederation, allowing you to retain a single Interior Gateway Protocol (IGP) for all the autonomous systems.

### Format

**config bgp confederation identifier <as_number 0-65535>**

### Parameters

**<as_number 0-65535>** - Autonomous System numbers which we use to specify a BGP confederation. If it is set to zero, the BGP confederation number is deleted. By default, this setting is zero. This value must be between 0 and 65535.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

To create a confederation, AS number is 20:

```
DGS-3620-28SC:admin#  config bgp confederation identifier 20
Command: config bgp confederation identifier 20

Success.

DGS-3620-28SC:admin#
```

## 12-33 config bgp confederation peers

### Description

The command is used to configure multiple adjacent Autonomous Systems in a confederation. The Autonomous Systems specified in this command are visible internally to the confederation. Each Autonomous System is fully meshed within itself or configures route reflector.

### Format

**config bgp confederation peers [add | delete] <aspath_list>**

### Parameters

**peers** - Specifies that a peer will be added or deleted.
- **add** - Specifies that a peer will be added.
- **delete** - Specifies that a peer will be deleted.
- **<aspath_list>** - Enter the AS number for BGP peers that will belong to the confederation here.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

To add two confederation peers, AS number are 50000 and 50001:

```
DGS-3620-28SC:admin#  config bgp confederation peers add 50000, 50001
Command: config bgp confederation peers add 50000, 50001

Success.

DGS-3620-28SC:admin#
```

## 12-34 clear bgp

### Description

This command is used to initiate a hard reset or a soft reset for a connection. If a hard reset is applied to the inbound session, the inbound session will be teared down and the local inbound routing table and the remote outbound routing table will be cleared. If a soft reset is applied to the inbound session, the session will not be rebuilded but the local inbound routing table will be cleared and needs to be rebuilt. If a soft reconfiguration inbound is enabled, then the routing table can be rebuilt based on the stored route updates information. If a soft reconfiguration inbound is disabled, then the local router will send the route refresh request to the neighbor to ask for the route refresh. When the inbound session is to soft reset with the prefix filter option, and capability_orf_prefix_list is enabled in the send direction, then the local BGP will send 'clear the routing table', and notify the remote neighbor for the prefix_filter. This is a way to notify the neighbor of the prefix filter whenever a change is made to the prefix filter.

### Format

**clear bgp [all | ipaddr <ipaddr> | as <as_number 1-65535> | peer_group <peer_group_name 16> | external] {soft {[in {prefix_filter} | out]}}**

### Parameters

**all** - Specifies that all current BGP sessions will be reset.

**ipaddr** - Specifies to reset the session with the specified neighbor.
- **<ipaddr>** - Enter the IP address used for this configuration here.

**as** - Specifies to reset sessions with BGP peers in the specified Autonomous System.
- **<as_number 1-65535>** - Enter the AS number used here. This value must be between 1 and 65535.

**peer_group** - Specifies to reset a peer group.

**<peer_group_name 16>** - Enter the peer group name here. This name can be up to 16 characters long.

**external** - All eBGP sessions will be reset.

**soft** - (Optional) Initiates a soft reset. Does not tear down the session.

**in** - Initiates inbound reconfiguration. If neither in nor out keywords are specified, both inbound and outbound sessions are reset.

**prefix_filter** - The local site configured prefix filter will be notified to the remote neighbor when inbound soft reset is applied.

**out** - Initiates outbound reconfiguration.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

To reset all Border Gateway Protocol (BGP) connections:

```
DGS-3620-28SC:admin# clear bgp all
Command: clear bgp all

Success.

DGS-3620-28SC:admin#
```

## 12-35 clear bgp dampening

### Description

This command clears the route dampening information stored in the routing table. If no parameters are specified, the dampening information for the entire routing table will be cleared.

### Format

**clear bgp dampening {[<ipaddr> | <network_address>]}**

### Parameters

**<ipaddr>** - (Optional) Specifies an IPv4 address to clear the dampening information.

**<network_address>** - (Optional) Specifies an IPv4 network to clear the dampening information.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

To clear route dampening information for network 192.168.10.0/24 and free suppressed routes:

```
DGS-3620-28SC:admin#  clear bgp dampening 192.168.10.0/24
Command: clear bgp dampening 192.168.10.0/24

Success.

DGS-3620-28SC:admin#
```

## 12-36 create bgp as_path access_list

### Description

The command is used to create an Autonomous System path access list. You can apply an Autonomous System path access lists to both inbound and outbound routes exchanged by a BGP peer session.

### Format

**create bgp as_path access_list <list_name 16>**

### Parameters

**access_list** - Specifies the AS path access list name.
**<list_name 16>** - Enter the AS path access list name here. This name can be up to 16 characters long.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

The following example creates an Autonomous System path access list:

```
DGS-3620-28SC:admin#  create bgp as_path access_list test
Command: create bgp as_path access_list test

Success.

DGS-3620-28SC:admin#
```

## 12-37 config bgp as_path access_list

### Description

This command is used to configure matching rules for an Autonomous System path access list using regular expressions.

### Format

**config bgp as_path access_list <list_name 16> [add | delete] <regexp_str 80> [deny | permit]**

### Parameters

**access_list** - Specifies the AS path access list name.
**<list_name 16>** - Enter the AS path access list name here. This name can be up to 16 characters long.

**add** - Specifies to add a matching rule.
**delete** - Specifies to delete a matching rule.

**<reg_express>** - Regular expression that defines the as_path filter.

**deny** - Denies advertisement based on matching conditions.
**permit** - Permits advertisement based on matching conditions.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

This example configures a matching rule for an AS path access list:

```
DGS-3620-28SC:admin#  create bgp as_path access_list test
Command: create bgp as_path access_list test

Success.

DGS-3620-28SC:admin# config bgp as_path access_list test add (_64[6-9][0-9][0-
9]_|_65[0-9][0-9][0-9]_) deny
Command: config bgp as_path access_list test add (_64[6-9][0-9][0-9]_|_65[0-
9][0-9][0-9]_) deny

Success.

DGS-3620-28SC:admin# config bgp as_path access_list test add .* permit
Command: config bgp as_path access_list test add .* permit

Success.

DGS-3620-28SC:admin#
```

## 12-38 delete bgp as_path access_list

### Description

This command is used to delete an Autonomous System path access list.

### Format

**delete bgp as_path access_list [list_name <list_name 16> | all]**

### Parameters

**list_name** - Specifies the AS path access list name.
**<list_name 16>** - Enter the AS path access list name here. This name can be up to 16 characters long.

**all** - Specifies that all the AS path lists will be used.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

This example deletes a matching rule for an AS path access list:

```
DGS-3620-28SC:admin# delete bgp as_path access_list list_name test
Command: delete bgp as_path access_list list_name test

Success.

DGS-3620-28SC:admin#
```

## 12-39 show bgp as_path access_list

### Description

This command displays the Autonomous System path’s access list. If a specific access list is not specified, all AS path access lists will be displayed.

### Format

**show bgp as_path access_list {<list_name 16>}**

### Parameters

**access_list** - Specifies the AS path access list name.

**<list_name 16>** - (Optional) Enter the AS path access list name here. This name can be up to 16 characters long.

### Restrictions

None. (EI Mode Only Command)

### Example

This example displays an AS path access list:

```
DGS-3620-28SC:admin#  show bgp as_path access_list 1
Command: show bgp as_path access_list 1

BGP AS Path Access List : 1
deny (_64[6-9][0-9][0-9]_|_65[0-9][0-9][0-9]_)
permit 33

Total Filter Entries: 2

Total AS Path Access List Number: 1

DGS-3620-28SC:admin#
```

## 12-40 create bgp community_list

### Description

This command is used to create a BGP community list.

### Format

**create bgp community_list [standard | expanded] <list_name 16>**

### Parameters

| |
|---|
| **standard** - Creates a standard named community list.<br>**expanded** - Creates an expanded named community list. |
| **<list_name 16>** - Enter the name of the community list that will be created here. This name can be up to 16 characters long. |

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

To create a standard BGP community list:

```
DGS-3620-28SC:admin#  create bgp community_list standard list1
Command: create bgp community_list standard list1

Success.

DGS-3620-28SC:admin#
```

## 12-41 config bgp community_list

### Description

This command is used to configure the matching rule for the community access list. Mutliple rules can be defined for a community list. Each rule is either in the permit form or in the deny form. Each rule in the standard community list contains one community. A community string, which contains multiple communities, can be defined for a rule. A Route can be associated with a community string. To match a rule, two community strings must exact match. The built-in community strings including internet, local_as, no_advertise, and no_export. The user-defined community is 4-bytes long, with the leading two bytes representing the AS number and the trailing two bytes representing a user defined number. BGP community attributes exchanged between BGP peers is controlled by the neighbor send-community command. The community string associated with routes can be controlled by the route map. By default, the community string "internet" will be sent. If the route map sets a community string, this community string will be added to the existing community string associated with the route. If permit rules exist in an access list, then routes with community that does not match any rule in the list will be denied. If there are no rules or only deny rules configured for the community list, all routes will be denied.

## Format

**config bgp community_list [standard <list_name 16> [add | delete] {internet | local_as | no_advertise | no_export | community_set <community_set 80>}(1) [deny | permit] | expanded <list_name 16> [add | delete] <regexp_str 80> [deny | permit]]**

## Parameters

**standard** - Configures a standard community list.
**<list_name 16>** - Enter the standard community list name here. This name can be up to 16 characters long.

**add** - Adds a rule to the community list.
**delete** - Deletes a rule from the community list.

**internet** - (Optional) Routes with this community will be sent to all peers either internal or external.

**local_as** - (Optional) Routes with this community will be sent to peers in the same AS, but will not be sent to peers in another sub AS in the same confederation and to the external peers.

**no_advertise** - Routes with this community will not be advertised to any peer either internal or external.

**no_export** - (Optional) Routes with this community will be sent to peers in the same AS or in other sub Autonomous Systems within a confederation, but will not be sent to an external BGP (eBGP) peer.

**community_set** - (Optional) A community is 4 bytes long, including the 2 bytes's for the Autonomous System's number and 2 bytes for the network number This value is configured with two 2-byte numbers separated by a colon. The valid range of both number are from 1 to 65535. A community set can be formed by multiple communities, separated by a comma.
**<community_set 80>** - Enter the community set value here. This value can be up to 80 characters long.

**deny** - To deny the routes if rule is matched.
**permit** - To permit the routes if rule is matched.

**expanded** - Configures an expanded community list.
**<list_name 16>** - Name of community list to be configured.

**add** - Adds a rule to the community list.
**delete** - Deletes a rule from the community list.

**<regexp_str 80>** - Enter the registration expiry string value here. This value can be up to 80 characters long.

**deny** - To deny the routes if rule is matched.
**permit** - To permit the routes if rule is matched.

## Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

This example creates a standard community list and configures permits routes from the network 10 in the Autonomous System 50000:10

```
DGS-3620-28SC:admin#  create bgp community_list standard list1
Command: create bgp community_list standard list1

Success.

DGS-3620-28SC:admin#  config bgp community_list standard list1 add
community_set 50000:10 permit
Command: config bgp community_list standard list1 add community_set 50000:10
permit

Success.

DGS-3620-28SC:admin#
```

## 12-42 delete bgp community_list

### Description

This command is used to delete a BGP community list.

### Format

**delete bgp community_list [list_name <list_name 16> | all]**

### Parameters

**list_name** - Specifies the name of the community list to be deleted.
**<list_name 16>** - Enter the community list name here. This name can be up to 16 characters long.
**all** - Specifies that all the community lists will be used.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

This example deletes the community list named as list1:

```
DGS-3620-28SC:admin# delete bgp community_list list_name test1
Command: delete bgp community_list list_name test1

Success.

DGS-3620-28SC:admin#
```

## 12-43 show bgp community_list

### Description

This command is used to show a BGP community list.

### Format

**show bgp community_list {<list_name 16>}**

### Parameters

**community_list** - Specifies the name of community list to be displayed.

**<list_name 16>** - (Optional) Enter the community list name here. This name can be up to 16 characters long.

### Restrictions

None. (EI Mode Only Command)

### Example

This example displays the community list name as list1:

```
DGS-3620-28SC:admin#  create bgp community_list standard list1
Command: create bgp community_list standard list1

Success.

DGS-3620-28SC:admin# config bgp community_list standard list1 add community_set
50000:10 permit
Command: config bgp community_list standard list1 add community_set 50000:10
permit

Success.

DGS-3620-28SC:admin#  show bgp community_list list1
Command: show bgp community_list list1

Community List Name: list1
--------------------------------
Type                : standard
permit  :  50000:10

DGS-3620-28SC:admin#
```

## 12-44 show bgp route

### Description

This command is used to display route entries in the Border Gateway Protocol (BGP) routing table

## Format

**show bgp route {[regexp <desc 80> | inconsistent_as | cidr_only | filter_list <list_name 16> | route_map <map_name 16> | community {community_set <community_set 80> | local_as | no_advertise | no_export | internet} {exact_match} | community_list <list_name 16> {exact_match} | ipaddress <ipaddr> | network <network_address> {longer_prefixes} | prefix_list <list_name 16>]}**

## Parameters

**regexp** - (Optional) Display routes matching the AS path regular expression.
**<desc 80>** - A regular expression to match the BGP AS paths, must enclose in the quotes. Can include blank space. The string can be up to 80 characters long.

**inconsistent_as** - (Optional) Display the routes if they have of same prefix and different AS path originate.

**cidr_only** - (Optional) Display only routes with non-natural network masks.

**filter_list** - (Optional) Display routes conforming to the filter list.
**<list_name 16>** - Enter the filter list name here. This name can be up to 16 characters long.

**route_map** - (Optional) Display routes matching the route map.
**<map_name 16>** - Enter the route map name here. This name can be up to 16 characters long.

**community** - (Optional) Display routes matching the communities.

**community_set** - (Optional) Specifies the community set here.
**<community_set 80>** - Enter the community set here. This value can be up to 80 characters long.

**local_as** - (Optional) Do not send outside local AS (well-known community).

**no_advertise** - (Optional) Do not advertise to any peer (well-known community).

**no_export** - (Optional) Do not export to next AS (well-known community).

**internet** - (Optional) Send to the Internet (well-known community>.

**exact_match** - (Optional) If specified, communities.need to match exactly.

**community_list** - (Optional) A community is in the form of <as_number> : <udn_number>. A community string can be formed by multiple communities, separated by a comma.
**<list_name 16>** - Enter the community list name here. This name can be up to 16 characters long.

**exact_match** - (Optional) If specified, communities.need to match exactly.

**ipaddress** - (Optional) Display the host route that matches the specified IP address.
**<ipaddr>** - Enter the IP address to be displayed here.

**network** - (Optional) Display the route that matches the specified network address.
**<network_address>** - Enter the network address to be displayed here.

**longer_prefixes** - (Optional) If specified, more specific routes will be also displayed.

**prefix_list** - (Optional) Display routes conforming to the prefix list
**<list_name 16>** - Specifies the list name for the specified prefix list, IP access list, or route map.

## Restrictions

None. (EI Mode Only Command)

## Example

The following example shows how to get the BGP route information:

```
DGS-3620-28SC:admin#  show bgp route
Command:  show bgp route


BGP local router ID is 10.0.40.1
```

```
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? – incomplete

    IP Address/Netmask  Gateway      Metric   LocPrf  Weight   Path

*>  10.10.10.0/24       172.16.10.1  0        0       300     10 i
*>  10.10.20.0/24       172.16.10.1  0        0       300     10 i
*   10.20.10.0/24       172.16.10.1  0        0       300     10 i
*dh 30.10.1.1/24        172.3.3.2    100      50      200     20 i

Total Entries :4

DGS-3620-28SC:admin#  show bgp route cidr_only
Command: show bgp route cidr_only
BGP local router ID is 172.16.73.131
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? – incomplete

    IP Address/Netmask  Gateway        Metric   LocPrf  Weight   Path

*> 192.0.0.0/8          172.16.72.24   0        1878    200      ?
*> 172.16.0.0/14        172.16.72.30   0        108     200      ?

Total Entries :2

DGS-3620-28SC:admin#  show bgp route community_list community_list_one
Command: show bgp route community_list community_list_one

BGP local router ID is 192.168.32.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? – incomplete

    IP Address/Netmask  Gateway      Metric   LocPrf      Weight    Path

* i10.3.0.0/16         10.0.22.1         0       100      1800      1239 ?
*>i10.3.0.0/16         10.0.16.1         0       100      1800      1239 ?
* i10.6.0.0/16         10.0.22.1         0       100      1800      690  568 ?

Total Entries :3


DGS-3620-28SC:admin#  show bgp route filter_list filter_list_one
Command: show bgp route filter_list filter_list_one

BGP local router ID is 172.16.72.24
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? – incomplete

    IP Address/Netmask  Gateway      Metric   LocPrf  Weight   Path

*  172.16.0.0/24        172.16.72.30                  0        109 108 ?
*  172.16.1.0/24        172.16.72.30                  0        109 108 ?
*  172.16.11.0/24       172.16.72.30                  0        109 108 ?
*  172.16.14.0/24       172.16.72.30                  0        109 108 ?
*  172.16.15.0/24       172.16.72.30                  0        109 108 ?
*  172.16.16.0/24       172.16.72.30                  0        109 108 ?

Total Entries :6

DGS-3620-28SC:admin#  show bgp route regexp “108$”
Command:  show bgp route regexp “108$”

BGP local router ID is 172.16.72.24
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? – incomplete

    IP Address/Netmask  Gateway      Metric   LocPrf  Weight   Path

s  172.16.0.0/24        172.16.72.30                  0        109 108 ?
s  172.16.0.0/24        172.16.72.31                  0        109 108 ?
*  172.16.1.0/24        172.16.72.30                  0        109 108 ?
*  172.16.11.0/24       172.16.72.30                  0        109 108 ?
*  172.16.14.0/24       172.16.72.30                  0        109 108 ?
*  172.16.15.0/24       172.16.72.30                  0        109 108 ?
*  172.16.16.0/24       172.16.72.30                  0        109 108 ?

Total Entries :7

DGS-3620-28SC:admin#  show bgp route inconsistent_as
Command:  show bgp route inconsistent_as

BGP local router ID is 172.16.72.24
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? – incomplete

    IP Address/Netmask  Gateway      Metric   LocPrf  Weight   Path

*  172.16.1.0/24        172.16.72.30                  0        109 108 i
                        172.16.72.21                  0        110 101 i
*  172.16.11.0/24       172.16.72.30                  0        109 108 i
                        172.16.72.10                  0        104 105 i
                        172.16.72.10                  0        104 103 i
Total Entries :2

DGS-3620-28SC:admin# show bgp route network 2.2.2.0/24
Command: show bgp route network 2.2.2.0/24

BGP routing table entry for 2.2.2.0/24
Paths:(1 available, best #1, table: Default_IP_Routing_Table,not advertised to
any
 peer.)
 Not advertised to any peer.

  as path is:Local
```

```
   next hop is:0.0.0.0 ,from 0.0.0.0 (local router_id is:192.168.1.1)
   origin IGP, metric 100, localpref 0, weight 32768, sourced, best
   Community: no_advertise

DGS-3620-28SC:admin#
```

## 12-45 show bgp neighbors

### Description

This command is used to display BGP and TCP connections with the BGP neighbor or routing table entries containing a BGP neighbor. To display BGP and TCP connection information for neighbor sessions, or routing table entries with BGP neighbor. For BGP, this includes detailed neighbor attribute, capability, path, and prefix information. For TCP, this includes statistics related to BGP neighbor session establishment and maintenance.

### Format

**show bgp neighbors {<ipaddr> {[advertised_routes | received_routes | routes | received_prefix_filter | statistics]}}**

### Parameters

**neighbors** - Detailed information about TCP and BGP neighbor connections.
**<ipaddr>** - (Optional) Enter the IP address used for the configuration here.

**advertised_routes** - (Optional) Displays the routes advertised to a BGP neighbor.

**received_routes** - (Optional) Displays the routes received from this neighbor.

**routes** - (Optional) Displays routes in the routing table learned from the neighbor.

**received_prefix_filter** - (Optional) Displays the prefix filter information that is received from a BGP neighbor.

**statistics** - (Optional) Displays the statistical information learned.

### Restrictions

None. (EI Mode Only Command)

### Example

To show the BGP neighbor or routes relative to one neighbor:

```
DGS-3620-28SC:admin# show bgp neighbor 10.10.10.2
Command: show bgp neighbor 10.10.10.2

BGP neighbor: 10.10.10.2 (Internal Peer)
-----------------------------------------------
Session State              : Enabled
Session Activity           : Enabled
Remote AS                  : 1
Remote Router ID           : 192.168.252.252
BGP State                  : Established ( UP for 00:24:25)
Hold Time                  : 180 Seconds
Keepalive Interval         : 60 Seconds
Advertisement Interval     : 5 Seconds
```

```
AS Origination Interval       : 15 seconds
Connect Retry Interval        : 120 seconds
EBGP Multihop                 : 2
Weight                        : 100
Next Hop Self                 : Disabled
Remove Private As             : Disabled
Allowas In                    : Enabled (Num: 3)
Address Family IPv4 Unicast
IPv4 Unicast                  : None
Soft Reconfiguration Inbound  : Enabled
Send Community                : None
Default Originate             : Enabled
Incoming Update Prefix List   : prelist1
Incoming Update Filter List   : ASlist1
Route Map for outgoing Routes : routemap1
Unsuppress Route Map          : us_routmp1
Outbound Route Filter (ORF) type (64) Prefix list:
   Send Mode                  : Enabled
   Receive Mode               : Disable
Prefix Max Count              : 12000
Prefix Warning Threshold      : 75
Prefix Warning Only           : Disabled

DGS-3620-28SC:admin#  show bgp neighbor 172.16.232.178 advertised_routes
Command:  show bgp neighbor 172.16.232.178 advertised_routes

BGP local router ID is 172.16.232.181
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

    IP Address/Netmask  Gateway          Metric   LocPrf  Weight   Path

*>i 10.0.0.0/24         172.16.232.179   0        100     0        ?
*>  10.20.2.0/24        0.0.0.0          0        32768            i

Total Entries :2

DGS-3620-28SC:admin#  show bgp neighbor 172.16.232.178 received_routes
Command:  show bgp neighbor 172.16.232.178 received_routes

BGP local router ID is 172.16.232.181
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

    IP Address/Netmask  Gateway          Metric   LocPrf  Weight   Path

*>i10.0.0.0/24          172.16.232.179   0        100     0        ?
*> 10.20.2.0/24         0.0.0.0          0        32768            i

Total Entries :2

DGS-3620-28SC:admin# show bgp neighbors 172.16.232.178 received_prefix_filter
```

```
Command: show bgp neighbors 172.16.232.178 received_prefix_filter

   Ip prefix-list 172.16.232.181: 1 entries
   Seq 5 deny 10.0.0.0/8 le 32

Total Entries :1

DGS-3620-28SC:admin# show bgp neighbors 172.16.232.178 routes
Command: show bgp neighbors 172.16.232.178 routes

BGP local router ID is 10.0.40.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? – incomplete

    IP Address/Netmask  Gateway      Metric   LocPrf  Weight   Path

*>  10.10.10.0/24   172.16.10.1    0       0        300         10 i
*>  10.10.20.0/24   172.16.10.1    0       0        300         10 i
*   10.20.10.0/24   172.16.10.1    0       0        300         10 i
*dh 30.10.1.1/24    172.3.3.2      100     50       200        20 i

Total Entries :4

DGS-3620-28SC:admin#
```

## 12-46 show bgp dampened_routes

### Description

This command is used to display dampened entries in the Border Gateway Protocol (BGP) routing table.

### Format

**show bgp dampened_routes**

### Parameters

None.

### Restrictions

None. (EI Mode Only Command)

### Example

To show the BGP dampened routes' information:

```
DGS-3620-28SC:admin#  show bgp dampened_routes
Command:  show bgp dampened_routes

BGP local router ID is 172.29.232.182
Status codes: s suppressed, d damped, h history, * valid, > best, i -internal
Origin codes: i - IGP, e - EGP, ? - incomplete
  Network              From             Reuse        Path

*d 10.0.0.0/16      172.16.232.177   00:18:4     100 ?
*d 10.2.0.0/16      172.16.232.177   00:28:5     100 ?

Total Entries :2

DGS-3620-28SC:admin#
```

## 12-47 show bgp flap_statistics

### Description

This command is used to display flap entries in the Border Gateway Protocol's (BGP) routing table

### Format

**show bgp flap_statistics**

### Parameters

None.

### Restrictions

None. (EI Mode Only Command)

### Example

To show flap BGProutes information:

```
DGS-3620-28SC:admin#  show bgp flap_statistics
Command:show bgp flap_statistics

BGP local router ID is 172.29.232.182
Status codes: s suppressed, d damped, h history, * valid, > best, i -internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network            From               Flaps   Duration    Reuse     Path

*d 10.0.0.0/16        172.29.232.177     4       00:13:31    00:18:10   100 ?
*d 10.2.0.0/16        172.29.232.177     4       00:02:45    00:28:20   100 i

Total Entries :2

DGS-3620-28SC:admin#
```

## 12-48 show bgp

### Description

This command is used to display BGP configuration and summary of the BGP status.

### Format

**show bgp {summary}**

### Parameters

| |
|---|
| **summary** - (Optional) Specifies that the summary of the BGP status will be included in the display. |

### Restrictions

None. (EI Mode Only Command)

### Example

This example displays the BGP setting:

```
DGS-3620-28SC:admin#  show bgp
Command:  show bgp

BGP Global State                   : Disabled
Version                            : 4
BGP Router Identifier              : 10.90.90.90
Synchronization                    : Enabled
Enforce First AS                   : Enabled
Local AS number                    : 100
Scan Time                          : 60
Hold Time                          : 300 Seconds
Keepalive Interval                 : 100 Seconds
Dampening                          : Enabled
Always Compare MED                 : Disabled
Deterministics MED                 : Disabled
Med Confed                         : Disabled
Default Local Preference           : 200
AS Path Ignore                     : Disabled
Compare Router ID                  : Enabled
MED Missing as Worst               : Disabled
Compare Confederation Path         : Disabled
Fast External Fallover             : Enabled
Aggregate Next Hop Check           : Disabled
BGP Trap                           : None

DGS-3620-28SC:admin#  show bgp summary
Command:  show bgp summary
BGP Router Identifier              : 172.16.1.1
```

```
local AS number                    : 100
Dampening                          : Enabled
BGP AS Path Entries                : 10
BGP Community Entries              : 7
Neighbor       Ver    AS     MsgRcvd  MsgSent  Up/Down     State/PfxRcvd
-----------    ---    --     -------  -------  -------     -------------
10.100.1.1     4      200    26       22       00:14:23    23
10.200.1.1     4      300    21       51       00:13:40    0
10.200.1.5     4      300    21       5        00:10:05    Idle

Total Number of Neighbors:3

DGS-3620-28SC:admin#
```

## 12-49 show bgp reflection

### Description

This command is used to display the route reflection configuration of BGP.

### Format

**show bgp reflection**

### Parameters

None.

### Restrictions

None. (EI Mode Only Command)

### Example

This example displays the BGP reflection setting:

```
DGS-3620-28SC:admin#  show bgp reflection
Command:  show bgp reflection

Client to Client Reflection State     : Disabled
Cluster ID                            : 0.0.0.0

Router Reflector Client:
  10.1.1.20
  10.1.1.30

DGS-3620-28SC:admin#
```

## 12-50 show bgp confederation

### Description

This command is used to display the confederation configuration of BGP.

### Format

**show bgp confederation**

### Parameters

None.

### Restrictions

None. (EI Mode Only Command)

### Example

This example displays the BGP confederation setting:

```
DGS-3620-28SC:admin#  show bgp confederation
Command: show bgp confederation

BGP as number               : 65501
Confederation identifier    : 10
Confederation Peer          : 65502,65503
Neighbor list:
 IP address             Remote AS number
 ---------------       --------------------
192.168.1.1               65502
192.168.1.2               65503
192.168.1.3               65501

DGS-3620-28SC:admin#
```

## 12-51 config bgp trap

### Description

This command is used to configure the BGP trap state.

### Format

**config bgp trap [peer_established | peer_idle | all] [enable | disable]**

### Parameters

**peer_established** - Enable or disable the sending of the peer established trap. This default value is disabled.

**peer_idle** - Enable or disable the sending of the peer idle trap. This default value is disabled.

**all** - Enable or disable the sending of both the peer idle and established trap. This default value is disabled.

**enable** - Specifies that the trap feature will be enabled.
**disable** - Specifies that the trap feature will be disabled.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

This example disables the BGP peer idle trap state:

```
DGS-3620-28SC:admin#  config bgp trap peer_idle disable
Command:  config bgp trap peer_idle disable

Success.

DGS-3620-28SC:admin#
```

## 12-52 show bgp trap_state

### Description

This command is used to show the BGP trap state.

### Format

**show bgp trap_state**

### Parameters

None.

### Restrictions

None. (EI Mode Only Command)

### Example

This example displays the BGP trap state:

```
DGS-3620-28SC:admin#  show bgp trap_state
Command:  show bgp trap_state

BGP Trap State          :
BGP Peer Established    : Enabled
BGP Peer Idle           : Enabled

DGS-3620-28SC:admin#
```

## 12-53 config bgp scan_timer

### Description

This command is used to configure the BGP scan timer value. BGP will check the next hop whether it is reachable from the BGP route before the timer expires.

### Format

**config bgp scan_timer [<sec 5-60> | default]**

### Parameters

**<sec 5-60>** - Set the BGP scan timer value from 5 to 60 seconds. Default is 60 seconds

**default** - Set the BGP scan timer to the default value.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

This example configures the BGP scan timer to 30 seconds:

```
DGS-3620-28SC:admin#  config bgp scan_timer 30
Command:  config bgp scan_timer 30

Success.

DGS-3620-28SC:admin#
```

## 12-54 config bgp aggregate_next_hop_check

### Description

This command is used to configure the BGP aggregated routes’ next hop check. Only the routes with the same next hop attribute can be aggregated if the BGP aggregate next hop check is enabled.

### Format

**config bgp aggregate_next_hop_check [enable | disable]**

### Parameters

**enable** - Specifies that the BGP aggregate next hop check will be enabled.

**disable** - Specifies that the BGP aggregate next hop check will be disabled.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

This is an example of configuring the BGP aggregate next hop check:

```
DGS-3620-28SC:admin# config bgp aggregate_next_hop_check enable
Command: config bgp aggregate_next_hop_check enable

Success.

DGS-3620-28SC:admin#
```

## 12-55 config bgp fast_external_fallover

### Description

This command configures a Border Gateway Protocol (BGP) routing process to immediately reset its external BGP peer sessions if the link used to reach these peers goes down,

### Format

**config bgp fast_external_fallover [enable | disable]**

### Parameters

**enable** - To enable BGP fast external fallover flag. Default is enabled.
**disable** - To disable BGP fast external fallover.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

This example disables BGP fast external fallver:

```
DGS-3620-28SC:admin#  config bgp fast_external_fallover disable
Command:  config bgp fast_external_fallover disable

Success.

DGS-3620-28SC:admin#
```

## 12-56 config bgp neighbor maximum_prefix

### Description

This command is used to configure the BGP neighbor maximum prefix.

### Format

**config bgp neighbor maximum_prefix [<ipaddr> | peer_group <peer_group_name 16>] <value 1-12000> {<value 1-100>} {warning_only}**

### Parameters

**<ipaddr>** - Specifies the IP address of the neighbor to be configured.

**peer_group** - Specifies the peer group to be configured.

**<peer_group_name 16>** - Enter the peer group name here. This name can be up to 16 characters long.

**<value 1-12000>** - Maximum number of prefixes allowed from the specified neighbor. The default is 12000.

**<value 1-100>** - (Optional) Integer specifying at what percentage the maximum prefix limit that the router starts to generate a warning message. The range is from 1 to 100; the default is 75.

**warning_only** - (Optional) Allows the router to generate a log message when the maximum prefix limit is exceeded, instead of terminating the peering session.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

This example sets the maximum number of prefixes that will be accepted from the neighbor 192.168.1.1 to 5000, when 50 percent of the maximum prefix limit has been reached. This will display a warning message:

```
DGS-3620-28SC:admin#  config bgp neighbor maximum_prefix 192.168.1.1 5000 50
Command:  config bgp neighbor maximum_prefix 192.168.1.1 5000 50

Success.

DGS-3620-28SC:admin#
```

## 12-57 clear bgp flap_statistics

### Description

The command is used to clear the accumulated penalties for routes that have been received on a router that has BGP dampening enabled. If no arguments or keywords are specified, flap statistics are cleared for all routes.

### Format

**clear bgp flap_statistics {[<ipaddr> | <network_address>]}**

### Parameters

**<ipaddr>** - (Optional) Specifies an IPv4 address to clear the dampening flap statistics.

**<network_address>** - (Optional) Specifies an IPv4 network to clear the dampening flap statistics.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

This is an example to clear the route dampening flap statistics of network 192.168.1.0/24:

```
DGS-3620-28SC:admin#  clear bgp flap_statistics 192.168.1.0/24
Command: clear bgp flap_statistics 192.168.1.0/24

Success.

DGS-3620-28SC:admin#
```

# Chapter 13 BPDU Attack Protection Commands

| |
|---|
| **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>}} |

## 13-1 config bpdu_protection ports

### Description

This command is used to configure port state and mode for BPDU protection.

### Format

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

### Parameters

| |
|---|
| **<portlist>** - Specify a range of ports to be configured. |
| **all** - Specify to set all ports in the system. |
| **state** - Specify the BPDU protection state. The default state is disabled.<br>**enable** - Enable the BPDU protection state.<br>**disable** - Disable the BPDU protection state. |
| **mode** - Specify the BPDU protection mode. The default mode is shutdown.<br>**drop** - Specify to drop all received BPDU packets when the port enters the under attack state.<br>**block** - Specify to drop all packets (include BPDU and normal packets) when the port enters the under attack state.<br>**shutdown**- Specify to shut down the port when the port enters the under attack state. |

**Note:** Only shutdown mode will make port link down, If the port status is Err-disabled but port link is up, please check “show ports err-disabled” command for the reason.

### Restrictions

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

### Example

To configure port state to enable and drop mode:

```
DGS-3620-28SC:admin#config bpdu_protection ports 1 state enable mode drop
Command: config bpdu_protection ports 1 state enable mode drop

Success.
DGS-3620-28SC:admin#
```

## 13-2 config bpdu_protection recovery_timer

### Description

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. This command is used to configure the auto-recovery timer. 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>** - Specify the timer (in seconds) used by the Auto-recovery mechanism to recover the port. The valid range is 60 to 1000000. Auto-recovery time is 60 seconds by default.

**infinite** - Specify the port will not be auto recovered.

### Restrictions

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

### Example

To configure the BPDU protection recovery timer to 120 seconds for the entire switch:

```
DGS-3620-28SC:admin#config bpdu_protection recovery_timer 120
Command: config bpdu_protection recovery_timer 120

Success.

DGS-3620-28SC:admin#
```

## 13-3 config bpdu_protection

### Description

This command is used to configure the BPDU protection trap state or log state.

### Format

**config bpdu_protection [trap | log] [none | attack_detected | attack_cleared | both]**

### Parameters

**trap** - Specify the trap state.

**log** - Specify the log state.

**none** - Specify neither attack_detected nor attack_cleared is trapped or logged.

**attack_detected** - Specify events will be logged or trapped when the BPDU attacks is detected.

**attack_cleared** - Specify events will be logged or trapped when the BPDU attacks is cleared.

**both** - Specify the events of attack_detected and attack_cleared shall be trapped or logged.

### Restrictions

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

### Example

To configure the BPDU protection trap state as both for the entire switch:

```
DGS-3620-28SC:admin#config bpdu_protection trap both
Command: config bpdu_protection trap both

Success.

DGS-3620-28SC:admin#
```

## 13-4 enable bpdu_protection

### Description

This command is used to enable BPDU protection globally for the entire switch.

### Format

**enable bpdu_protection**

### Parameters

None.

### Restrictions

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

### Example

To enable BPDU protection for the entire switch:

```
DGS-3620-28SC:admin#enable bpdu_protection
Command: enable bpdu_protection

Success.

DGS-3620-28SC:admin#
```

## 13-5 disable bpdu_protection

### Description

This command is used to disable BPDU protection globally for the entire switch.

### Format

**disable bpdu_protection**

### Parameters

None.

### Restrictions

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

### Example

To disable BPDU protection:

```
DGS-3620-28SC:admin#disable bpdu_protection
Command: disable bpdu_protection

Success.

DGS-3620-28SC:admin#
```

## 13-6 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 all ports to be displayed.

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

### Restrictions

None.

### Example

To display BPDU protection information for the entire switch:

```
DGS-3620-28SC:admin#show bpdu_protection
Command: show bpdu_protection

BPDU Protection Global Settings
---------------------------------------
BPDU Protection Status        : Disabled
BPDU Protection Recover Time  : 60 seconds
BPDU Protection Trap State    : None
BPDU Protection Log State     : Both

DGS-3620-28SC:admin#
```

To display BPDU protection status for ports 1 to 3:

```
DGS-3620-28SC:admin#show bpdu_protection ports 1-3
Command: show bpdu_protection ports 1-3

Port  State        Mode       Status
----- -----------  ---------- -----------
1    Disabled     Shutdown   Normal
2    Disabled     Shutdown   Normal
3    Disabled     Shutdown   Normal

DGS-3620-28SC:admin#
```

# Chapter 14 Cable Diagnostics Commands

**cable_diag ports** [<portlist> | all]

## 14-1 cable_diag ports

### Description

This command is used to test copper cabling.

For 10/100Based-TX link speed RJ45 cables, two pairs of cables will be diagnosed.

For 1000Base-T link speed RJ45 cables, four pairs of cables will be diagnosed.

The type of cable errors can be open, short, or crosstalk.

- **Open** means that the cable in the error pair does not have a connection at the specified position.
- **Short** means that the cables in the error pair has a short problem at the specified position.
- **Crosstalk** means that the cable in the error pair has a crosstalk problem at the specified position.

**For Fast 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 can 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**, 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.

**For 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 can 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**, 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.

The Cable length range that can be detected is as follows:

- Smaller than 50m (<50m)
- Between 50m and 80m (50m~80m)
- Between 80m and 100m (80m~100m)
- Greater than 100m (>100m)

**Note:** This test will consume a low number of packets. Since this test is for copper cable, the port with fiber cable will be skipped from the test.

## Format

**cable_diag ports [<portlist> | all]**

## Parameters

| |
|---|
| **<portlist>** - Specify a range of ports to be configured. |
| **all** – Specify to set all ports in the system. |

## Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

## Example

To test the cable on ports 1 to 4, and 8:

```
DGS-3620-28SC:admin# cable_diag ports 1:1-1:10,1:21
Command: cable_diag ports 1:1-1:10,1:21
Perform Cable Diagnostics ...

Port      Type       Link Status    Test Result                  Cable Length
(M)
------  ----------  -------------  ----------------------------  ------------
1:1     1000BASE-T  Link Up        OK                             65
1:2     1000BASE-T  Link Up        OK                              -
1:3     1000BASE-T  Link Down      Shutdown                       25
1:4     1000BASE-T  Link Down      Shutdown                        -
1:5     1000BASE-T  Link Down      Unknown                         -
1:6     1000BASE-T  Link Down      Pair 1 Crosstalk at  30M        -
                                   Pair 2 Crosstalk at  30M
                                   Pair 3 OK        at 110M
                                   Pair 4 OK        at 110M
1:7     1000BASE-T  Link Down      NO Cable                        -
1:8     1000BASE-T  Link Down      Pair 1 Open      at  16M        -
                                   Pair 2 Open      at  16M
                                   Pair 3 OK        at  50M
                                   Pair 4 OK        at  50M
1:9     1000BASE-T  Link Down      Pair 1 Short     at   5M        -
                                   Pair 2 Short     at   5M
                                   Pair 3 OK        at 110M
                                   Pair 4 OK        at 110M
1:10    1000BASE-T  Link Down      Pair 1 Unknown                  -
                                   Pair 2 Short     at   5M
                                   Pair 3 OK        at 110M
                                   Pair 4 OK        at 110M
1:21    1000BASE-X  Link Up        Unknown                         -

DGS-3620-28SC:admin#
```

# Chapter 15 CFM Commands

```
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 [3.3ms | 10ms | 100ms | 1sec |
        10sec | 1min | 10min] | mepid_list [add | delete] <mepid_list 1-8191> | mode [software |
        hardware]}(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 {[md [<string 22> | md_index <uint 1-4294967295>] {ma [<string 22> | ma_index <uint
        1-4294967295>] {mepid <int 1-8191>}} | mepname <string 32>]}
show cfm fault {md [<string 22> | md_index <uint 1-4294967295>] {ma [<string 22> | ma_index
        <uint 1-4294967295>]}}
show cfm port <port> {level <int 0-7> | direction [inward | outward] | vlanid <vlanid 1-4094>}
cfm 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>}
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>]}
config cfm mp_ltr_all [enable | disable]
show cfm mipccm
show cfm mp_ltr_all
show cfm pkt_cnt {[ports <portlist> {[rx | tx]} | [rx | tx] | ccm]}
clear cfm pkt_cnt {[ports <portlist> {[rx | tx]} | [rx | tx] | ccm]}
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>
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]}

**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]}

## 15-1 create cfm md

### Description

This command is used to create a CFM 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 used here. This name can be up to 22 characters long.

**md_index** - Specifies the maintenance domain index used.
**<uint 1-4294967295>** - Enter the maintenace domain index value used here. This value must be between 1 and 4294967295.

**level** - Specify the maintenance domain level.
**<int 0-7>** - Specify the maintenance domain level from 0 to 7.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

To create a CFM maintenance domain called “op_domain” and assign a maintenance domain level of “2”:

```
DGS-3620-28SC:admin#create cfm md op_domain level 2
Command: create cfm md op_domain level 2

Success.

DGS-3620-28SC:admin#
```

## 15-2 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 used here. This name can be up to 22 characters long.

**md_index** - Specifies the maintenance domain index used.
- **<uint 1-4294967295>** - Enter the maintenace domain index value used here. This value must be between 1 and 4294967295.

**mip** - (Optional) This is the control creations of MIPs.
- **none** - Do not create MIPs. This is the default value.
- **auto** - MIPs can always be created on any port in this MD if the port is not configured with an MEP of this MD.
- **explicit** - MIPs can only be created on any port in this MD if the next existing lower level has an MEP configured on that port, and that port is not configured with an MEP of this MD.

**sender_id** - (Optional) This is the control transmission of the sender ID TLV.
- **none** - Do not transmit the sender ID TLV. This is the default value.
- **chassis** - Transmit the sender ID TLV with the chassis ID information.
- **manage** - Transmit the sender ID TLV with the managed address information.
- **chassis_manage** - Transmit the sender ID TLV with chassis ID information and manage address information.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

To configure the maintenance domain called “op_domain” and specify the explicit option for creating MIPs:

```
DGS-3620-28SC:admin#config cfm md op_domain mip explicit
Command: config cfm md op_domain mip explicit

Success.

DGS-3620-28SC:admin#
```

## 15-3 create cfm ma

### Description

This command is used to create a maintenance association. Different MAs in a 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 used here. This name can be up to 22 characters long.

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

**md** - Specify the maintenance domain name.
**<string 22>** - Specify the maintenance domain name. The maximum length is 22 characters.

**md_index** - Specifies the maintenance domain index used.
**<uint 1-4294967295>** - Enter the maintenance domain index value used here. This value must be between 1 and 4294967295.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

To create a maintenance association called “op1” and assign it to the maintenance domain “op_domain”:

```
DGS-3620-28SC:admin#create cfm ma op1 md op_domain
Command: create cfm ma op1 md op_domain

Success.

DGS-3620-28SC:admin#
```

## 15-4 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 [3.3ms | 10ms | 100ms | 1sec | 10sec | 1min | 10min] | mepid_list [add | delete] <mepid_list 1-8191> | mode [software | hardware]}(1)**

### Parameters

**<string 22>** - Specify the maintenance association name. The maximum length is 22 characters.

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

**md** - Specify the maintenance domain name.
**<string 22>** - Specify the maintenance domain name. The maximum length is 22 characters.
**md_index** - Specifies the maintenance domain index used.
**<uint 1-4294967295>** - Enter the maintenance domain index value used here. This value must be between 1 and 4294967295.

**vlanid** - (Optional) Specify the VLAN Identifier. Different MAs must be associated with different VLANs.
**<vlanid 1-4094>** - Specify the VLAN ID between 1 and 4094.

**mip** - (Optional) This is the control creation of MIPs.
**none** - Do not create MIPs.
**auto** - MIPs can always be created on any port in this MA if that port is not configured with an MEP of that MA.
**explicit** - MIPs can be created on any ports in this MA only if the next existing lower level has an MEP configured on that port, and that port is not configured with an MEP of this MA.
**defer** - Inherit the setting configured for the maintenance domain that this MA is associated with. This is the default value.

**sender_id** - (Optional) This is the control transmission of the sender ID TLV.
**none** - Do not transmit the sender ID TLV. This is the default value.
**chassis** - Transmit the sender ID TLV with the chassis ID information.
**manage** - Transmit the sender ID TLV with the manage address information.
**chassis**_manage - Transmit the sender ID TLV with the chassis ID information and the manage address information.
**defer** - Inherit the setting configured for the maintenance domain that this MA is associated with. This is the default value.

**ccm_interval** - (Optional) Specify the CCM interval.
**3.3ms** - 3.3 milliseconds. Only work in CFM hardware mode.
**10ms** - 10 milliseconds. Only works in CFM hardware mode.
**100ms** - 100 milliseconds. Not recommended in CFM software mode.
**1sec** - One second.
**10sec** - Ten seconds. This is the default value.
**1min** - One minute.
**10min** - Ten minutes.

**mepid_list** - (Optional) Specify the MEPIDs contained in the maintenance association.
**add** - Add MEPID(s).
**delete** - Delete MEPID(s).
**<mepid_list 1-8191>** - Specify the MEPIDs contained in the maintenance association. The range of the MEPID is 1 to 8191.

**mode** - (Optional) Specifies the mode of the MA.
**software** - Specifies that the MA will work in the CFM software mode. This is the default value.
**hardware** - Specifies that the MA will work in the CFM hardware mode.

## Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

## Example

To configure the parameters of a maintenance association:

```
DGS-3620-28SC: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-3620-28SC:admin#
```

## 15-5 create cfm mep

### Description

This command is used to create an MEP entry. Different MEPs in the same MA must have a different MEPID. To put MD name, MA name, and MEPID together identifies an MEP. Different MEPs on the same device must have a different MEP name. Before creating an MEP, its MEPID should be configured in the MA's MEPID list.

### Format

**create cfm mep <string 32> mepid <int 1-8191> md [<string 22> | md_index <uint 1-4294967295>] ma [<string 22> | ma_index <uint 1-4294967295>] direction [inward | outward] port <port>**

### Parameters

**<string 32>** - Enter the MEP name used here. It is unique among all MEPs configured on the device. The name can be up to 32 characters long.

**mepid** - Specify the MEP MEPID. It should be configured in the MA's MEPID list.
**<int 1-8191>** - Specify the MEP MEPID between 1 and 8191.

**md** - Specify the maintenance domain name.
**<string 22>** - Specify 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>** - Specify 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.

**direction** - Specify the MEP direction.
**inward** - Inward facing (up) MEP.
**outward** - Outward facing (down) MEP.

**port** - Specify the port number. This port should be a member of the MA's associated VLAN.
**<port>** - Specify a port.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

To create an MEP:

```
DGS-3620-28SC: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-3620-28SC:admin#
```

## 15-6 config cfm mep

### Description

This command is used to configure the parameters of an MEP. An MEP may generate five types of Fault Alarms, as shown below by their priorities from high to low:

1. Cross-connect CCM Received: priority 5
2. Error CCM Received: priority 4
3. Some Remote MEPs Down: priority 3
4. Some Remote MEP MAC Status Errors: priority 2
5. 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>** - Specify the MEP name. The maximum length is 32 characters.

**mepid** - Specify the MEP MEPID.
**<int 1-8191>** - Specify the MEP MEPID between 1 and 8191.

**md** - Specify the maintenance domain name.
**<string 22>** - Specify 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>** - Specify 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.

**state** - Specify the MEP administrative state. The default is disable.
**enable** - Enable MEP.
**disable** - Disable MEP.

**ccm** - Specify the CCM transmission state. The default is disable.
**enable** - Enable the CCM transmission.
**disable** - Disable the CCM transmission.

**pdu_priority** - The 802.1p priority is set in the CCM and the LTM messages transmitted by the MEP. The default value is 7.
**<int 0-7>** - Specify the value between 0 and 7.

**fault_alarm** - This is the control types of the fault alarms sent by the MEP. The default value is none.
**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.

**alarm_time** - Specify the time that a defect must exceed before the fault alarm can be sent. The unit is centiseconds. The default value is 250.
**<centisecond 250-1000>** - Specify the time that a defect must exceed before the fault alarm can be sent. The unit is centiseconds. The range is 250 to 1000.

**alarm_reset_time** - Specify the dormant duration time before a defect is triggered before the fault can be re-alarmed. The unit is centiseconds. The default value is 1000.
**<centisecond 250-1000>** - Specify the dormant duration time before a defect is triggered before the fault can be re-alarmed. The unit is centiseconds. The range is 250 to 1000.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

To configure the parameters of an MEP:

```
DGS-3620-28SC:admin#config cfm mep mepname mep1 state enable ccm enable
Command: config cfm mep mepname mep1 state enable ccm enable

Success.

DGS-3620-28SC:admin#
```

## 15-7 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>** - Specify the MEP name. The maximum length is 32 characters.

**mepid** - Specify the MEP MEPID.
**<int 1-8191>** - Specify the MEP MEPID between 1 and 8191.
**md** - Specify the maintenance domain name.
**<string 22>** - Specify 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>** - Specify the maintenance association name. The maximum length is 22 characters.

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

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

To delete a previously created MEP:

```
DGS-3620-28SC:admin#delete cfm mep mepname mep1
Command: delete cfm mep mepname mep1

Success.

DGS-3620-28SC:admin#
```

## 15-8 delete cfm ma

### Description

This command is used to delete a created maintenance association.

### Format

**delete cfm ma [<string 22> | ma_index <uint 1-4294967295>] md [<string 22> | md_index <uint 1-4294967295>]**

### Parameters

| |
|---|
| **<string 22>** - Specify the maintenance association name. The maximum length is 22 characters.<br>**ma_index** - Specify the maintenance association index.<br>**<uint 1-4294967295>** - Enter the maintenance association index value here. This value must be between 1 and 4294967295. |
| **md** - Specify the maintenance domain name.<br>**<string 22>** - Specify the maintenance domain name. The maximum length is 22 characters.<br>**md_index** - Specify the maintenance domain index.<br>**<uint 1-4294967295>** - Enter the maintenance domain index value here. This value must be between 1 and 4294967295. |

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

To delete a created maintenance association:

```
DGS-3620-28SC:admin#delete cfm ma op1 md op_domain
Command: delete cfm ma op1 md op_domain
```

```
Success.

DGS-3620-28SC:admin#
```

## 15-9 delete cfm md

### Description

This command is used to delete a previously created maintenance domain. When the command is executing, 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>** - Specify 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.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

To delete a previously created maintenance domain:

```
DGS-3620-28SC:admin#delete cfm md op_domain
Command: delete cfm md op_domain

Success.

DGS-3620-28SC:admin#
```

## 15-10 enable cfm

### Description

This command is used to enable the CFM globally.

### Format

**enable cfm**

### Parameters

None.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

To enable the CFM globally:

```
DGS-3620-28SC:admin#enable cfm
Command: enable cfm

Success.

DGS-3620-28SC:admin#
```

## 15-11 disable cfm

### Description

This command is used to disable the CFM globally.

### Format

**disable cfm**

### Parameters

None.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

To disable the CFM globally:

```
DGS-3620-28SC:admin#disable cfm
Command: disable cfm

Success.

DGS-3620-28SC:admin#
```

## 15-12 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:

- MIPs are never created on that port.
- MEPs can still be created on that port, and the configuration can be saved.
- 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>** - Specify the logical port list.

**state** - Specify the CFM function status.
**enable** - Specify to enable the CFM function.
**disable** - Specify to disable  the CFM function.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

To enable the CFM function on ports 2 to 5:

```
DGS-3620-28SC:admin#config cfm ports 2-5 state enable
Command: config cfm ports 2-5 state enable

Success.

DGS-3620-28SC:admin#
```

## 15-13 show cfm ports

### Description

This command is used to display the CFM state of specified ports.

### Format

**show cfm ports <portlist>**

### Parameters

**<portlist>** - Specify the logical port list.

### Restrictions

None. (EI Mode Only Command)

### Example

To display the CFM state for ports 3 to 6:

```
DGS-3620-28SC:admin#show cfm ports 3-6
Command: show cfm ports 3-6

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

DGS-3620-28SC:admin#
```

## 15-14 show cfm

### Description

This command is used to display 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>** - Specify 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** - (Optional) Specify the maintenance association name.
- **<string 22>** - Specify 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** - (Optional) Specify the MEPID.
- **<int 1-8191>** - Specify the MEP MEPID between 1 and 8191.

**mepname** - (Optional) Specify the MEP name.
- **<string 32>** - Specify the MEP name. The maximum length is 32 characters.

### Restrictions

None. (EI Mode Only Command)

### Example

To display the CFM configuration:

```
DGS-3620-28SC:admin#show cfm
Command: show cfm

CFM State: Enabled

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

DGS-3620-28SC:admin#
```

## 15-15 show cfm fault

### Description

This command is used to display all the fault conditions detected by the MEPs contained in the specified MA or MD. The 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>** - Specify 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** - (Optional) Specify the maintenance association name.
  **<string 22>** - Specify 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.

### Restrictions

None. (EI Mode Only Command)

### Example

To display the MEPs that have faults:

```
DGS-3620-28SC: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     Normal       Normal

DGS-3620-28SC:admin#
```

## 15-16 show cfm port

### Description

This command is used to display 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>** - Specify the port number.

**level** - (Optional) Specify the maintenance domain level. If not specified, all levels are shown.
  **<int 0-7>** - Specify the value between 0 and 7.

**direction** - (Optional) Specify the MEP direction.
  **inward** - Specify inward  facing MEP.
  **outward** - Specify outward facing MEP.

**vlanid** - (Optional) Specify the VLAN identifier. If not specified, all VLANs are displayed.
  **<vlanid 1-4094>** - Specify the VLAN ID between 1 and 4094.

### Restrictions

None. (EI Mode Only Command)

### Example

To display a CFM port:

```
DGS-3620-28SC:admin#show cfm port 1
Command: show cfm port 1

MAC Address: 00-05-78-82-32-01

MD Name     MA Name    MEPID  Level    Direction  VID
----------- ---------- ------- ------- --------- ---
op_domain    op1        1      2       inward    2
cust_domain  cust1      8      4       inward    2
serv_domain  serv2      MIP    3                 2

DGS-3620-28SC:admin#
```

## 15-17 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

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

**ma** - Specifies the maintenance association name.
 **<string 22>** - Enter the maintenance association name here. This name can be up to 22 characters long.
 **ma_index** – Specifies the MA index value used.
  **<uint 1-4294967295>** - Enter the MA index value used here. This value must be between 1 and 4294967295.

**mepid** - The MEP ID in the MD which sends 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** - Specifies to start or to stop the management lock function.
 **start** - Specifies to start the management lock function.
 **stop** - Specifies to stop the management lock function.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

To start management lock:

```
DGS-3620-28SC: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-3620-28SC:admin#
```

## 15-18 cfm loopback

### Description

This command is used to start a CFM loopback test. Press Ctrl+C to exit the loopback test. The MAC address represents the destination MEP or MIP that can be reached by this MAC address. The MEP represents the source MEP to initiate the loopback message.

## Format

**cfm loopback <macaddr> [mepname <string 32> | mepid <int 1-8191> md [<string 22> | md_index <uint 1-4294967295>] ma [<string 22> | ma_index <uint 1-4294967295>]] {num <int 1-65535> | [length <int 0-1500> | pattern <string 1500>] | pdu_priority <int 0-7>}**

## Parameters

**<macaddr>** - Specify the destination MAC address.

**mepname** - Specify the MEP name.
    **<string 32>** - Specify the MEP name. The maximum length is 32 characters.

**mepid** - (Optional) Specify the MEPID.
    **<int 1-8191>** - Specify the MEP MEPID between 1 and 8191.
    **md** - (Optional) Specify the maintenance domain name.
        **<string 22>** - Specify the maintenance domain name. The maximum length is 22 characters.
    **md_index** – Specifies the MD index value used.
        **<uint 1-4294967295>** - Enter the MD index value used here. This value must be between 1 and 4294967295.
    **ma** - (Optional) Specify the maintenance association name.
        **<string 22>** - Specify the maintenance association name. The maximum length is 22 characters.
    **ma_index** – Specifies the MA index value used.
        **<uint 1-4294967295>** - Enter the MA index value used here. This value must be between 1 and 4294967295.

**num** - (Optional) Specify the number of LBMs to be sent. The default value is 4.
    **<int 1-65535>** - Specify the value between 1 and 65535.

**length** - (Optional) Specify the payload length of the LBM to be sent. The default is 0.
    **<int 0-1500>** - Specify the value between 0 and 1500.

**pattern** - (Optional) Specify an 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 value used here. This value can be up to 1500 characters long.

**pdu_priority** - (Optional) Specify 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>** - Specify the value between 0 and 7.

## Restrictions

None. (EI Mode Only Command)

## Example

To start a CFM loopback test:

```
DGS-3620-28SC:admin#cfm loopback 00-01-02-03-04-05 mepname mep1
Command: cfm loopback 00-01-02-03-04-05 mepname mep1

Request timed out.
Request timed out.
Reply from MPID 52: bytes=xxx time=xxxms
Request timed out.

CFM loopback statistics for 00-01-02-03-04-05:
   Packets: Sent=4, Received=1, Lost=3(75% loss)
```

```
DGS-3620-28SC:admin#
```

## 15-19 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>** - Specify the destination MAC address.

**mepname** - Specify the MEP name.
**<string 32>** - Specify the MEP name. The maximum length is 32 characters.

**mepid** - (Optional) Specify the MEPID.
**<int 1-8191>** - Specify the MEP MEPID between 1 and 8191.
**md** - (Optional) Specify the maintenance domain name.
**<string 22>** - Specify the maintenance domain name. The maximum length is 22 characters.
**md_index** – Specifies the MD index value used.
**<uint 1-4294967295>** - Enter the MD index value used here. This value must be between 1 and 4294967295.
**ma** - (Optional) Specify the maintenance association name.
**<string 22>** - Specify the maintenance association name. The maximum length is 22 characters.
**ma_index** – Specifies the MA index value used.
**<uint 1-4294967295>** - Enter the MA index value used here. This value must be between 1 and 4294967295.

**ttl** - (Optional) Specify the link trace message TTL value. The default value is 64.
**<int 2-255>** - Specify the link trace message TTL value. Enter a value between 2 and 255.

**pdu_priority** - (Optional) Specify 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>** - Specify 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. Enter a value between 0 and 7.

### Restrictions

None. (EI Mode Only Command)

### Example

To transmit a LTM:

```
DGS-3620-28SC: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-3620-28SC:admin#
```

## 15-20 show cfm linktrace

### Description

This command is used to display the link trace responses. The maximum linktrace 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.<br>**<string 32>** - Specify the MEP name. The maximum length is 32 characters. |
| **mepid** - (Optional) Specify the MEPID.<br>**<int 1-8191>** - Specify the MEP MEPID between 1 and 8191.<br>**md** - (Optional) Specify the maintenance domain name.<br>**<string 22>** - Specify the maintenance domain name. The maximum length is 22 characters.<br>**md_index** - Specify the maintenance domain index.<br>**<uint 1-4294967295>** - Enter the maintenance domain index value here. This value must be between 1 and 4294967295.<br>**ma** - (Optional) Specify the maintenance association name.<br>**<string 22>** - Specify the maintenance association name. The maximum length is 22 characters.<br>**ma_index** - Specify the maintenance association index.<br>**<uint 1-4294967295>** - Enter the maintenance association index value here. This value must be between 1 and 4294967295. |
| **trans_id** - (Optional) The identifier of the transaction to be displayed.<br>**<uint>** - The identifier of the transaction to be displayed. |

### Restrictions

None. (EI Mode Only Command)

### Example

To display a CFM linktrace reply:

```
DGS-3620-28SC:admin#show cfm linktrace mepname mep1
Command: show cfm linktrace mepname mep1

Trans ID  Source MEP    Destination
-------- ------------- -----------------
26       mep1          XX-XX-XX-XX-XX-XX

DGS-3620-28SC:admin#
```

To display a CFM linktrace reply:

```
DGS-3620-28SC:admin# show cfm linktrace mepname mep trans_id 0
```

```
Command: show cfm linktrace mepname mep trans_id 0

Transaction ID: 0
From MEP mep to 00-15-72-20-91-09
Start Time    : 2010-12-31 00:51:49

Hop  MEPID  Ingress MAC Address  Egress MAC Address   Forwarded  Relay Action
---  -----  -------------------  -------------------  ---------  ------------
1    -      00-00-00-00-00-00    00-01-02-00-01-14    Yes        FDB
2    2      00-15-72-20-91-14    00-15-72-20-91-09    No         Hit

DGS-3620-28SC:admin#
```

## 15-21 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.<br>**<string 22>** - Specify the maintenance domain name. The maximum length is 22 characters.<br>**md_index** – Specifies the MD index value used.<br>**<uint 1-4294967295>** - Enter the MD index value used here. This value must be between 1 and 4294967295.<br>**ma** - (Optional) Specify the maintenance association name.<br>**<string 22>** - Specify the maintenance association name. The maximum length is 22 characters.<br>**ma_index** – Specifies the MA index value used.<br>**<uint 1-4294967295>** - Enter the MA index value used here. This value must be between 1 and 4294967295.<br>**mepid** - (Optional) Specify the MEPID.<br>**<int 1-8191>** - Specify the MEP MEPID between 1 and 8191. |
| **mepname** - (Optional) Specify the MEP name.<br>**<string 32>** - Specify the MEP name. The maximum length is 32 characters. |

### Restrictions

None. (EI Mode Only Command)

### Example

To delete the CFM link trace reply:

```
DGS-3620-28SC:admin#delete cfm linktrace mepname mep1
Command: delete cfm linktrace mepname mep1

```

```
Success.

DGS-3620-28SC:admin#
```

## 15-22 config cfm mp_ltr_all

### Description

This command is to enable or disable the "all MPs reply LTRs" function. This function is for test purposes. According to IEEE 802.1ag, a Bridge replies with one LTR to an LTM. This command can make all MPs on the LTM’s forwarding path reply with LTRs, no matter whether they are on a Bridge or not.

### Format

**config cfm mp_ltr_all [enable | disable]**

### Parameters

**enable** - Enable this feature.

**disable** - Disable this feature.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

To enable the all-MPs-reply-to-LTR function:

```
DGS-3620-28SC:admin#config cfm mp_ltr_all enable
Command: config cfm mp_ltr_all enable

Success.

DGS-3620-28SC:admin#
```

## 15-23 show cfm mipccm

### Description

This command is used to display the MIP CCM database entries. All entries in the MIP CCM database will be displayed. An MIP CCM entry is similar to an FDB which keeps the forwarding port information of a MAC entry.

### Format

**show cfm mipccm**

### Parameters

None. (EI Mode Only Command)

### Restrictions

None.

### Example

To display the MIP CCM database entries:

```
DGS-3620-28SC:admin#show cfm mipccm
Command: show cfm mipccm

MA                      VID   MAC Address          Port
------------------------ ----  -------------------- -------
opma                     1    XX-XX-XX-XX-XX-XX-XX  2
opma                     1    XX-XX-XX-XX-XX-XX-XX  3

Total:  2

DGS-3620-28SC:admin#
```

## 15-24 show cfm mp_ltr_all

### Description

This command is used to display the current configuration of the "all MPs reply LTRs" function. This command is for test purposes.

### Format

**show cfm mp_ltr_all**

### Parameters

None.

### Restrictions

None. (EI Mode Only Command)

### Example

To display the configuration of the all-MPs-reply-to-LTR function:

```
DGS-3620-28SC:admin#show cfm mp_ltr_all
Command: show cfm mp_ltr_all

All MPs reply LTRs: Disabled

```

```
DGS-3620-28SC:admin#
```

## 15-25 show cfm pkt_cnt

### Description

This command is used to display 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 display. If not specified, all ports will be displayed.
**<portlist>** - Specify a list of ports.
**rx** - (Optional) Display the RX counter. If not specified, both the RX and TX counters will be displayed.
**tx** - (Optional) Display the TX counter. If not specified, both the RX and TX counters will be displayed.

**rx** - (Optional) Display the RX counter. If not specified, both the RX and TX counters will be displayed.

**tx** - (Optional) Display the TX counter. If not specified, both the RX and TX counters will be displayed.

**ccm** - (Optional) Display the CCM RX counters.

### Restrictions

None. (EI Mode Only Command)

### Example

To display CFM packet RX/TX counters for ports 1 to 2:

```
DGS-3620-28SC:admin#show cfm pkt_cnt ports 1-2
Command: show cfm pkt_cnt ports 1-2

CFM RX Statistics
-------------------------------------------------------------------------------
Port  AllPkt   CCM      LBR      LBM       LTR    LTM     VidDrop  OpcoDrop
----- -------- -------- -------- --------- ------ ------- -------- --------
all   0        0        0       0          0      0       0       0
1     0        0        0       0          0      0       0       0
2     0        0        0       0          0      0       0       0

CFM TX Statistics
-----------------------------------------------------------
Port  AllPkt   CCM      LBR      LBM       LTR    LTM
----- -------- -------- -------- --------- ------ -------
all   0        0        0       0          0      0
1     0        0        0       0          0      0
2     0        0        0       0          0      0

```

```
DGS-3620-28SC:admin#
```

## 15-26 clear cfm pkt_cnt

### Description

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

### Format

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

### Parameters

**ports** - (Optional) Specify the port counters to clear. If not specified, all ports will be cleared.
  **<portlist>** - Specify a list of ports.
  **rx** - (Optional) Clear the RX counter. If not specified, both the RX and TX counters will be cleared.
  **tx** - (Optional) Clear the TX counter. If not specified, both the RX and TX counters will be cleared.

**rx** - (Optional) Clear the RX counter. If not specified, both the RX and TX counters will be cleared.

**tx** - (Optional) Clear the TX counter. If not specified, both the RX and TX counters will be cleared.

**ccm** - (Optional) Clear The CCM RX counters.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

To clear all the CFM packet RX/TX counters:

```
DGS-3620-28SC:admin#clear cfm pkt_cnt
Command: clear cfm pkt_cnt

Success.

DGS-3620-28SC:admin#
```

To clear the CFM packet CCM counters:

```
DGS-3620-28SC:admin#clear cfm pkt_cnt ccm
Command: clear cfm pkt_cnt ccm

Success.

DGS-3620-28SC:admin#
```

## 15-27 show cfm remote_mep

### Description

This command is used to display CFM remote MEP information.

### 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.
**<string 32>** - Specify the MEP name. The maximum length is 32 characters.

**md** - Specify the maintenance domain name.
**<string 22>** - Specify 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>** - Specify 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>** - Specify the MEP MEPID between 1 and 8191.

**remote_mepid** - Specify the remote MEPID.
**<int 1-8191>** - Specify the remote MEPID between 1 and 8191.

### Restrictions

None. (EI Mode Only Command)

### Example

To display CFM remote MEP information:

```
DGS-3620-28SC: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
Interface Name          : Down
Last CCM Serial Number  : 1000
Send Chassis ID         : 00-11-22-33-44-00
Sender Management Address: SNMP-UDP-IPv4 10.90.90.90:161
Detect Time             : 2008-01-01
```

```
DGS-3620-28SC:admin#
```

## 15-28 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]}**

### Parameters

**md** - Specify the maintenance domain name.
**<string 22>** - Specify 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>** - Specify 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>** - Specify the MEP MEPID between 1 and 8191.

**period** - (Optional) Specifies the transmitting interval of the AIS PDU.
**1sec** - Specifies that the transmitting interval period will be set to 1 second.
**1min** - Specifies that the transmitting interval period will be set to 1 minute.

**level** - (Optional) Specifies the client level ID to which the MEP sends AIS PDU. The default client MD level is the MD level that the most immediate client layer MIPs and MEPs exist on.
**<int 0-7>** - Enter the client level ID used here. This value must be between 0 and 7.

**state** - (Optional) Specifies the AIS function state used.
**enable** - Specifies that AIS function state will be enabled.
**disable** - Specifies that AIS function state will be disabled.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

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

```
DGS-3620-28SC: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-3620-28SC:admin#
```

## 15-29 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]}**

### Parameters

**md** - Specify the maintenance domain name.
**<string 22>** - Specify 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>** - Specify 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>** - Specify the MEP MEPID between 1 and 8191.

**period** - (Optional) Specifies the transmitting interval of the LCK PDU.
**1sec** - Specifies that the transmitting interval period will be set to 1 second.
**1min** - Specifies that the transmitting interval period will be set to 1 minute.

**level** - (Optional) Specifies the client level ID to which the MEP sends LCK PDU. The default client MD level is the MD level that the most immediate client layer MIPs and MEPs exist on.
**<int 0-7>** - Enter the client level ID used here. This value must be between 0 and 7.

**state** - (Optional) Specifies the LCK function state used.
**enable** - Specifies that LCK function state will be enabled.
**disable** - Specifies that LCK function state will be disabled.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

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

```
DGS-3620-28SC: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-3620-28SC:admin#
```

# Chapter 16 Command List History Commands

**?** {<Command>}
**show command_history**
**config command_history** <value 1-40>

## 16-1 ?

### Description

This command is used to display all of the commands available, on the current login account level, through the Command Line Interface (CLI).

### Format

**? {<Command>}**

### Parameters

**<Command>** – (Optional) Specify a command.

**Note:** If no command is specified, the system will display all commands of the corresponding user level.

### Restrictions

None.

### Example

To display all commands:

```
DGS-3620-28SC:admin#?
Command: ?

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

To display the syntax for "config account":

```
DGS-3620-28SC:admin#? config account
Command: ? config account

Command: config account
Usage:  <username> {encrypt [plain_text| sha_1] <password>}
Description: Used to configure user accounts.

DGS-3620-28SC:admin#
```

## 16-2 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-3620-28SC:admin# show command_history
Command: show command_history

?
?
show traffic_segmentation 1-6
```

```
config traffic_segmentation 1-6 forward_list 7-8
config radius delete 1
config radius add 1 10.48.74.121 key dlink default
config 802.1x reauth port_based ports all
config 802.1x init port_based ports all
config 802.1x auth_mode port_based
config 802.1x auth_parameter ports 1-50 direction both
config 802.1x capability ports 1-5 authenticator
show 802.1x auth_configuration ports 1
show 802.1x auth_state ports 1-5
enable 802.1x
show 802.1x auth_state ports 1-5
show igmp_snooping
enable igmp_snooping

DGS-3620-28SC:admin#
```

## 16-3 config command_history

### Description

This command is used to configure the number of commands that the switch can record. The switch can keep records for the last 40 (maximum) commands you entered.

### Format

**config command_history <value 1-40>**

### Parameters

**<value 1-40>** – Specify the number of commands (1 to 40) that the switch can record. The default value is 25.

### Restrictions

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

### Example

To configure the number of commands the switch can record to the last 20 commands:

```
DGS-3620-28SC:admin#config command_history 20
Command: config command_history 20

Success.

DGS-3620-28SC:admin#
```

# Chapter 17 Command Logging Command List

**enable command logging**

**disable command logging**

**show command logging**

## 17-1 enable command logging

### Description

The enable command logging command is used to enable the command logging function.

**Note:** When the switch is under the booting procedure and the procedure of downloading the configuration to execute immediately, all configuration commands should not be logged. When the user is 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 Administrator-level users can issue this command.

### Example

To enable the command logging function:

```
DGS-3620-28SC:admin# enable command logging
Command: enable command logging

Success.

DGS-3620-28SC:admin#
```

## 17-2 disable command logging

### Description

The disable command logging command is used to disable the command logging function.

### Format

**disable command logging**

### Parameters

None.

### Restrictions

Only Administrator-level users can issue this command.

### Example

To disable the command logging:

```
DGS-3620-28SC:admin# disable command logging
Command: disable command logging

Success.

DGS-3620-28SC:admin#
```

## 17-3 show command logging

### Description

This command displays the switch’s general command logging configuration status.

### Format

**show command logging**

### Parameters

None.

### Restrictions

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

### Example

To show the command logging configuration status:

```
DGS-3620-28SC:admin# show command logging
Command: show command logging

Command Logging State : Disabled

DGS-3620-28SC:admin#
```

# Chapter 18 Common Unicast Routing Command List

**config route preference** [static | default | rip | ospfIntra | ospfInter | ospfExt1 | ospfExt2 | ebgp | ibgp] <value 1-999>

**show route preference** {[local | static | default | rip | ospf | ospfIntra | ospfInter | ospfExt1 | ospfExt2 | ebgp | ibgp]}

**create route redistribute dst ospf src** [static | rip | bgp | local] {mettype [1 | 2] | metric <value 0-16777214>}

**config route redistribute dst ospf src** [static | rip| bgp | local] {mettype [1 | 2] | metric <value 0-16777214>}(1)

**create route redistribute dst rip src** [local | static | bgp | ospf [all | internal | external | type_1 | type_2 | inter+e1 | inter+e2]] {metric <value 0-16>}

**config route redistribute dst rip src** [local | static | bgp | ospf [all | internal | external | type_1 | type_2 | inter+e1 | inter+e2]] {metric <value 0-16>}

**create route redistribute dst bgp src** [static | local | rip | ospf [all | internal | external | type_1 | type_2 | inter+e1 | inter+e2]] {metric <uint 0-4294967295> | route_map <map_name 16>}

**config route redistribute dst bgp src** [static | rip | local | ospf [all | internal | external | type_1 | type_2 | inter+e1 | inter+e2]] {metric <uint 0-4294967295> | [route_map <map_name 16> | no_route_map]}

**delete route redistribute** [dst [rip | ospf | bgp] src [rip | static | local | ospf | bgp]]

**show route redistribute** {dst [rip | ospf | bgp] | src [rip | static | local | ospf | bgp]}

## 18-1 config route preference

### Description

This command is used to configure the route type preference. The route with smaller preference has higher priority. The preference for local routes is fixed to 0.

### Format

**config route preference [static | default | rip | ospfIntra | ospfInter | ospfExt1 | ospfExt2 | ebgp | ibgp] <value 1-999>**

### Parameters

**static** - Configure the preference of static route.

**default** - Configure the preference of default route.

**rip** - Configure the preference of RIP route.

**ospfIntra** - Configure the preference of OSPF intra-area route.

**ospfInter** - Configure the preference of OSPF inter-area route.

**ospfExt1** - Configure the preference of OSPF external type-1 route.

**ospfExt2** - Configure the preference of OSPF external type-2 route.

**ebgp** - Configure the preference of BGP AS-external route. **(EI Mode Only Parameter)**

**ibgp** - Configure the preference of BGP AS-internal route. **(EI Mode Only Parameter)**

**<value 1-999>** - Enter the route preference value here. This value must be between 1 and 999.

### Restrictions

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

### Example

To configure the route preference for static routes to 70:

```
DGS-3620-28SC:admin# config route preference static 70
Command: config route preference static 70

Success.

DGS-3620-28SC:admin#
```

## 18-2 show route preference

### Description

This command is used to display the route preference of each route type.

### Format

**show route preference {[local | static | default | rip | ospf | ospfIntra | ospfInter | ospfExt1 | ospfExt2 | ebgp | ibgp]}**

### Parameters

**local** - (Optional) Specifies to display the preference of local route.

**static** - (Optional) Specifies to display the preference of static route.

**default** - (Optional) Specifies to display the preference of default route.

**rip** - (Optional) Specifies to display the preference of RIP route.

**ospf** - (Optional) Specifies to display the preference of all types of OSPF route.

**ospfIntra** - (Optional) Specifies to display the preference of OSPF intra-area route.

**ospfInter** - (Optional) Specifies to display the preference of OSPF inter-area route.

**ospfExt1** - (Optional) Specifies to display the preference of OSPF external type-1 route.

**ospfExt2** - (Optional) Specifies to display the preference of OSPF external type-2 route.

**ebgp** - (Optional) Specifies to display the preference of BGP AS-external route. **(EI Mode Only Parameter)**

**ibgp** - (Optional) Specifies to display the preference of BGP AS-internal route. **(EI Mode Only Parameter)**

### Restrictions

None.

### Example

To display the route preference for all route types:

```
DGS-3620-28SC:admin#show route preference
Command: show route preference

Route Preference Settings

Protocol    Preference
----------  ----------
RIP         100
Static      60
Default     1
Local       0
OSPF Intra  80
OSPF Inter  90
OSPF ExtT1  110
OSPF ExtT2  115
EBGP        70
IBGP        130

DGS-3620-28SC:admin#
```

## 18-3 create route redistribute dst ospf src

### Description

This command is used to redistribute the routing information from other routing protocols to OSPF.

### Format

**create route redistribute dst ospf src [static | rip | bgp | local] {mettype [1 | 2] | metric <value 0-16777214>}**

### Parameters

**static** - To redistribute static routes to OSPF.
**rip** - To redistribute the RIP routes to OSPF.
**bgp** - To redistribute the BGP routes to OSPF. **(EI Mode Only Parameter)**
**local** - To redistribute the local routes to OSPF.

**mettype** - (Optional) Allows the selection of one of two methods for calculating the metric value. 1 calculates the metric (for other routing protocols to OSPF) by adding the destination's interface cost to the metric entered in the Metric field. 2 uses the metric entered in the Metric field without change. This field applies only when the destination field is OSPF. If the metric type is not specified, it will be type 2.
**1** - Specifies that the method type value will be set to 1.
**2** - Specifies that the method type value will be set to 2.

**metric** - (Optional) Specifies the metric for the redistributed routes. If it is not specified or specified as 0, the redistributed routes will be associated with the default metric 20.
**<value 0-16777214>** - Enter the metric value used here. This value can be between 0 and 16777214.

### Restrictions

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

### Example

To add route redistribution to OSPF:

```
DGS-3620-28SC:admin# create route redistribute dst ospf src rip
Command: create route redistribute dst ospf src rip

Success.

DGS-3620-28SC:admin#
```

## 18-4 config route redistribute dst ospf src

### Description

This command is used to update the metric to be associated with the redistributed routes from a specific protocol to OSPF protocol.

### Format

**config route redistribute dst ospf src [static | rip| bgp | local] {mettype [1 | 2] | metric <value 0-16777214>}(1)**

### Parameters

**static** - To redistribute the static routes to OSPF.
**rip** - To redistribute RIP routes to OSPF
**bgp** - To redistribute BGP routes to OSPF. **(EI Mode Only Parameter)**
**local** - To redistribute the local routes to OSPF

**mettype** - (Optional) Allows the selection of one of two methods for calculating the metric value. 1 calculates the metric (for other routing protocols to OSPF) by adding the destination’s interface cost to the metric entered in the Metric field. 2 uses the metric entered in the Metric field without change. This field applies only when the destination field is OSPF. If the metric type is not specified, it will be type 2.
**1** - Specifies that the method type value will be set to 1.
**2** - Specifies that the method type value will be set to 2.

**metric** - (Optional) Specifies the metric for the redistributed routes. If it is not specified or specified as 0, the redistributed routes will be associated with the default metric 20.
**<value 0-16777214>** - Enter the metric value used here. This value can be between 0 and 16777214.

### Restrictions

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

### Example

To configure route redistributions:

```
DGS-3620-28SC:admin# config route redistribute dst ospf src rip mettype 1
metric 2
Command: config route redistribute dst ospf src rip mettype 1 metric 2

Succuss.

DGS-3620-28SC:admin#
```

## 18-5 create route redistribute dst rip src

### Description

This command is used to redistribute routing information from other routing protocols to RIP. When the metric is specified as 0, the metric in the original route will become the metric of the redistributed RIP routes transparently. If the metric of the original route is greater than 16, the route will be not redistributed.

### Format

**create route redistribute dst rip src [local | static | bgp | ospf [all | internal | external | type_1 | type_2 | inter+e1 | inter+e2]] {metric <value 0-16>}**

### Parameters

**local** - To redistribute local routes to RIP.

**static** - To redistribute static routes to RIP.

**bgp** - To redistribute BGP routes to RIP. **(EI Mode Only Parameter)**

**ospf** - To redistribute OSPF routes to RIP.
- **all** - To redistribute both OSPF AS-internal and OSPF AS-external routes to RIP.
- **internal** - To redistribute only the OSPF AS-internal routes.
- **external** - To redistribute only the OSPF AS-external routes, including type-1 and type-2 routes.
- **type_1** - To redistribute only the OSPF AS-external type-1 routes.
- **type_2** - To redistribute only the OSPF AS-external type-2 routes.
- **inter+e1** - To redistribute only the OSPF AS-external type-1 and OSPF AS-internal routes.
- **inter+e2** - To redistribute only the OSPF AS-external type-2 and OSPF AS-internal routes.

**metric** - (Optional) Specifies the RIP route metric value for the redistributed routes.
- **<value 0-16> -** Enter the metric value used here. This value must be between 0 and 16.

### Restrictions

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

### Example

To add route redistribution settings:

```
DGS-3620-28SC:admin# create route redistribute dst rip src ospf all metric 2
Command: create route redistribute dst rip src ospf all metric 2

Success.

DGS-3620-28SC:admin#
```

## 18-6 config route redistribute dst rip src

### Description

This command is used to update the metric to be associated with the redistributed routes from a specific protocol to RIP protocol.

### Format

**config route redistribute dst rip src [local | static | bgp | ospf [all | internal | external | type_1 | type_2 | inter+e1 | inter+e2]] {metric <value 0-16>}**

### Parameters

**local** - To redistribute local routes to RIP.

**static** - To redistribute static routes to RIP.

**bgp** - To redistribute BGP routes to RIP. **(EI Mode Only Parameter)**

**ospf** - To redistribute OSPF routes to RIP.
- **all** - To redistribute both OSPF AS-internal and OSPF AS-external routes to RIP.
- **internal** - To redistribute only the OSPF AS-internal routes.
- **external** - To redistribute only the OSPF AS-external routes, including type-1 and type-2 routes.
- **type_1** - To redistribute only the OSPF AS-external type-1 routes.
- **type_2** - To redistribute only the OSPF AS-external type-2 routes.
- **inter+e1** - To redistribute only the OSPF AS-external type-1 and OSPF AS-internal routes.
- **inter+e2** - To redistribute only the OSPF AS-external type-2 and OSPF AS-internal routes.

**metric** - (Optional) Specifies the RIP metric value for the redistributed routes.
- **<value 0-16>** - Enter the metric value used here. This value must be between 0 and 16.

### Restrictions

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

### Example

To configure route redistributions:

```
DGS-3620-28SC:admin# config route redistribute dst rip src ospf internal
Command: config route redistribute dst rip src ospf internal

Success.

DGS-3620-28SC:admin#
```

## 18-7 create route redistribute dst bgp src

### Description

This command is used to redistribute routing information from other routing protocols to BGP.

### Format

**create route redistribute dst bgp src [static | local | rip | ospf [all | internal | external | type_1 | type_2 | inter+e1 | inter+e2]] {metric <uint 0-4294967295> | route_map <map_name 16>}**

### Parameters

**local** - To redistribute local routes to BGP.

**static** - To redistribute static routes to BGP.

**rip** - To redistribute RIP routes to BGP.

**ospf** - To redistribute OSPF routes to BGP.
- **all** - To redistribute both OSPF AS-internal and OSPF AS-external routes to BGP.
- **internal** - To redistribute only the OSPF AS-internal routes.
- **external** - To redistribute only the OSPF AS-external routes, including type-1 and type-2 routes.
- **type_1** - To redistribute only the OSPF AS-external type-1 routes.
- **type_2** - To redistribute only the OSPF AS-external type-2 routes.
- **inter+e1** - To redistribute only the OSPF AS-external type-1 and OSPF AS-internal routes.
- **inter+e2** - To redistribute only the OSPF AS-external type-2 and OSPF AS-internal routes.

**metric** - (Optional) Specifies the BGP metric value for the redistributed routes.
- **<value 0-4294967295>** - Enter the metric value used here. This value must be between 0 and 4294967295.

**route_map** - (Optional) Specifies a route map which will be used as the criteria to determine whether to redistribute specific routes.
- **<map_name 16>** - Enter the route map name used here. This name can be up to 16 characters long.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

To add route redistribution settings:

```
DGS-3620-28SC:admin# create route redistribute dst bgp src ospf all metric 2
Command: create route redistribute dst bgp src ospf all metric 2

Success.

DGS-3620-28SC:admin#
```

## 18-8 config route redistribute dst bgp src

### Description

This command updates the metric to be associated with the redistributed routes from a specific protocol to BGP protocol.

### Format

**config route redistribute dst bgp src [static | rip | local | ospf [all | internal | external | type_1 | type_2 | inter+e1 | inter+e2]] {metric <uint 0-4294967295> | [route_map <map_name 16> | no_route_map]}**

### Parameters

**local** - To redistribute local routes to BGP.

**static** - To redistribute static routes to BGP.

**rip** - To redistribute RIP routes to BGP.

**ospf** - To redistribute OSPF routes to BGP.
- **all** - To redistribute both OSPF AS-internal and OSPF AS-external routes to BGP.
- **internal** - To redistribute only the OSPF AS-internal routes.
- **external** - To redistribute only the OSPF AS-external routes, including type-1 and type-2 routes.
- **type_1** - To redistribute only the OSPF AS-external type-1 routes.
- **type_2** - To redistribute only the OSPF AS-external type-2 routes.
- **inter+e1** - To redistribute only the OSPF AS-external type-1 and OSPF AS-internal routes.
- **inter+e2** - To redistribute only the OSPF AS-external type-2 and OSPF AS-internal routes.

**metric** - (Optional) Specifies the BGP metric value for the redistributed routes.
- **<value 0-4294967295>** - Enter the metric value used here. This value must be between 0 and 4294967295.

**route_map** - (Optional) Specifies a route map which will be used as the criteria to determine whether to redistribute specific routes.
- **<map_name 16>** - Enter the route map name used here. This name can be up to 16 characters long.
- **no_route_map** - Specifies to withdraw the route map setting.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

To add route redistribution settings:

```
DGS-3620-28SC:admin# config route redistribute dst bgp src ospf all metric 2
Command: config route redistribute dst bgp src ospf all metric 2

Success.

DGS-3620-28SC:admin#
```

## 18-9 delete route redistribute

### Description

This command is used to delete the route redistribute configuration on the switch.

### Format

**delete route redistribute [dst [rip | ospf | bgp] src [rip | static | local | ospf | bgp]]**

### Parameters

**dst** - Specifies the target protocol.
- **rip** - Specifies to not redistribute other routing protocols to RIP.
- **ospf** - Specifies to not redistribute other routing protocols to OSPF.
- **bgp** - Specifies to not redistribute other routing protocols to BGP. **(EI Mode Only Parameter)**

**src** - Specifies the source protocol.
- **rip** - Specifies to not redistribute RIP routes.
- **static** - Specifies to not redistribute static routes.
- **local** - Specifies to not redistribute local routes.
- **ospf** - Specifies to not redistribute OSPF routes.
- **bgp** - Specifies to not redistribute BGP routes. **(EI Mode Only Parameter)**

### Restrictions

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

### Example

To delete route redistribution settings:

```
DGS-3620-28SC:admin# delete route redistribute dst rip src ospf
Command: delete route redistribute dst rip src ospf

Success.

DGS-3620-28SC:admin#
```

## 18-10 show route redistribute

### Description

This command is used to display the route redistribution settings on the switch.

### Format

**show route redistribute {dst [rip | ospf | bgp] | src [rip | static | local | ospf | bgp]}**

### Parameters

**dst** - (Optional) Specifies the target protocol.
- **rip** - Specifies to display the redistribution with the target protocol RIP.
- **ospf** - Specifies to display the redistribution with the target protocol OSPF.
- **bgp** - Specifies to display the redistribution with the target protocol BGP. **(EI Mode Only Parameter)**

**src** - (Optional) Specifies the source protocol.
- **rip** - Specifies to display the redistribution with the source protocol RIP.
- **static** - Specifies to display the redistribution with the source static.
- **local** - Specifies to display the redistribution with the source local.
- **ospf** - Specifies to display the redistribution with the source protocol OSPF.
- **bgp** - Specifies to display the redistribution with the source protocol BGP. **(EI Mode Only Parameter)**

If no parameter is specified, the system will display all route redistributions.

### Restrictions

None.

## Example

To display route redistributions:

```
DGS-3620-28SC:admin#show route redistribute
Command: show route redistribute

Route Redistribution Settings

Source    Destination   Type      Metric      RouteMapName
Protocol  Protocol
--------  ------------  --------  ------      ------------
RIP       OSPF          Type-1    2

Total Entries : 1

DGS-3620-28SC:admin#
```

# Chapter 19 Compound Authentication Commands

| |
|---|
| **create authentication guest_vlan** [vlan <vlan_name 32> \| vlanid <vlanid 1-4094>] |
| **delete authentication guest_vlan** [vlan <vlan_name 32> \| vlanid <vlanid 1-4094>] |
| **config authentication guest_vlan** [vlan <vlan_name 32> \| vlanid <vlanid 1-4094>] [add \| delete] ports [<portlist> \| all] |
| **config authentication 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_jwac \| impb_wac \| mac_impb]}(1) |
| **show authentication** |
| **show authentication guest_vlan** |
| **show authentication mac_format** |
| **show authentication ports** {<portlist>} |
| **enable authorization attributes** |
| **disable authorization attributes** |
| **show authorization** |
| **config authentication server failover** [local \| permit \| block] |

## 19-1 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.<br>**<vlan_name 32>** - Specify the guest VLAN by VLAN name. The VLAN name can be up to 32 characters long. |
| **vlanid** - Specify the guest VLAN by VLAN ID.<br>**<vlanid 1-4094>** - Specify the guest VLAN by VLAN ID. The VLAN ID value must be between 1 and 4094. |

### Restrictions

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

### Example

To assign a static VLAN to be a guest VLAN:

```
DGS-3620-28SC:admin#create authentication guest_vlan vlan guestVLAN
Command: create authentication guest_vlan vlan guestVLAN

Success.

DGS-3620-28SC:admin#
```

## 19-2 delete authentication guest_vlan

### Description

This command is used to delete a guest VLAN setting, but not a static VLAN. All ports which are enabled as guest VLANs will move to the original VLAN after deleting the 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>** - Specify 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>** - Specify the guest VLAN by VLAN ID. The VLAN ID value must be between 1 and 4094.

### Restrictions

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

### Example

To delete a guest VLAN setting:

```
DGS-3620-28SC:admin#delete authentication guest_vlan vlan guestVLAN
Command: delete authentication guest_vlan vlan guestVLAN

Success.

DGS-3620-28SC:admin#
```

## 19-3 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>** - Specify the guest VLAN name. The VLAN name can be up to 32 characters long.

**vlanid** - Specify the guest VLAN VID.
    **<vlanid 1-4094>** - Specify 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>** - Specify a range of ports to configure.
    **all** - Specify to configure all ports.

### Restrictions

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

### Example

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

```
DGS-3620-28SC:admin#config authentication guest_vlan vlan gv add ports all
Command: config authentication guest_vlan vlan gv add ports all

Success.

DGS-3620-28SC:admin#
```

## 19-4 config authentication mac_format

### Description

This command will 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** - (Optional) Specifies the case format used.
    **lowercase** - Specifies using the lowercase format, the RADIUS authentication username will be formatted as: aa-bb-cc-dd-ee-ff.
    **uppercase** - Specifies using the uppercase format, the RADIUS authentication username will be formatted as: AA-BB-CC-DD-EE-FF.

**delimiter** - (Optional) Specifies the delimiter format used.

**hyphen** - Specifies using the “-“ as delimiter, the format is: AA-BB-CC-DD-EE-FF
**colon** - Specifies using the “:“ as delimiter, the format is: AA:BB:CC:DD:EE:FF
**dot** - Specifies using the “.“ as delimiter, the format is: AA.BB.CC.DD.EE.FF
**none** - Specifies not using any delimiter, the format is: AABBCCDDEEFF

**number** - (Optional) Specifies 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 Administrator, Operator and Power-User level users can issue this command.

### Example

To configure the MAC address format to IETF style:

```
DGS-3620-28SC:admin#config authentication mac_format case uppercase delimiter
hyphen number 5
Command: config authentication mac_format case uppercase delimiter hyphen
number 5


Success.


DGS-3620-28SC:admin#
```

## 19-5 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_jwac | impb_wac | mac_impb]}(1)**

### Parameters

**<portlist>** - Specify a port or range of ports to configure.
**all** - Specify to configure all ports.

**auth_mode** - (Optional) 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 authorization, this port will keep trying the next authentication.
**host-based** - Specify to allow every user to be authenticated individually.
**vlanid** - (Optional) Specifies the VLAN ID used for this configuration.
**<vid_list>** - Enter the VLAN ID used for this configuration here.

**state** - (Optional) Specifies whether the authorization mode will be enabled or disabled.
**enable** - Specifies that the authorization mode will be enabled.
**disable** - Specifies that the authorization mode will be disabled.

**multi_authen_methods** - (Optional) Specify the method for compound authentication.
**none** - Specify that compound authentication is not enabled.
**any** - Specify if any of the authentication methods (802.1X, MAC, and JWAC/WAC) pass, then

pass.

**dot1x_impb** - Dot1x will be verified first, and then IMPB will be verified. Both authentications need to be passed.

**impb_jwac** - JWAC 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.

### Restrictions

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

### Example

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

```
DGS-3620-28SC:admin#config authentication ports all auth_mode host_based
Command: config authentication ports all auth_mode host_based

Success.

DGS-3620-28SC:admin#
```

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

```
DGS-3620-28SC:admin#config authentication ports all multi_authen_methods any
Command: config authentication ports all multi_authen_methods any

Success.

DGS-3620-28SC:admin#
```

## 19-6 show authentication

### Description

This command is used to display the global authentication configuration.

### Format

**show authentication**

### Parameters

None.

### Restrictions

None.

### Example

To display the global authentication configuration:

```
DGS-3620-28SC:admin#show authentication
Command: show authentication

Authentication Server Failover: Block.

DGS-3620-28SC:admin#
```

## 19-7 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-3620-28SC:admin#show authentication guest_vlan
Command: show authentication guest_vlan

Guest VLAN VID         :
Guest VLAN Member Ports:

 Total Entries: 0

DGS-3620-28SC:admin#
```

## 19-8 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-3620-28SC:admin#show authentication mac_format
Command: show authentication mac_format

 Case              : Uppercase
 Delimiter         : None
 Delimiter Number  : 5

DGS-3620-28SC:admin#
```

## 19-9 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) Specify to display compound authentication on specific port(s).

### Restrictions

None.

### Example

To display the authentication settings for ports 1 to 3:

```
DGS-3620-28SC: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-3620-28SC:admin#
```

## 19-10 enable authorization attributes

### Description

This command is used to enable the authorization global state.

### Format

**enable authorization attributes**

### Parameters

None.

### Restrictions

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

### Example

To enable the authorization global state:

```
DGS-3620-28SC:admin#enable authorization attributes
Command: enable authorization attributes

Success.

DGS-3620-28SC:admin#
```

## 19-11 disable authorization attributes

### Description

This command is used to disable the authorization global state.

### Format

**disable authorization attributes**

### Parameters

None.

### Restrictions

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

### Example

To disable the authorization global state:

```
DGS-3620-28SC:admin#disable authorization attributes
Command: disable authorization attributes

Success.

DGS-3620-28SC:admin#
```

## 19-12 show authorization

### Description

This command is used to display the authorization status.

### Format

**show authorization**

### Parameters

None.

### Restrictions

None.

### Example

To display the authorization status:

```
DGS-3620-28SC:admin#show authorization
Command: show authorization
Authorization for Atributes: Enabled

DGS-3620-28SC:admin#
```

## 19-13 config authentication server failover

### Description

This command is used to configure the authentication server failover function. When authentication server fails, administrator can configure to:

* Use the local database to authenticate the client. The switch will resort to using the local database to authenticate the client. If the client fails on local authentication, the client is regarded as un-authenticated, otherwise, it authenticated.

* Pass authentication. The client is always regarded as authenticated. If guest VLAN is enabled, clients will stay on the guest VLAN, otherwise, they will stay on the original VLAN.

* Block the client (default setting). The client is always regarded as un-authenticated.

## Format

**config authentication server failover [local | permit | block]**

## Parameters

| |
|---|
| **local** - Specify to use the local database to authenticate the client. |
| **permit** - Specify that the client is always regarded as authenticated. |
| **block** - Specify to block the client. This is the default setting. |

## Restrictions

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

## Example

To set the authentication server failover state:

```
DGS-3620-28SC:admin#config authentication server failover local
Command: config authentication server failover local

Success.

DGS-3620-28SC:admin#
```

# Chapter 20 Debug Software Command List

| |
|---|
| **debug address_binding** [event \| dhcp \| all] state [enable \| disable] |
| **no debug address_binding** |
| **debug error_log** [dump \| clear \| upload_toTFTP <ipaddr> <path_filename 64>] |
| **debug buffer** [utilization \| dump \| clear \| upload_toTFTP <ipaddr> <path_filename 64>] |
| **debug output** [module <module_list> \| all] [buffer \| console] |
| **debug config error_reboot** [enable \| disable] |
| **debug config state** [enable \| disable] |
| **debug show error_reboot state** |
| **debug stp clear counter** {ports [<portlist> \| all]} |
| **debug stp config ports** [<portlist> \| all] [event \| bpdu \| state_machine \| all] state [disable \| brief \| detail] |
| **debug stp show counter** {ports [<portlist> \| all]} |
| **debug stp show flag** {ports <portlist>} |
| **debug stp show information** |
| **debug stp state** [disable \| enable] |
| **debug ospf** [neighbor_state_change \| interface_state_change {dr_bdr_selection} \| lsa {all \| originating \| installing \| receiving \| flooding} (1) \| packet {all \| receiving \| sending} (1) \| retransmission \| spf {all \| intra \| inter \| extern} (1) \| timer \| virtual_link \| route \| redistribution] state [enable \| disable] |
| **debug ospf clear counter** {packet \| neighbor \| spf} |
| **debug ospf log state** [enable \| disable] |
| **debug ospf show counter** {packet \| neighbor \| spf} |
| **debug ospf show detail external_link** |
| **debug ospf show detail net_link** |
| **debug ospf show detail rt_link** |
| **debug ospf show detail summary_link** |
| **debug ospf show detail type7_link** |
| **debug ospf show flag** |
| **debug ospf show log state** |
| **debug ospf show redistribution** |
| **debug ospf show request_list** |
| **debug ospf show summary_list** |
| **debug ospf state** [enable \| disable] |
| **debug vrrp** [vr_state_change \| packet [all \| {receiving \| sending}(1)] \| mac_addr_update \| interface_change \| timers] state [enable \| disable] |
| **debug vrrp clear counter** |
| **debug vrrp log state** [enable \| disable] |
| **debug vrrp show counter** |
| **debug vrrp show flag** |
| **debug vrrp show log state** |
| **debug vrrp state** [enable \| disable] |
| **debug bgp show flag** |
| **debug bgp all flag** [enable \| disable] |
| **debug bgp fsm_event** [enable \| disable] |
| **debug bgp packet** [{open \| update \| keepalive \| notify \| refresh \| capability}(1) \| all] [in \| out] [enable \| disable] |
| **debug bgp error state** [enable \| disable] |
| **debug bgp show global_info** |
| **debug bgp show peer** |

| |
|---|
| **debug bgp show peer_group** |
| **debug bgp show network** |
| **debug bgp show aggregate** |
| **debug bgp show damp** |
| **debug bgp show interface_info** |
| **debug bgp show as_path_access_list** |
| **debug bgp show bgp_timer** |
| **debug bgp show community_list** |
| **debug bgp show redist_info** |
| **debug bgp router_map** [enable \| disable] |
| **debug bgp access_list** [enable \| disable] |
| **debug bgp prefix_list** [enable \| disable] |
| **debug dhcpv6_client state enable** |
| **debug dhcpv6_client state disable** |
| **debug dhcpv6_client output** [buffer \| console] |
| **debug dhcpv6_client packet** {all \| receiving \| sending} state [enable \| disable] |
| **debug dhcpv6_relay state enable** |
| **debug dhcpv6_relay state disable** |
| **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_server packet** [all \| receiving \| sending] state [enable \| disable] |
| **debug dhcpv6_server state disable** |
| **debug dhcpv6_server state enable** |
| **debug pim ssm** |
| **no debug pim ssm** |
| **debug ripng flag** [{interface \| packet [all \| rx \| tx] \| route} \| all] state [enable \| disable] |
| **debug ripng show flag** |
| **debug ripng state disable** |
| **debug ripng state enable** |
| **debug routefilter show** [prefix_list \| access_list \| route_map] |
| **debug show status** {module <module_list>} |
| **debug super_vlan state** [enable \| disable] |

## 20-1 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** - To print out the debug messages when IMPB module receives ARP/IP packets.<br>**dhcp** - To print out the debug messages when the IMPB module receives the DHCP packets.<br>**all** - Print out all debug messages. | |
| **state** - Specifies the state of the address binding debugging option.<br>**enable** - Specifies that the address binding debugging option will be enabled.<br>**disable** - Specifies that the address binding debugging option will be disabled. | |

### Restrictions

Only Administrator level users can issue this command.

### Example

To print out all debug IMPB messages:

```
DGS-3620-28SC:admin# debug address_binding all state enable
Command: debug address_binding all state enable

Success.

DGS-3620-28SC:admin#
```

## 20-2 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 level users can issue this command.

### Example

To stop IMPB debug: starting when the IMPB module receives an ARP/IP or DHCP packet:

```
DGS-3620-28SC:admin# no debug address_binding
Command: no debug address_binding

Success.

DGS-3620-28SC:admin#
```

## 20-3 debug error_log

### Description

Use this command 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** - Display the debug message of the debug log.

**clear** - Clear the debug log.

**upload_toTFTP** - Upload the debug log to a TFTP server specified by IP address.
  **<ipaddr>** - Specifies the IPv4 address of the TFTP server.
  **<path_filename 64>** - The pathname specifies the DOS pathname on the TFTP server. It can be a relative pathname or an absolute pathname. This value can be up to 64 characters long.

## Restrictions

Only Administrator level users can issue this command.

## Example

To dump the error log:

```
DGS-3620-28SC:admin# debug error_log dump
Command: debug error_log dump

**************************************************************************
# debug log: 1
# firmware version: 1.00.011
# level: CPU exception
# clock: 437453880 ms
# time : 2000-01-08 05:55:40

======================== CPU EXCEPTION ========================
Current Task = IP-Tic Stack Pointer = 4CFEA7A0
---------------------------CP0 Registers-----------------------
Status : 1000FC01  Interrupt enable  Normal level
Cause  : 00000008  TLB exception (load or instruction fetch)
EPC    : 80A0297C        Addr   : 00000008
Stack  : 4CFEA7A0        Return : 80A02938
------------------------normal registers-----------------------
$0( $0) : 00000000  at( $1) : FFFFFFFE  v0( $2) : 00000000  v1( $3) : 00000001
a0( $4) : 00000000  a1( $5) : 4825B4A8  a2( $6) : 00000001  a3( $7) : 00000001
t0( $8) : 814D7FCC  t1( $9) : 0000FC00  t2($10) : 828100C4  t3($11) : 00000017
t4($12) : 828100BC  t5($13) : 4CFEA430  t6($14) : 82810048  t7($15) : 00000000
s0($16) : 4825D94A  s1($17) : 4825D890  s2($18) : 4825D949  s3($19) : 4825D946
s4($20) : 00000000  s5($21) : 00000008  s6($22) : 81800000  s7($23) : 00090000
t8($24) : 00000000  t9($25) : FFFFFFC0  k0($26) : 00000000  k1($27) : 00000000
gp($28) : 8180ADA0  sp($29) : 4CFEA7A0  fp($30) : 00000001  ra($31) : 80A02938



------------------------- TASK STACKTRACE ------------------------
->81150A58
->809B346C
```

```
->809E1DEC
->809D7E6C
->80A038CC
->80A033B0
->80A0297C
```

To clear the error log:

```
DGS-3620-28SC:admin# debug error_log clear
Command: debug error_log clear

Success.

DGS-3620-28SC:admin#
```

To upload the error log to TFTP server:

```
DGS-3620-28SC: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 configuration.................. Done.

DGS-3620-28SC:admin#
```

## 20-4 debug buffer

### Description

Use this command to show the debug buffer’s state, or dump, clear, or upload the debug buffer to a TFTP server.

**Note:** When selecting to output to the debug buffer and there are debug messages being outputted, the system memory pool will be used as the debug buffer. The functions which will use the system memory pool resource may fail to execute command such as download and upload firmware, or save configuration. If you want to execute these commands successfully, please use the command “debug buffer clear” to release the system’s memory pool resources manually first.

### Format

**debug buffer [utilization | dump | clear | upload_toTFTP <ipaddr> <path_filename 64>]**

### Parameters

**utilization** - Display the debug buffer’s state.

**dump** - Display the debug message in the debug buffer.

**clear** - Clear the debug buffer.

**upload_toTFTP** - Upload the debug buffer to a TFTP server specified by IP address.
- **<ipaddr>** - Specifies the IPv4 address of the TFTP server.
- **<path_filename 64>** - The pathname specifies the DOS pathname on the TFTP server. It can be a relative pathname or an absolute pathname. This value can be up to 64 characters

| | |
|---|---|
| | long. |

### Restrictions

Only Administrator level users can issue this command.

### Example

To show the debug buffer's state:

```
DGS-3620-28SC:admin# debug buffer utilization
Command: debug buffer utilization

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

DGS-3620-28SC:admin#
```

To clear the debug buffer:

```
DGS-3620-28SC:admin# debug buffer clear
Command: debug buffer clear

Success.

DGS-3620-28SC:admin#
```

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

```
DGS-3620-28SC: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 configuration.................. Done.

DGS-3620-28SC:admin#
```

## 20-5 debug output

### Description

Use the command 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.

**Note:** When selecting to output to the debug buffer and there are debug messages being outputted, the system memory pool will be used as the debug buffer. The functions which will use the system memory pool resource may fail to execute command such as download and upload firmware, or save configuration. If you want to execute these commands successfully, please use the command "debug buffer clear" to release the system's memory pool resources manually first.

### Format

**debug output [module <module_list> | all] [buffer | console]**

### Parameters

**module** - Specifies the module list.
  **<module_list>** - Enter the module list here.
  **all** - Control output method of all modules.

**buffer** - Direct the debug message of the module output to debug buffer(default).

**console** - Direct the debug message of the module output to local console.

### Restrictions

Only Administrator level users can issue this command.

### Example

To set all module debug message outputs to local console:

```
DGS-3620-28SC:admin# debug output all console
Command: debug output all console

Success.

DGS-3620-28SC:admin#
```

## 20-6 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** - Need reboot switch when fatal error happens.(if the project do not define the default setting, enable for default).

**disable** - Do not need reboot switch when fatal error happens, system will hang-up for debug and enter the debug shell mode for debug.

### Restrictions

Only Administrator level users can issue this command.

### Example

To set the switch to not need a reboot when a fatal error occurs:

```
DGS-3620-28SC:admin# debug config error_reboot disable
Command: debug config error_reboot disable

Success.

DGS-3620-28SC:admin#
```

## 20-7 debug config state

### Description

Use the command to set the state of the debug.

### Format

**debug config state [enable | disable]**

### Parameters

**enable** - Enable the debug state.
**disable** - Disable the debug state.

### Restrictions

Only Administrator level users can issue this command.

### Example

To set the debug state to disabled:

```
DGS-3620-28SC:admin# debug config state disable
Command: debug config state disable

Success.

DGS-3620-28SC:admin#
```

## 20-8 debug show error_reboot state

### Description

Use the command to show the error reboot status.

### Format

**debug show error_reboot state**

### Parameters

None.

### Restrictions

Only Administrator level users can issue this command.

### Example

To show the error reboot status:

```
DGS-3620-28SC:admin#debug show error_reboot state
Command: debug show error_reboot state

Error Reboot: Enabled

DGS-3620-28SC:admin#
```

## 20-9 debug stp clear counter

### Description

This command used to clear the STP counters.

### Format

**debug stp clear counter {ports [<portlist> | all]}**

### Parameters

**ports** - Specifies the port range.
  **<portlist>** - Enter the list of port used for this configuration here.
  **all** - Clears all port counters.

### Restrictions

Only Administrator level users can issue this command.

### Example

To clear all STP counters on the switch:

```
DGS-3620-28SC:admin# debug stp clear counter ports all
Command : debug stp clear counter ports all

Success.

DGS-3620-28SC:admin#
```

## 20-10 debug stp config ports

### Description

This command 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

| |
|---|
| **ports** - Specifies the STP port range to debug.<br>**<portlist>** - Enter the list of port used for this configuration here.<br>**all** - Specifies to debug all ports on the switch. |
| **event** - Debug the external operation and event processing.<br>**bpdu** - Debug the BPDU's that have been received and transmitted.<br>**state_machine** - Debug the state change of the STP state machine.<br>**all** - Debug all of the above. |
| **state** - Specifies the state of the debug mechanism.<br>**disable** - Disables the debug mechanism.<br>**brief** - Sets the debug level to brief.<br>**detail** - Sets the debug level to detail. |

### Restrictions

Only Administrator level users can issue this command.

### Example

To configure all STP debug flags to brief level on all ports:

```
DGS-3620-28SC:admin# debug stp config ports all all state brief
Command: debug stp config ports all all state brief

Success.

DGS-3620-28SC:admin#
```

## 20-11 debug stp show counter

### Description

This command used to display the STP counters.

### Format

**debug stp show counter {ports [<portlist> | all]}**

### Parameters

| |
|---|
| **ports** - (Optional) Specifies the STP ports for display.<br>**<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 Administrator level users can issue this command.

### Example

To show the STP counters for port 9:

```
DGS-3620-28SC:admin# debug stp show counter ports 9
Command: debug stp show counter ports 9

STP Counters
--------------------------------------
 Port 9 :
  Receive:                                          Transmit:
  Total STP Packets            :32                  Total STP Packets   :32
  Configuration BPDU           :0                   Configuration BPDU  :0
  TCN BPDU                     :0                 TCN BPDU            :0
  RSTP TC-Flag                 :15                  RSTP TC-Flag       :7
  RST BPDU                     :32                  RST BPDU
            :32

  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

DGS-3620-28SC:admin#
```

## 20-12 debug stp show flag

### Description

This command used to display the STP debug level on specified ports.

### Format

**debug stp show flag {ports <portlist>}**

### Parameters

**ports** - (Optional) Specifies the STP ports to display.

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

If no parameter is specified, all ports on the switch will be displayed.

### Restrictions

Only Administrator level users can issue this command.

### Example

To display the debug STP levels on all ports:

```
DGS-3620-28SC:admin# debug stp show flag
Command: debug stp show flag

Global State: Enabled

Port Index   Event flag   BPDU Flag    State Machine Flag
----------   ----------   ---------    ------------------
  1            Detail        Brief        Disable
  2            Detail        Brief        Disable
  3            Detail        Brief        Disable
  4            Detail        Brief        Disable
  5            Detail        Brief        Disable
  6            Detail        Brief        Disable
  7            Detail        Brief        Disable
  8            Detail        Brief        Disable
  9            Detail        Brief        Disable
  10           Detail        Brief        Disable
  11           Detail        Brief        Disable
  12           Detail        Brief        Disable

DGS-3620-28SC:admin#
```

## 20-13 debug stp show information

### Description

This command used to display STP detailed information, such as the hardware tables, the STP state machine, etc.

### Format

**debug stp show information**

### Parameters

None.

### Restrictions

Only Administrator level users can issue this command.

## Example

To show STP debug information:

```
DGS-3620-28SC:admin# debug stp show information
Command: debug stp show information

Spanning Tree Debug Information:
----------------------------------------
Port Status In Hardware Table:
Instance 0:
Port 1 :BLK  Port 2 :BLK  Port 3 :BLK  Port 4 :BLK  Port 5 :BLK  Port 6 :BLK
Port 7 :FOR  Port 8 :BLK  Port 9 :BLK  Port 10:BLK  Port 11:BLK  Port 12:BLK
Instance 1:
Port 1 :BLK  Port 2 :BLK  Port 3 :BLK  Port 4 :BLK  Port 5 :BLK  Port 6 :BLK
Port 7 :FOR  Port 8 :BLK  Port 9 :BLK  Port 10:BLK  Port 11:BLK  Port 12:BLK
--------------------------------------
Root Priority And Times :
Instance 0:
 Designated Root Bridge    : 32768/00-01-02-03-04-00
 External Root Cost      : 0
 Regional Root Bridge      : 32768/00-01-02-03-04-00
 Internal Root Cost        : 0
 Designated Bridge       : 32768/00-01-02-03-04-00
 Designated Port           : 0
 Message Age               : 0
 Max Age                        : 20
 Forward Delay             : 15
 Hello Time                : 2
Instance 1:
 Regional Root Bridge      : 32769/00-01-02-03-04-00
 Internal Root Cost        : 0
 Designated Bridge         : 32769/00-01-02-03-04-00
 Designated Port           : 0
 Remaining Hops            : 20
--------------------------------------
Designated  Priority And Times:
 Instance 0:
 Port 1 :
 Designated Root Bridge    : 0    /00-00-00-00-00-00
 External Root Cost        : 0
 Regional Root Bridge      : 0    /00-00-00-00-00-00
 Internal Root Cost        : 0
 Designated Bridge         : 0    /00-00-00-00-00-00
 Designated Port           : 0
 Message Age               : 0
 Max Age                   : 20
 Forward Delay             : 15
 Hello Time                : 2

 Instance 1:
 Port 1 :
 Regional Root Bridge      : 0    /00-00-00-00-00-00
 Internal Root Cost        : 0
 Designated Bridge         : 0    /00-00-00-00-00-00
 Designated Port           : 0
 Remaining Hops            : 20


DGS-3620-28SC:admin#
```

## 20-14 debug stp state

### Description

This command is used to enable or disable the STP debug state.

### Format

**debug stp state [enable | disable]**

### Parameters

**state** - Specifies the STP debug state.
**enable** - Enable the STP debug state.
**disable** - Disable the STP debug state.

### Restrictions

Only Administrator level users can issue this command.

### Example

To configure the STP debug state to enable, and then disable the STP debug state:

```
DGS-3620-28SC:admin# debug stp state enable
Command: debug stp state enable

Success.

DGS-3620-28SC:admin# debug stp state disable
Command: debug stp state disable

Success.

DGS-3620-28SC:admin#
```

## 20-15 debug ospf

### Description

This command is used to enable or disable OSPF debug flags.

### Format

**debug ospf [neighbor_state_change | interface_state_change {dr_bdr_selection} | lsa {all | originating | installing | receiving | flooding} (1) | packet {all | receiving | sending} (1) | retransmission | spf {all | intra | inter | extern} (1) | timer | virtual_link | route | redistribution] state [enable | disable]**

### Parameters

**neighbor_state_change** - The state of the OSPF neighbor state change debug.

**interface_state_change** - The state of the OSPF interface state change debug.

**dr_bdr_selection** - (Optional) Used to include or exclude debug information for DR/BDR selection.

**lsa** - The state of the designated debug flag.
- **all** - (Optional) Specifies to set all LSA debug flags.
- **originating** - (Optional) Specifies to set LSA originating debug flag.
- **installing** - (Optional) Specifies to set LSA installing debug flag.
- **receiving** - (Optional) Specifies to set LSA receiving debug flag.
- **flooding** - (Optional) Specifies to set LSA flooding debug flag.

**packet** - The state of the designated debug flag.
- **all** - (Optional) Specifies to set all packet debug flags.
- **receiving** - (Optional) Specifies to set packet receiving debug flag.
- **sending** - (Optional) Specifies to set packet sending debug flag.

**retransmission** - The state of the OSPF retransmission debug flag.

**spf** - The state of the designated debug flag.
- **all** - (Optional) Specifies to set all SPF debug flags.
- **intra** - (Optional) Specifies to set intra-area SPF debug flag.
- **inter** - (Optional) Specifies to set inter-area SPF debug flag.
- **extern** - (Optional) Specifies to set AS external SPF debug flag.

**timer** - The state of the OSPF timer debug flag.

**virtual_link** - The state of the OSPF virtual link debug flag.

**route** - The state of OSPF route debug flag.

**redistribution** - The state of OSPF redistribution debug flag.

**state** - Specifies to set the OSPF debug flags state.
- **enable** - Specifies that the OSPF debug flags state will be enabled.
- **disable** - Specifies that the OSPF debug flags state will be disabled.

### Restrictions

Only Administrator level users can issue this command.

### Example

To enable OSPF neighbor state change debug:

```
DGS-3620-28SC:admin# debug ospf neighbor_state_change state enable
Command: debug ospf neighbor_state_change state enable

Success.

DGS-3620-28SC:admin#
```

To enable OSPF interface state change debug:

```
DGS-3620-28SC:admin# debug ospf interface_state_change state enable
Command: debug ospf interface_state_change state enable

Success.

DGS-3620-28SC:admin#
```

To enable all OSPF LSA debug flags:

```
DGS-3620-28SC:admin# debug ospf lsa all state enable
Command: debug ospf lsa all state enable

Success.

DGS-3620-28SC:admin#
```

To enable all OSPF packet debug flags:

```
DGS-3620-28SC:admin# debug ospf packet all state enable
Command: debug ospf packet all state enable

Success.

DGS-3620-28SC:admin#
```

To enable OSPF retransmission debug flag:

```
DGS-3620-28SC:admin# debug ospf retransmission state enable
Command: debug ospf retransmission state enable

Success.

DGS-3620-28SC:admin#
```

To enable all OSPF SPF debug flags:

```
DGS-3620-28SC:admin# debug ospf spf all state enable
Command: debug ospf spf all state enable

Success.

DGS-3620-28SC:admin#
```

## 20-16 debug ospf clear counter

### Description

This command is used to reset the OSPF statistic counters.

### Format

**debug ospf clear counter {packet | neighbor | spf}**

### Parameters

**packet** - (Optional) Specifies to reset the OSPF packet counter.

**neighbor** - (Optional) Specifies to reset the OSPF neighbor event counter.

**spf** - (Optional) Specifies to reset the OSPF SPF event counter.

If the parameter is not specified, all OSPF counters will be cleared.

### Restrictions

Only Administrator level users can issue this command.

### Example

To clear all OSPF statistic counters:

```
DGS-3620-28SC:admin# debug ospf clear counter
Command: debug ospf clear counter

Success.

DGS-3620-28SC:admin#
```

## 20-17 debug ospf log state

### Description

This command is used to enable or disable the OSPF debug log.

### Format

**debug ospf log state [enable | disable]**

### Parameters

**state** - Specifies the state of the OSPF debug log.
  **enable** - Specifies that the OSPF debug log state will be enabled.
  **disable** - Specifies that the OSPF debug log state will be disabled.

### Restrictions

Only Administrator level users can issue this command.

### Example

To enable the OSPF debug log:

```
DGS-3620-28SC:admin# debug ospf log state enable
Command: debug ospf log state enable

Success.

DGS-3620-28SC:admin#
```

## 20-18 debug ospf show counter

### Description

This command is used to display OSPF statistic counters.

## Format

**debug ospf show counter {packet | neighbor | spf}**

## Parameters

| |
|---|
| **packet** - (Optional) Specifies to display the OSPF packet counter. |
| **neighbor** - (Optional) Specifies to display the OSPF neighbor event counter. |
| **spf** - (Optional) Specifies to display the OSPF SPF event counter. |
| If the parameter is not specified, all OSPF counters will be displayed. |

## Restrictions

Only Administrator level users can issue this command.

## Example

To show all OSPF statistic counters:

```
DGS-3620-28SC:admin# debug ospf show counter
Command: debug ospf show counter

OSPF Debug Statistic Counters
Packet Receiving:
  Total  : 30
  Hello  : 30
  DD     : 0
  LSR    : 0
  LSU    : 0
  LSAck  : 0
  Drop   : 0
  Auth Fail : 0

Packet Sending:
  Total  : 59
  Hello  : 59
  DD     : 0
  LSR    : 0
  LSU    : 0
  LSAck  : 0

Neighbor State:
  Change : 0
  SeqMismatch : 0

SPF Calculation:
  Intra  : 0
  Inter  : 0
  Extern : 0

DGS-3620-28SC:admin#
```

## 20-19 debug ospf show detail external_link

### Description

This command is used to display all AS external LSAs with detail information.

### Format

**debug ospf show detail external_link**

### Parameters

None.

### Restrictions

Only Administrator level users can issue this command.

### Example

To display all AS external LSAs with detail information:

```
DGS-3620-28SC:admin#debug ospf show detail external_link
Command: debug ospf show detail external_link

OSPF Phase2 External Link:

===========
AREA 0.0.0.0:

 AS-External LSA:
 Link-State ID: 192.168.205.0
 Advertising Router: 1.1.1.1
 LS Age: 10 Seconds
 Options: 0x2
 .... ...0 = 0 Bit Isn't Set
 .... ..1. = E: ExternalRoutingCapability
 .... .0.. = MC: NOT Multicast Capable
 .... 0... = N/P: NSSA Bit
 ...0 .... = EA: Not Support Rcv And Fwd EA_LSA
 ..0. .... = DC: Not Support Handling Of Demand Circuits
 .0.. .... = O: O Bit Isn't Set
 0... .... = 7 Bit Isn't Set
 LS Sequence Number: 0x80000001
 Length: 36
 Netmask: 255.255.255.0
 Metric: 20
 Forwarding Address: 10.90.90.101
 External Route Tag: 0
 Internal Field:
 Del_flag: 0x0  I_ref_count: 0  Seq: 0x80000001  Csum: 0xd08e
 Rxtime: 384  Txtime: 0  Orgage: 0
 Current Time: 394

DGS-3620-28SC:admin#
```

## 20-20 debug ospf show detail net_link

### Description

This command is used to display all Network LSAs with detail information.

### Format

**debug ospf show detail net_link**

### Parameters

None.

### Restrictions

Only Administrator level users can issue this command.

### Example

To display all Network LSAs with detail information:

```
DGS-3620-28SC:admin#debug ospf show detail net_link
Command: debug ospf show detail net_link

OSPF Phase2 NET Link:

===========
AREA 0.0.0.0:
 Network LSA:
 Link-State ID: 10.90.90.123
 Netmask: 255.0.0.0
 Advertising Router: 10.90.90.91
 LS Age: 109 Seconds
 Options: 0x2
 .... ...0 = 0 Bit Isn't Set
 .... ..1. = E: ExternalRoutingCapability
 .... .0.. = MC: NOT Multicast Capable
 .... 0... = N/P: NSSA Bit
 ...0 .... = EA: Not Support Rcv And Fwd EA_LSA
 ..0. .... = DC: Not Support Handling Of Demand Circuits
 .0.. .... = O: O Bit Isn't Set
 0... .... = 7 Bit Isn't Set
 LS Sequence Number: 0x80000001
 Length: 32
 Attached Router: 10.90.90.91
 Attached Router: 1.1.1.1
 Internal Field:
 Del_flag: 0x0  I_ref_count: 0  Seq: 0x80000001  Csum: 0x4e99
 Rxtime: 4  Txtime: 4  Orgage: 1
 Current Time: 112

DGS-3620-28SC:admin#
```

## 20-21 debug ospf show detail rt_link

### Description

This command is used to display all Router LSAs with detail information.

### Format

**debug ospf show detail rt_link**

### Parameters

None.

### Restrictions

Only Administrator level users can issue this command.

### Example

To display all Router LSAs with detail information:

```
DGS-3620-28SC:admin#debug ospf show detail rt_link
Command: debug ospf show detail rt_link

OSPF Phase2 RT Link:

===========
AREA 0.0.0.0:
 Router LSA:
 Link-State ID: 1.1.1.1
 Advertising Router: 1.1.1.1
 LS Age: 10 Seconds
 Options: 0x2
 .... ...0 = 0 Bit Isn't Set
 .... ..1. = E: ExternalRoutingCapability
 .... .0.. = MC: NOT Multicast Capable
 .... 0... = N/P: NSSA Bit
 ...0 .... = EA: Not Support Rcv And Fwd EA_LSA
 ..0. .... = DC: Not Support Handling Of Demand Circuits
 .0.. .... = O: O Bit Isn't Set
 0... .... = 7 Bit Isn't Set
 LS Sequence Number: 0x80000002
 Length: 36
 Flags: 0x0
 .... ...0 = B: Not Area Border Router
 .... ..0. = E: Not AS Boundary Router
 .... .0.. = V: Not Virtual Link Endpoint
 Number Of Links: 1
 Type: Transit    ID: 10.90.90.123     Data: 10.90.90.91      Metric: 1
 Internal Field:
 Del_flag: 0x0  I_ref_count: 0  Seq: 0x80000002  Csum: 0xd81d
 Rxtime: 5  Txtime: 0  Orgage: 0
 Current Time: 15

DGS-3620-28SC:admin#
```

## 20-22 debug ospf show detail summary_link

### Description

This command is used to display all Summary LSAs with detail information.

### Format

**debug ospf show detail summary_link**

### Parameters

None.

### Restrictions

Only Administrator level users can issue this command.

### Example

To display all Summary LSAs with detail information:

```
DGS-3620-28SC:admin#debug ospf show detail summary_link
Command: debug ospf show detail summary_link

OSPF Phase2 Summary Link:

===========
AREA 0.0.0.0:
 Summary LSA:
 Link-State ID: 20.1.1.0
 Advertising Router: 10.90.90.91
 LS Age: 10 Seconds
 Options: 0x2
 .... ...0 = 0 Bit Isn't Set
 .... ..1. = E: ExternalRoutingCapability
 .... .0.. = MC: NOT Multicast Capable
 .... 0... = N/P: NSSA Bit
 ...0 .... = EA: Not Support Rcv And Fwd EA_LSA
 ..0. .... = DC: Not Support Handling Of Demand Circuits
 .0.. .... = O: O Bit Isn't Set
 0... .... = 7 Bit Isn't Set
 LS Sequence Number: 0x80000001
 Length: 28
 Netmask: 255.255.255.0
 Metric: 1
 Internal Field:
 Del_flag: 0x0  I_ref_count: 0  Seq: 0x80000001  Csum: 0x8f9c
 Rxtime: 246  Txtime: 246  Orgage: 1
 Current Time: 255

DGS-3620-28SC:admin#
```

## 20-23 debug ospf show detail type7_link

### Description

This command is used to display all type-7 LSAs with detail information.

### Format

**debug ospf show detail type7_link**

### Parameters

None.

### Restrictions

Only Administrator level users can issue this command.

### Example

To display all type-7 LSAs with detail information:

```
DGS-3620-28SC:admin#debug ospf show detail type7_link
Command: debug ospf show detail type7_link

OSPF Phase2 NSSA-External Link:

===========
AREA 0.0.0.1:

 NSSA-External LSA:
 Link-State ID: 0.0.0.0
 Advertising Router: 10.90.90.91
 LS Age: 855 Seconds
 Options: 0x2
 .... ...0 = 0 Bit Isn't Set
 .... ..1. = E: ExternalRoutingCapability
 .... .0.. = MC: NOT Multicast Capable
 .... 0... = N/P: NSSA Bit
 ...0 .... = EA: Not Support Rcv And Fwd EA_LSA
 ..0. .... = DC: Not Support Handling Of Demand Circuits
 .0.. .... = O: O Bit Isn't Set
 0... .... = 7 Bit Isn't Set
 LS Sequence Number: 0x80000002
 Length: 36
 Netmask: 0.0.0.0
 Metric: 0
 Forwarding Address: 0.0.0.0
 External Route Tag: 0
 Internal Field:
 Del_flag: 0x0  I_ref_count: 0  Seq: 0x80000002  Csum: 0x77be
 Rxtime: 2301  Txtime: 0  Orgage: 0
 Current Time: 3156

DGS-3620-28SC:admin#
```

## 20-24 debug ospf show flag

### Description

This command is used to display the OSPF debug flag setting.

### Format

**debug ospf show flag**

### Parameters

None.

### Restrictions

Only Administrator level users can issue this command.

### Example

To show the current OSPF debug flag setting:

```
DGS-3620-28SC:admin# debug ospf show flag
Command: debug ospf show flag

Global State: Enabled

Current OSPF Flags Setting:

 Neighbor State Change
 Interface State Change
 LSA Originating
 LSA Operating
 LSA Receiving
 LSA Flooding
 Packet Receiving
 Packet Sending
 Retransmission
 Timer
 DR Selection
 Route
 Redistribution
 Virtual Link
 SPF Intra
 SPF Inter
 SPF Extern

DGS-3620-28SC:admin#
```

## 20-25 debug ospf show log state

### Description

This command is used to display the OSPF debug log state.

### Format

**debug ospf show log state**

### Parameters

None.

### Restrictions

Only Administrator level users can issue this command.

### Example

To display the debug OSPF log state:

```
DGS-3620-28SC:admin# debug ospf show log state
Command: debug ospf show log state

 OSPF Log State : Enabled

DGS-3620-28SC:admin#
```

## 20-26 debug ospf show redistribution

### Description

This command is used to display the current internal OSPF redistribute list.

### Format

**debug ospf show redistribution**

### Parameters

None.

### Restrictions

Only Administrator level users can issue this command.

### Example

To display the current OSPF redistribution list:

```
DGS-3620-28SC:admin# debug ospf show redistribution
Command: debug ospf show redistribution

OSPF Redistribution List:

IP                  Nexthop          State Type Tag
------------------  ---------------  ----- ---- ---------------
1.1.1.0/24          0.0.0.0          ON    2    0.0.0.0

OSPF ASE Table:

IP                  Nexthop          State Type Tag
------------------  ---------------  ----- ---- ---------------
1.1.1.0/24          0.0.0.0          ON    2    0.0.0.0

DGS-3620-28SC:admin#
```

## 20-27 debug ospf show request_list

### Description

This command is used to display the current internal OSPF request list.

### Format

**debug ospf show request_list**

### Parameters

None.

### Restrictions

Only Administrator level users can issue this command.

### Example

To display the current OSPF request list:

```
DGS-3620-28SC:admin# debug ospf show request_list
Command: debug ospf show request_list

OSPF Request List:

Area 0.0.0.0:
Circuit: 1.1.1.1
Neighbor: 90.2.0.1  IP: 1.1.1.2
 LSID: 192.194.134.0  RTID: 90.2.0.1
 LSID: 192.194.135.0  RTID: 90.2.0.1
 LSID: 192.194.136.0  RTID: 90.2.0.1
 LSID: 192.194.137.0  RTID: 90.2.0.1
 LSID: 192.194.138.0  RTID: 90.2.0.1

DGS-3620-28SC:admin#
```

## 20-28 debug ospf show summary_list

### Description

This command is used to display the current internal OSPF summary list.

### Format

**debug ospf show summary_list**

### Parameters

None.

### Restrictions

Only Administrator level users can issue this command.

### Example

To display the current OSPF summary list:

```
DGS-3620-28SC:admin# debug ospf show summary_list
Command: debug ospf show summary_list

OSPF Summary List:

Area 0.0.0.0:
Circuit: 1.1.1.1
Neighbor: 90.2.0.1  IP: 1.1.1.2
LSID: 1.1.1.1 RTID: 1.1.1.1

Circuit: 2.2.2.1

Circuit: 10.1.1.6

DGS-3620-28SC:admin#
```

## 20-29 debug ospf state

### Description

This command is used to set the OSPF debug global state.

### Format

**debug ospf state [enable | disable]**

### Parameters

**state** - Specifies the OSPF debug global state.
**enable** - Specifies that the OSPF debug global state will be enabled.
**disable** - Specifies that the OSPF debug global state will be disabled.

### Restrictions

Only Administrator level users can issue this command.

### Example

To enable the OSPF debug global state:

```
DGS-3620-28SC:admin# debug ospf state enable
Command: debug ospf state enable

Success.

DGS-3620-28SC:admin# debug ospf show flag
Command: debug ospf show flag

Global State: Enabled

Current OSPF Flags Setting:

 Neighbor State Change

DGS-3620-28SC:admin#
```

## 20-30 debug vrrp

### Description

This command is used to set VRRP debug flags.

### Format

**debug vrrp [vr_state_change | packet [all | {receiving | sending}(1)] | mac_addr_update | interface_change | timers] state [enable | disable]**

### Parameters

| |
|---|
| **vr_state_change** - Specifies the state of the VRRP change debug flag. |
| **packet** - Specifies to set the VRRP packet flags.<br>**all** - Specifies to set VRRP all packet debug flags.<br>**receiving** - (Optional) Specifies to set the VRRP packet receiving flag.<br>**sending** - (Optional) Specifies to set the VRRP packet sending flag. |
| **mac_addr_update** - Specifies the state of VRRP MAC debug flag. |
| **interface_change** - Specifies the state of VRRP interface debug flag. |
| **timers** - Specifies the state of VRRP timer's debug flag. |
| **state** - Specifies the state of the configured VRRP debug flag.<br>**enable** - Specifies that the configured VRRP debug flag will be enabled.<br>**disable** - Specifies that the configured VRRP debug flag will be disabled. |

### Restrictions

Only Administrator level users can issue this command.

### Example

To enable the VRRP virtual router state change debug flag:

```
DGS-3620-28SC:admin# debug vrrp vr_state_change state enable
Command: debug vrrp vr_state_change state enable

Success.

DGS-3620-28SC:admin#
```

To enable all VRRP packet debug flags:

```
DGS-3620-28SC:admin# debug vrrp packet all state enable
Command: debug vrrp packet all state enable

Success.

DGS-3620-28SC:admin#
```

To enable VRRP virtual MAC address update debug flag:

```
DGS-3620-28SC:admin# debug vrrp mac_addr_update state enable
Command: debug vrrp mac_addr_update state enable

Success.

DGS-3620-28SC:admin#
```

To enable VRRP interface state change debug flag:

```
DGS-3620-28SC:admin# debug vrrp interface_change state enable
Command: debug vrrp interface_change state enable

Success.

DGS-3620-28SC:admin#
```

To enable VRRP timer debug flag:

```
DGS-3620-28SC:admin# debug vrrp timers state enable
Command: debug vrrp timers state enable

Success.

DGS-3620-28SC:admin#
```

## 20-31 debug vrrp clear counter

### Description

This command is used to reset the VRRP debug statistic counters.

### Format

**debug vrrp clear counter**

### Parameters

None.

### Restrictions

Only Administrator level users can issue this command.

### Example

To clear VRRP statistic counters:

```
DGS-3620-28SC:admin# debug vrrp clear counter
Command: debug vrrp clear counter

Success

DGS-3620-28SC:admin#
```

## 20-32 debug vrrp log state

### Description

This command is used to enable or disable the VRRP debug log state.

### Format

**debug vrrp log state [enable | disable]**

### Parameters

**state** - Specifies the state of the VRRP log. The default setting is disabled.
  **enable** - Specifies that the VRRP log state will be enabled.
  **disable** - Specifies that the VRRP log state will be disabled.

### Restrictions

Only Administrator level users can issue this command.

### Example

To enable the VRRP debug log state:

```
DGS-3620-28SC:admin# debug vrrp log state enable
Command: debug vrrp log state enable

Success.

DGS-3620-28SC:admin#
```

## 20-33 debug vrrp show counter

### Description

This command is used to display the VRRP debug statistic counters.

### Format

**debug vrrp show counter**

### Parameters

None.

### Restrictions

Only Administrator level users can issue this command.

### Example

To display VRRP statistic counters:

```
DGS-3620-28SC:admin# debug vrrp show counter
Command: debug vrrp show counter

VRRP debug statistic counters
  Received ADV : 9
  Drop         : 52
  Auth fail    : 0
  Sent ADV     : 0

DGS-3620-28SC:admin#
```

## 20-34 debug vrrp show flag

### Description

This command is used to display VRRP debug flag settings.

### Format

**debug vrrp show flag**

### Parameters

None.

### Restrictions

Only Administrator level users can issue this command.

### Example

To display VRRP debug flag settings:

```
DGS-3620-28SC:admin#debug vrrp show flag
Command: debug vrrp show flag

Global State: Disabled

Current VRRP debug level setting:

 virtual router state change
 packet receiving
 packet sending
 mac address update
 interface change
 timer

DGS-3620-28SC:admin#
```

## 20-35 debug vrrp show log state

### Description

The command is used to display the VRRP debug log state.

### Format

**debug vrrp show log state**

### Parameters

None.

### Restrictions

Only Administrator level users can issue this command.

### Example

To display the VRRP debug log state:

```
DGS-3620-28SC:admin# debug vrrp show log state
Command: debug vrrp show log state

VRRP Debug Log State: Disabled

DGS-3620-28SC:admin#
```

## 20-36 debug vrrp state

### Description

The command is used to enable or disable the VRRP debug state.

### Format

**debug vrrp state [enable | disable]**

### Parameters

**state** - Specifies the state of the VRRP debug state. The default setting is disabled.
  **enable** - Specifies that the VRRP debug state will be enabled.
  **disable** - Specifies that the VRRP debug state will be disabled.

### Restrictions

Only Administrator level users can issue this command.

### Example

To enable the VRRP debug state:

```
DGS-3620-28SC:admin# debug vrrp state enable
Command: debug vrrp state enable

Success.

DGS-3620-28SC:admin#
```

## 20-37 debug bgp show flag

### Description

This command is used for displaying current BGP debugging flags' setting.

### Format

**debug bgp show flag**

### Parameters

None.

### Restrictions

Only Administrator-level users can issue this command. (EI Mode Only Command)

### Example

Show BGP debug flag:

```
DGS-3620-28SC:admin# debug bgp show flag
Command: debug bgp show flag

Current BGP flags setting:

  Peer FSM Event                  Disable
  OPEN Packet Receive             Disable
  OPEN Packet Send                Disable
  UPDATE Packet Receive           Disable
  UPDATE Packet Send              Disable
  KEEPALIVE Packet Receive        Disable
  KEEPALIVE Packet Send           Disable
  NOTIFY Packet Receive           Disable
  NOTIFY Packet Send              Disable
  REFRESH Packet Receive          Disable
  REFRESH Packet Send             Disable
  CAPABILITY Packet Receive       Disable
  CAPABILITY Packet Send          Disable
  Filter Info                     Disable
  Route MAP                       Disable
  Access List                     Disable
  Prefix List                     Disable
  ERROR Information               Disable
  Zebros Debug Info               Disable
  Other Normal Information.       Disable

DGS-3620-28SC:admin#
```

## 20-38 debug bgp all flag

### Description

This command is used for setting all BGP debugging flags to disable or enable.

### Format

**debug bgp all flag [enable | disable]**

### Parameters

**enable** - Enable the BGP debug function.
**disable** - Disable the BGP debug function.

### Restrictions

Only Administrator-level users can issue this command. (EI Mode Only Command)

### Example

Configure all BGP debug flags’ state to enable:

```
DGS-3620-28SC:admin#  debug bgp all flag enable
Command: debug bgp all flag enable

Success.

DGS-3620-28SC:admin#
```

## 20-39 debug bgp fsm_event

### Description

This command is used for setting the flag of debugging information about peer FSM Event.

### Format

**debug bgp fsm_event [enable | disable]**

### Parameters

**enable** - Enable the BGP debug function.
**disable** - Disable the BGP debug function.

### Restrictions

Only Administrator-level users can issue this command. (EI Mode Only Command)

### Example

Configure BGP peer FSM event debug flag to enable:

```
DGS-3620-28SC:admin# debug bgp fsm_event enable
Command: debug bgp fsm_event enable

Success.

DGS-3620-28SC:admin#
```

Output Examples: After BGP peer FSM event debug flag to enable, it may print following information.

```
BGP: 10.1.1.1-10.2.2.2, [FSM] State Change: Idle -> Connect.
BGP: 10.1.1.1-10.2.2.2, [FSM] Hold-Timer Expiry.
BGP: 10.1.1.1-10.2.2.2, [FSM] State: Open, Event: 3.
```

## 20-40 debug bgp packet

### Description

This command is used for setting the flag of debugging information about different type of BGP packets' receiving and sending.

### Format

**debug bgp packet [{open | update | keepalive | notify | refresh | capability}(1) | all] [in | out] [enable | disable]**

### Parameters

**packet** - Specifies the packet type for the debug information to display.

**open** - (Optional) Specifies that 'open' information will be displayed.
**update** - (Optional) Specifies that 'update' information will be displayed.
**keepalive** - (Optional) Specifies that 'keepalive' information will be displayed.
**notify** - (Optional) Specifies that 'notify' information will be displayed.
**refresh** - (Optional) Specifies that 'refresh' information will be displayed.
**capability** - (Optional) Specifies that 'capability' information will be displayed.
**all** - (Optional) Specifies that all information will be displayed.

**in** - Specifies that the incoming information will be displayed.
**out** - Specifies that the outgoing information will be displayed.

**enable** - Enable the BGP debug function.
**disable** - Disable the BGP debug function.

### Restrictions

Only Administrator-level users can issue this command. (EI Mode Only Command)

### Example

Configure BGP to display debugging information after received update packet:

```
DGS-3620-28SC:admin# debug bgp packet all in enable
Command: debug bgp packet all in enable

Success.

DGS-3620-28SC:admin#
```

Output Examples: After BGP peer FSM event debug flag to enable, it may print following information.

```
BGP:Peer:<10.1.1.10> RCV OPEN, version:<4>,remote-as:<40>,
HoldTime:<180>,RID:<16.0.0.1>
BGP:Peer:<10.1.1.10> RCV KEEPALIVE.
BGP:Peer:<10.1.1.10> RCV UPDATE, withdraw:
<21.0.0.0/8>,<22.0.0.0/8>,<23.0.0.0/8>, <24.0.0.0/8>,<25.0.0.0/8>...
BGP:Peer:<10.1.1.10> RCV UPDATE,attr:<Orign:i,As-path:10,Next-
hop:10.1.1.10,Med:5>, NLRI: <21.0.0.0/8>,<22.0.0.0/8>
BGP:Peer:<10.1.1.10> RCV NOTIFYCATION,Code:<OPEN Message Error.>,SubCode:<Bad
Peer AS.>
BGP:Peer:<10.1.1.10> RCV REFRESH,afi:<1>,safi:<1>
BGP:Peer:<10.1.1.10> RCV Capability Action:Set,Code: GRST ,Length:2
```

## 20-41 debug bgp error state

### Description

This command is use for setting the flag of debugging information about BGP Error not need send BGP NOTIFICATION.

### Format

**debug bgp error state [enable | disable]**

### Parameters

| | |
|---|---|
| **enable** - Enable the BGP debug function.<br>**disable** - Disable the BGP debug function. | |

### Restrictions

Only Administrator-level users can issue this command. (EI Mode Only Command)

### Example

Configure BGP to enable error debug flag:

```
DGS-3620-28SC:admin# debug bgp error enable
Command: debug bgp error enable

Success.

DGS-3620-28SC:admin#
```

Output Examples: After configure BGP to enable error debug flag, it may print following information when error happens.

```
BGP: 10.1.1.1-10.2.2.2, NHop Validate: Invalid NHop address 250.3.0.0/8
received.
BGP: Hold-Timer: Invalid Peer.
```

## 20-42 debug bgp show global_info

### Description

This command is used for displaying global information of current BGP instance.

### Format

**debug bgp show global_info**

### Parameters

None.

### Restrictions

Only Administrator-level users can issue this command. (EI Mode Only Command)

### Example

Configure BGP to show global information:

```
DGS-3620-28SC:admin# debug bgp show global_info
Command: debug bgp show global_info

As Number: 1
Router ID                :10.2.2.2
Cluster ID               : 30.1.1.1
Confed ID                : 10
Confederation Peers      : 65510 65511
Fast External Fallover   : Disabled
Graceful Restart         : Disabled
Restart Time             : 120 Seconds
Stalepath Time           : 360 Seconds
Update Delay Time        : 120 Seconds
Dampening Ability        : Enable
Client to Client Ability : Enable
Cluster peers are:
1.1.1.2 group1
Default Local PREF       : 100
Default HoldTime         : 180
Default Keepalive        : 60
Scan Time                : 60

BGP active flag:

BGP active af-flag is:
BGP_AF_CFLAG_NETWORK_SYNC
note: address family is IPv4 Unicast

BGP active Redist-Flags:
note: The address family is IPv4
```

```
BGP Trap                           : None

DGS-3620-28SC:admin#
```

## 20-43 debug bgp show peer

### Description

This command is used for displaying information of all peers in BGP protocol DB.

### Format

**debug bgp show peer**

### Parameters

None.

### Restrictions

Only Administrator-level users can issue this command. (EI Mode Only Command)

### Example

Configure BGP to show all peers' information:

```
DGS-3620-28SC:admin# debug bgp show peer
Command: debug bgp show peer

BGP neighbor: 10.10.10.2 (Internal Peer)
-----------------------------------------------
Session State: Enabled
Session Activity: Enabled
Peer Group: NULL
Remote AS: 1
Local AS:10
Remote Router ID:192.168.252.252
BGP State: Established ( UP for 00:24:25)
Hold Time (Configured): 180 Seconds
Hold Time(Current Used): 180 Seconds
Keepalive Interval (Configured): 60 Seconds
Keepalive Interval(Current Used): 60 Seconds
Advertisement Interval(Configured): 5 Seconds
Advertisement Interval(Current Used): 5 Seconds
AS Origination Interval (Configured) : 0 Seconds
AS Origination Interval (Current Used) : 15 Seconds
Connect Retry Interval (Configured) : 0 Seconds
Connect Retry Interval (Current Used) : 120 Seconds
EBGP Multihop : 2
Weight: 100
Next Hop Self: Disabled
```

```
Remove Private AS: Disabled
Allowas In: Disabled
Graceful Restart  : Disabled
Address Family IPv4 Unicast
IPv4 Unicast: None
Soft Reconfiguration Inbound: Enabled
Community Sent to this Neighbor: None
Default Originate: Enabled
Incoming Update Prefix List: prelist1
Incoming Update Filter List: ASlist1
Route Map for Outgoing Routes: routemap1
Unsuppress Route Map: us_routmp1
Outbound Route Filter (ORF) type (64) Prefix list:
        Send Mode : Disabled
        Receive Mode : Disabled
Pass Word: NULL
Prefix count: 0
Send Prefix count: 0
Prefix max count: 12000
Prefix warning threshold: 75
Prefix max warning: Disabled

DGS-3620-28SC:admin#
```

## 20-44 debug bgp show peer_group

### Description

This command is used for displaying current peer group’s configuration in BGP protocol stack.

### Format

**debug bgp show peer_group**

### Parameters

None.

### Restrictions

Only Administrator-level users can issue this command. (EI Mode Only Command)

### Example

Configure BGP to show peer group’s configuration:

```
DGS-3620-28SC:admin# :5#debug bgp show peer_group
Command: debug bgp show peer_group

BGP Peer Group :tt
-------------------------------------------------------
Session State : Enabled
Session Activity : Enabled
Members : None
Remote AS : Not Set
Holdtime Interval : 180 seconds
Keepalive Interval : 60 seconds
Advertisement Interval : 0 seconds
AS Origination Interval : 0 Seconds
Connect Retry Interval : 0 Seconds
EBGP Multihop : 1
Weight : 0
Next Hop Self : Disabled
Remove Private As : Disabled
Allowas In : Disabled
Graceful Restart : Disabled
Soft Reconfiguration Inbound : Disabled
Community Sent to this Neighbor : None
Default Originate : Disabled
Capability Orf Prefix List : None
Pass Word: NULL
Prefix max count: 12000
Prefix warning threshold: 75
Prefix max warning: Disabled

DGS-3620-28SC:admin#
```

## 20-45 debug bgp show network

### Description

This command is used for displaying current network’s configuration in BGP protocol stack.

### Format

**debug bgp show network**

### Parameters

None.

### Restrictions

Only Administrator-level users can issue this command. (EI Mode Only Command)

### Example

Configure BGP to show network information:

```
DGS-3620-28SC:admin# debug bgp show network
Command: debug bgp show network

Network             Route Map
-------------      -----------
192.168.0.0/8      NULL
172.16.0.0/16      map1

Total Entries :2

DGS-3620-28SC:admin#
```

## 20-46 debug bgp show aggregate

### Description

This command is used for displaying current aggregate’s configuration in BGP protocol stack.

### Format

**debug bgp show aggregate**

### Parameters

None.

### Restrictions

Only Administrator-level users can issue this command. (EI Mode Only Command)

### Example

Configure BGP to show aggregate information:

```
DGS-3620-28SC:admin# debug bgp show aggregate
Command: debug bgp show aggregate

Network          Summary Only   AS Set    Suppress Count
-------------   ------------   ------   -------------
192.168.0.0/8   YES              NO        0
172.16.0.0/16    NO              NO        2

Total Entries :2

DGS-3620-28SC:admin#
```

## 20-47 debug bgp show damp

### Description

This command is used for displaying current dampening configuration and corresponding dynamic information in BGP protocol stack.

### Format

**debug bgp show damp**

### Parameters

None.

### Restrictions

Only Administrator-level users can issue this command. (EI Mode Only Command)

### Example

Configure BGP to show current dampening information:

```
DGS-3620-28SC:admin# debug bgp show damp
Command: debug bgp show damp

Route Map                          : NULL
Reach Half Life Time is            : 900 seconds
Reuse Value                        : 750
Suppress Value                     : 2000
MAX Suppress Time                  : 3600 seconds
Unreach Half Life Time is          : 900 seconds
Reuse Index Size                   : 1024
Reuse List Size                    : 256
Reuse Offset                       : 19

Current dampened routes:

 Damp Reuse List Info:
reuse_index index  ptr penalty    flap   start_time  t_updated
suppress_time evt

show BGP Damp  no reuse list info: 0
index ptr penalty flap  start_time  t_updated  suppress_time evt

BGP Damp Decay List Info:
decay array size is 90.

Index  Value
-----  -----
1      1
2      0.969663
3      0.940247
4      0.911722
5      0.884064
6      0.857244
7      0.831238
8      0.806021
9      0.781569
10     0.757858

Output truncated...

DGS-3620-28SC:admin#
```

## 20-48 debug bgp show interface_info

### Description

This command is used for displaying current interface information in BGP protocol stack.

### Format

**debug bgp show interface_info**

### Parameters

None.

### Restrictions

Only Administrator-level users can issue this command. (EI Mode Only Command)

### Example

Configure BGP to show current interface information:

```
DGS-3620-28SC:admin# debug bgp show interface_info
Command: debug bgp show interface_info

Interface Information:

Name    Index   Network             Flags   Status
----     ----   ------------       -----   ------
System   0001  30.30.30.30/8       0        Up

DGS-3620-28SC:admin#
```

## 20-49 debug bgp show as_path_access_list

### Description

This command is used for displaying current BGP as path access list configuration in BGP protocol stack.

### Format

**debug bgp show as_path_access_list**

### Parameters

None.

### Restrictions

Only Administrator-level users can issue this command. (EI Mode Only Command)

### Example

Configure BGP to show current BGP as_path access_list information:

```
DGS-3620-28SC:admin# debug bgp show as_path_access_list
Command: debug bgp show as_path_access_list

BGP AS Path Access List 1
deny (_64[6-9][0-9][0-9]_|_65[0-9][0-9][0-9]_)
permit 33

Total entry: 1

DGS-3620-28SC:admin#
```

## 20-50 debug bgp show bgp_timer

### Description

This command is used for displaying current BGP timer chain information in BGP protocol stack.

### Format

**debug bgp show bgp_timer**

### Parameters

None.

### Restrictions

Only Administrator-level users can issue this command. (EI Mode Only Command)

### Example

Configure BGP to show current BGP timer chain information.

```
DGS-3620-28SC:admin# debug bgp show bgp_timer
Command: debug bgp show bgp_timer

BGP timer Link:
Node       Time        Func
----       ----        ------
08B108D0    0001     00675AF4
08B1AC70    0016     0065F4F4
08B1ACA8    0017     0065F5CC
08B37DCC    0029     0065F4F4
08B37E04    0030     0065F5CC
032821BC    0035     00662840
08B1AC54    0135     0065F40C
08B37DB0    0148     0065F40C

DGS-3620-28SC:admin#
```

## 20-51 debug bgp show community_list

### Description

This command is used for displaying current community list configuration in protocol stack.

### Format

**debug bgp show community_list**

### Parameters

None.

### Restrictions

Only Administrator-level users can issue this command. (EI Mode Only Command)

### Example

Configure BGP to show current community list information:

```
DGS-3620-28SC:admin# debug bgp show community_list
Command: debug bgp show community_list

Community list:1  standard
    permit   50000:100

Total Entry: 1

DGS-3620-28SC:admin#
```

## 20-52 debug bgp show redist_info

### Description

This command is used for displaying current BGP redistribution information.

### Format

**debug bgp show redist_info**

### Parameters

None.

### Restrictions

Only Administrator-level users can issue this command. (EI Mode Only Command)

### Example

Configure BGP to show current BGP redistribution information:

```
DGS-3620-28SC:admin# debug bgp show redist_info
Command: debug bgp show redist_info

Last redistribution count summary:
Type    Route_count_rib  total_count      Time(msec)
------  ---------------- --------------- ---------
OSPF      0                 0            0
RIP       0                 0            0
STATIC    0                 0            0
LOCAL     7                 0            0

Redistributed routes summary:
Network              Type      Next_hop
-------              ----     -------------
1.10.0.1/32         LOCAL     0.0.0.0
1.10.0.2/32         LOCAL     0.0.0.0
1.10.0.3/32         LOCAL     0.0.0.0

DGS-3620-28SC:admin#
```

## 20-53 debug bgp router_map

### Description

This command is used for setting route_map debugging flags to disable or enable. If this flag is enable, route-map permit or deny in BGP module will be displayed.

### Format

**debug bgp router_map [enable | disable]**

### Parameters

**enable** - Enable the route_map debug function.
**disable** - Disable the route_map debug function.

### Restrictions

Only Administrator-level users can issue this command. (EI Mode Only Command)

### Example

Configure routemap debug flags' state to enable:

```
DGS-3620-28SC:admin#  debug bgp router_map enable
Command: debug bgp router_map enable

Success.

DGS-3620-28SC:admin#  config bgp neighbor map 15.0.0.1 route_map in add map1
Command: config bgp neighbor map 15.0.0.1 route_map in add map1

Success.

DGS-3620-28SC:admin#
```

Output Examples: After configure BGP to enable route map debug flag, it may print following information when route map applied.

```
route_map:<map1>,apply bgp neighbor:<13.0.0.1> MATCH.
route_map:<map1>,apply bgp static route:<32.0.0.0/8> Not MATCH.
```

## 20-54 debug bgp access_list

### Description

This command is used for setting access_list debugging flags to disable or enable. If this flag is enable, access list permit or deny in BGP module will be displayed

### Format

**debug bgp access_list [enable | disable]**

### Parameters

**enable** - Enable the access_list debug function.
**disable** - Disable the access_list debug function.

### Restrictions

Only Administrator-level users can issue this command. (EI Mode Only Command)

### Example

Configure access list debug flags' state to enable:

```
DGS-3620-28SC:admin#  debug bgp access_list enable
Command: debug bgp access_list enable

Success.

DGS-3620-28SC:admin#
```

Output Examples: After configure BGP to enable access list debug flag, it may print following information when access list applied.

```
access_list:<acl>,apply bgp neighbor:<19.0.0.1> MATCH.
```

## 20-55 debug bgp prefix_list

### Description

This command is used for setting prefix_list debugging flags to disable or enable. If this flag is enable, prefix list permit or deny in BGP module will be displayed.

### Format

**debug bgp prefix_list [enable | disable]**

### Parameters

**enable** - Enable the prefix_list debug function.
**disable** - Disable the prefix_list debug function.

### Restrictions

Only Administrator-level users can issue this command. (EI Mode Only Command)

### Example

Configure prefix list debug flags' state to enable:

```
DGS-3620-28SC:admin#  debug bgp prefix_list enable
Command: debug bgp prefix_list enable

Success.

DGS-3620-28SC:admin#
```

Output Examples: After configure BGP to enable prefix list debug flag, it may print following information when prefix list applied.

```
Prefix_list:<list1>,apply bgp neighbor:<15.0.0.1> MATCH.
```

## 20-56 debug dhcpv6_client state enable

### Description

This command is used to enable the DHCPv6 client Debug function.

### Format

**debug dhcpv6_client state enable**

### Parameters

None.

### Restrictions

Only Administrator-level users can issue this command.

### Example

To enabled DHCPv6 client debug function:

```
DGS-3620-28SC:admin# debug dhcpv6_client state enable
Command:   debug dhcpv6_client state enable

Success.

DGS-3620-28SC:admin#
```

## 20-57 debug dhcpv6_client state disable

### Description

This command is used to disable the DHCPv6 client Debug function.

### Format

**debug dhcpv6_client state enable**

### Parameters

None.

### Restrictions

Only Administrator-level users can issue this command.

### Example

To disabled DHCPv6 client debug function:

```
DGS-3620-28SC:admin# debug dhcpv6_client state disable
Command:   debug dhcpv6_client state disable

Success.

DGS-3620-28SC:admin#
```

## 20-58 debug dhcpv6_client output

### Description

Used to set debug message to output to buffer or console.

### Format

**debug dhcpv6_client output [buffer | console]**

### Parameters

**buffer** - Let the debug message output to buffer.

**console** - Let the debug message output to console.

### Restrictions

Only Administrator-level users can issue this command.

### Example

To set debug information to output to console:

```
DGS-3620-28SC:admin# debug dhcpv6_client output console
Command: debug dhcpv6_client output console

Success.

DGS-3620-28SC:admin#
```

## 20-59 debug dhcpv6_client packet

### Description

Used to enable or disable debug information flag for DHCPv6 client packet, including packet receiving and sending.

### Format

**debug dhcpv6_client packet {all | receiving | sending} state [enable | disable]**

### Parameters

**all** - (Optional) Set packet receiving and sending debug flags.
**receiving** - (Optional) Set packet receiving debug flag.
**sending** - (Optional) Set packet sending debug flag.

**state** - Specifies that the designated flags will be enabled or disabled.
  **enable** - Enable the designated flags.
  **disable** - Disable the designated flags.

### Restrictions

Only Administrator-level users can issue this command.

### Example

To enable dhcpv6_client packet sending debug:

```
DGS-3620-28SC:admin# debug dhcpv6_client packet sending state enable
Command: debug dhcpv6_client packet sending state enable

Success.

DGS-3620-28SC:admin#
```

## 20-60 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 Administrator-level users can issue this command.

### Example

To enabled DHCPv6 relay debug function:

```
DGS-3620-28SC:admin#  debug dhcpv6_relay state enable
Command:   debug dhcpv6_relay state enable

Success.

DGS-3620-28SC:admin#
```

## 20-61 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 Administrator-level users can issue this command.

### Example

To disabled DHCPv6 relay debug function:

```
DGS-3620-28SC:admin#  debug dhcpv6_relay state disable
Command:   debug dhcpv6_relay state disable

Success.

DGS-3620-28SC:admin#
```

## 20-62 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

**state** - Specifies the hop count debugging state.
**enable** - Specifies that the hop count state will be enabled.
**disable** - Specifies that the hop count state will be disabled.

### Restrictions

Only Administrator-level users can issue this command.

### Example

To enable debug information flag about the hop count:

```
DGS-3620-28SC:admin# debug dhcpv6_relay hop_count state enable
Command: debug dhcpv6_relay hop_count state enable

Success.

DGS-3620-28SC:admin#
```

## 20-63 debug dhcpv6_relay output

### Description

Used to set debug message to output to buffer or console.

### Format

**debug dhcpv6_relay output [buffer | console]**

### Parameters

**output** - Specifies the location of the debug message output.
  **buffer** - Let the debug message output to buffer.
  **console** - Let the debug message output to console.

### Restrictions

Only Administrator-level users can issue this command.

### Example

To set debug information to output to console:

```
DGS-3620-28SC:admin#  debug dhcpv6_relay output console
Command: debug dhcpv6_relay output console

Success.

DGS-3620-28SC:admin#
```

## 20-64 debug dhcpv6_relay packet

### Description

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** - (Optional) Set packet receiving and sending debug flags.
**receiving** - (Optional) Set packet receiving debug flag.
**sending** - (Optional) Set packet sending debug flag.

**state** - Specifies if the designated flags function will be enabled or disabled.
  **enable** - Enable the designated flags.
  **disable** - Disable the designated flags.

### Restrictions

Only Administrator-level users can issue this command.

### Example

To enabled DHCPv6 relay packet sending debug:

```
DGS-3620-28SC:admin#  debug dhcpv6_relay packet sending state enable
Command: debug dhcpv6_relay packet sending state enable

Success.

DGS-3620-28SC:admin#
```

## 20-65 debug dhcpv6_server packet

### Description

This command is used to enable or disable the debug information flag of the DHCPv6 server packet, including packets receiving and sending.

### Format

**debug dhcpv6_server packet [all | receiving | sending] state [enable | disable]**

### Parameters

| |
|---|
| **all** - Set packet receiving and sending debug flags.<br>**receiving** - Set packet receiving debug flag.<br>**sending** - Set packet sending debug flag. |
| **state** - Specifies the state of the designated flags.<br>**enable** - Enable the designated flags.<br>**disable** - Disable the designated flags. |

### Restrictions

Only Administrator-level users can issue this command.

### Example

To enabled the DHCPv6 server packet sending debug:

```
DGS-3620-28SC:admin# debug dhcpv6_server packet sending state enable
Command: debug dhcpv6_server packet sending state enable

Success.

DGS-3620-28SC:admin#
```

## 20-66 debug dhcpv6_server state disable

### Description

This command is used to disable the DHCPv6 server debug functions.

### Format

**debug dhcpv6_server state disable**

### Parameters

None.

### Restrictions

Only Administrator-level users can issue this command.

### Example

To disabled the DHCPv6 server debug function:

```
DGS-3620-28SC:admin# debug dhcpv6_server state disable
Command: debug dhcpv6_server state disable

Success.

DGS-3620-28SC:admin#
```

## 20-67 debug dhcpv6_server state enable

### Description

This command is used to enable the DHCPv6 server debug functions.

### Format

**debug dhcpv6_server state enable**

### Parameters

None.

### Restrictions

Only Administrator-level users can issue this command.

### Example

To enabled the DHCPv6 server debug function:

```
DGS-3620-28SC:admin# debug dhcpv6_server state enable
Command: debug dhcpv6_server state enable

Success.

DGS-3620-28SC:admin#
```

## 20-68 debug pim ssm

### Description

This command is used to enable the PIM-SSM debug function.

### Format

**debug pim ssm**

### Parameters

None.

### Restrictions

Only Administrator-level users can issue this command.

### Example

To enable the PIM-SSM debug function:

```
DGS-3620-28SC:admin# debug pim ssm
Command: debug pim ssm

Success.

DGS-3620-28SC:admin#
```

Once the PIM-SSM debug enabled, the debug information maybe outputted.

```
DGS-3620-28SC:admin# Group Record mode 2 for SSM group 232.1.1.1 from
192.168.2.14, ignored

Output truncated...
```

## 20-69 no debug pim ssm

### Description

This command is used to disable the PIM-SSM debug function.

### Format

**no debug pim ssm**

### Parameters

None.

### Restrictions

Only Administrator-level users can issue this command.

### Example

To disable the PIM-SSM debug function:

```
DGS-3620-28SC:admin# no debug pim ssm
Command: no debug pim ssm

Success.

DGS-3620-28SC:admin#
```

## 20-70 debug ripng flag

### Description

This command is used to enable or disable the RIPng debug flag.

### Format

**debug ripng flag [{interface | packet [all | rx | tx] | route} | all] state [enable | disable]**

### Parameters

**interface** - (Optional) Specifies the state of the RIPng interface debug. The default setting is disabled.

**packet** - (Optional) Specifies which packets should be set with debug flags.
- **all** - Specifies to set all packets with debug flags.
- **rx** - Specifies to set inbound packets with debug flag.
- **tx** - Specifies to set outbound packets with debug flag.

**route** - (Optional) Specifies the state of the RIPng route debug. The default setting is disabled.

**all** - Specifies to set all debug flags.

**state** - Specifies the designated flags state.
- **enable** - Specifies that the designated flags state will be enabled.
- **disable** - Specifies that the designated flags state will be disabled.

### Restrictions

Only Administrator-level users can issue this command. (EI Mode Only Command)

### Example

To enable the RIPng debug:

```
DGS-3620-28SC:admin# debug ripng state enable
Command: debug ripng state enable

Success.

DGS-3620-28SC:admin#
```

After enabling RIPng on an interface, the following information may appear when the interface state changes.

```
The RIPng interface System has changed the link state to down.
```

## 20-71 debug ripng show flag

### Description

This command is used to display the RIPng debug flag setting.

### Format

**debug ripng show flag**

### Parameters

None.

### Restrictions

Only Administrator-level users can issue this command. (EI Mode Only Command)

### Example

To show the current RIPng debug flag setting:

```
DGS-3620-28SC:admin# debug ripng show flag
Command: debug ripng show flag

Current Enabled RIPng Flags:
Interface State Change
Packet Receiving
Packet Sending
Route

DGS-3620-28SC:admin#
```

## 20-72 debug ripng state disable

### Description

This command is used to disable the RIPng debug state.

### Format

**debug ripng state disable**

### Parameters

None.

### Restrictions

Only Administrator-level users can issue this command. (EI Mode Only Command)

### Example

To disable RIPng debug globally:

```
DGS-3620-28SC:admin# debug ripng state disable
Command: debug ripng state disable

Success.

DGS-3620-28SC:admin#
```

## 20-73 debug ripng state enable

### Description

This command is used to enable the RIPng debug state.

### Format

**debug ripng state enable**

### Parameters

None.

### Restrictions

Only Administrator-level users can issue this command. (EI Mode Only Command)

### Example

To enable RIPng debug globally:

```
DGS-3620-28SC:admin# debug ripng state enable
Command: debug ripng state enable

Success.

DGS-3620-28SC:admin#
```

## 20-74 debug routefilter show

### Description

This command is used to display route filter information in kernel, including prefix list, access list, and route map.

### Format

**debug routefilter show [prefix_list | access_list | route_map]**

### Parameters

**prefix_list** - Specifies to display prefix list debug information.
**access_list** - Specifies to display access list debug information.
**route_map** - Specifies to display route map debug information.

### Restrictions

Only Administrator-level users can issue this command.

### Example

To display route filter information in kernel:

```
DGS-3620-28SC:admin# debug routefilter show route_map
Command: debug routefilter show route_map

   route_map :   map1
--------------------------
      sequence : 10   (Permit)
            Match clauses:
                   prefix_list :  pr_list1
            Set clauses:
                   metric :  80

Success.

DGS-3620-28SC:admin#
```

## 20-75 debug show status

### Description

Show the debug handler state and the specified module’s debug status.

If the input module list is empty, the states of all registered modules which support debug module will be shown.

### Format

**debug show status {module <module_list>}**

### Parameters

**module** – (Optional) Specifies the module list.
**<module_list>** - Enter the module list here.

### Restrictions

Only Administrator-level users can issue this command.

### Example

To show the specified module’s debug state:

```
Prompt# debug show status module MSTP
Command: debug show status module MSTP

Debug Global State  : Enable

MSTP                : Enable

Prompt#
```

To show the debug state:

```
Prompt# debug show status
Command: debug show status

Debug Global State: Enable

MSTP                : Disabled
IMPB                : Disabled
DHCPv6_CLIENT       : Disabled
DHCPv6_RELAY        : Disabled
OSPFV2              : Disabled
VRRP                : Disabled
RIPNG               : Disabled
ERPS                : Disabled
DHCPv6_SERVER       : Disabled

Prompt#
```

## 20-76 debug super_vlan state

### Description

This command is used to enable or disable the super VLAN Debug Function.

### Format

**debug super_vlan state [enable | disable]**

### Parameters

**state** - Specifies the super VLAN debug function state.

- **enable** - Specifies that the super VLAN debug function will be enabled.
- **disable** - Specifies that the super VLAN debug function will be disabled.

### Restrictions

Only Administrator-level users can issue this command.

## Example

To disable the super VLAN Debug Function:

```
DGS-3620-28SC:admin# debug super_vlan state disable
Command: debug super_vlan state disable

Success.

DGS-3620-28SC:admin#
```

After enabling super VLAN debug, the following information may appear when receive an ARP packet form sub VLAN.

```
The ARP request packet received from sub vlan 200.
```

# Chapter 21 DHCP Local Relay Commands

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

**config dhcp_local_relay vlan vlanid** <vlan_id> state [enable | disable]

**enable dhcp_local_relay**

**disable dhcp_local_relay**

**show dhcp_local_relay**

## 21-1 config dhcp_local_relay vlan

### Description

This command is used to enable or disable the DHCP local relay function for a specified VLAN. By default, the switch will not broadcast DHCP packets on any VLAN for which a DHCP relay is configured. DHCP packets will be intercepted, and only be relayed to the servers specified in the dhcp_relay command. This is done to minimise the risk with rogue DHCP servers. Enabling the dhcp_local_relay feature will restore the broadcast behaviour, and cause DHCP packets to also be broadcast on the specified VLAN.

**Note:** When “dhcp_local_relay” is enabled, the switch will automatically add DHCP option 82, and the source MAC and gateway in the packet will remain unchanged.

### Format

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

### Parameters

**<vlan_name 32>** - Specify the name of the VLAN to be enabled for DHCP local relay.

**state** - Enable or disable DHCP local relay for a specified VLAN.
- **enable** - Enable DHCP local relay for a specified VLAN.
- **disable** - Disable DHCP local relay for a specified VLAN.

### Restrictions

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

### Example

To enable DHCP local relay for the default VLAN:

```
DGS-3620-28SC:admin#config dhcp_local_relay vlan default state enable
Command: config dhcp_local_relay vlan default state enable

Success.

DGS-3620-28SC:admin#
```

## 21-2 config dhcp_local_relay vlan vlanid

### Description

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

### Format

**config dhcp_local_relay vlan vlanid <vlan_id> state [enable | disable]**

### Parameters

| | |
|---|---|
| **vlanid** - Specifies the VLAN ID used to enabled DHCP local relay.<br>**<vlan_id>** - Enter the VLAN ID used here. | |
| **state** - Enable or disable DHCP local relay for a specified VLAN.<br>**enable** - Enable DHCP local relay for a specified VLAN.<br>**disable** - Disable DHCP local relay for a specified VLAN. | |

### Restrictions

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

### Example

To enable DHCP local relay for the default VLAN:

```
DGS-3620-28SC:admin#config dhcp_local_relay vlan vlanid 1 state enable
Command: config dhcp_local_relay vlan vlanid 1 state enable

Success.

DGS-3620-28SC:admin#
```

## 21-3 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 Administrator, Operator and Power-User level users can issue this command.

### Example

To enable the DHCP local relay function:

```
DGS-3620-28SC:admin#enable dhcp_local_relay
Command: enable dhcp_local_relay

Success.

DGS-3620-28SC:admin#
```

## 21-4 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 Administrator, Operator and Power-User level users can issue this command.

### Example

To disable the DHCP local relay function:

```
DGS-3620-28SC:admin#disable dhcp_local_relay
Command: disable dhcp_local_relay

Success.

DGS-3620-28SC:admin#
```

## 21-5 show dhcp_local_relay

### Description

This command is used to display the current DHCP local relay configuration on the switch.

### Format

**show dhcp_local_relay**

### Parameters

None.

## Restrictions

None.

## Example

To display the local DHCP relay status:

```
DGS-3620-28SC:admin#show dhcp_local_relay
Command: show dhcp_local_relay

DHCP/BOOTP Local Relay Status      : Disabled
DHCP/BOOTP Local Relay VID List    : 1,3-4

DGS-3620-28SC:admin#
```

# Chapter 22 DHCP Relay Commands

| |
|---|
| **config dhcp_relay** {hops <int 1-16> \| time <sec 0-65535>}(1) |
| **config dhcp_relay add ipif** <ipif_name 12> <ipaddr> |
| **config dhcp_relay delete ipif** <ipif_name 12> <ipaddr> |
| **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>}] |
| **config dhcp_relay option_60 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] |
| **config dhcp_relay option_61 state** [enable \| disable] |
| **config dhcp_relay option_82 check** [enable \| disable] |
| **config dhcp_relay option_82 policy** [replace \| drop \| keep] |
| **config dhcp_relay option_82 remote_id** [default **\|** user_define <desc 32>] |
| **config dhcp_relay option_82 state** [enable \| disable] |
| **enable dhcp_relay** |
| **disable dhcp_relay** |
| **show dhcp_relay** {ipif <ipif_name 12>} |
| **show dhcp_relay option_60** {[string <multiword 255> **\|** ipaddress <ipaddr> **\|** default]} |
| **show dhcp_relay option_61** |

**Note:** The DHCP relay commands include all the commands defined in the BOOTP relay command section. If this DHCP relay command set is supported in your system, the BOOTP relay commands can be ignored.

**Note:** The system supporting DHCP relay will accept BOOTP relay commands in the **config file** but not allow input from the console screen, and these BOOTP relay commands setting from the config file will be saved as DHCP relay commands while the **save** command is performed.

## 22-1 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 router hops that the DHCP/BOOTP packets can cross. The range is 1 to 16. The default value is 4.
**<int 1-16>** - Specify the maximum number of router hops that the DHCP/BOOTP packets can cross. The maximum number of hops value must be between 1 and 16.

**time** - Specify the minimum time in seconds within which the switch must relay the DHCP/BOOTP request. If this time is larger than the DHCP packet's time, the switch will drop the DHCP/BOOTP packet. The range is 0 to 65535. The default value is 0.
**<sec 0-65535>** - Specify the minimum time in seconds within which the switch must relay the DHCP/BOOTP request. The minimum time value must be between 0 and 65535 seconds.

### Restrictions

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

### Example

To configure the DHCP relay:

```
DGS-3620-28SC:admin#config dhcp_relay hops 4 time 2
Command: config dhcp_relay hops 4 time 2

Success.

DGS-3620-28SC:admin#
```

## 22-2 config dhcp_relay add ipif

### Description

This command is used to add an IP destination address to the switch's DHCP relay table.

**Note:** Adding a server to which DHCP packets will be relayed, will cause the switch to intercept DHCP packets on the specified VLAN, and relay them directly to the specified server. DHCP packets will not be broadcast on the VLAN. To restore broadcast functionality, see the "dhcp_local_relay" command

### Format

**config dhcp_relay add ipif <ipif_name 12> <ipaddr>**

### Parameters

**<ipif_name 12> -** Specify the name of the IP interface which contains the IP address below.

**<ipaddr>** - Specify the DHCP/BOOTP server IP address.

### Restrictions

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

### Example

To add an IP destination address to the switch's DHCP relay table:

```
DGS-3620-28SC:admin#config dhcp_relay add ipif System 10.43.21.12
Command: config dhcp_relay add ipif System 10.43.21.12

Success.

DGS-3620-28SC:admin#
```

## 22-3 config dhcp_relay delete ipif

### Description

This command is used to delete an IP destination address from the switch's DHCP relay table.

### Format

**config dhcp_relay delete ipif <ipif_name 12> <ipaddr>**

### Parameters

| |
|---|
| **<ipif_name 12>** - Specify the name of the IP interface which contains the IP address below. |
| **<ipaddr>** - Specify the DHCP/BOOTP server IP address. |

### Restrictions

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

### Example

To delete an IP destination address from the switch's DHCP relay table:

```
DGS-3620-28SC:admin#config dhcp_relay delete ipif System 10.43.21.12
Command: config dhcp_relay delete ipif System 10.43.21.12

Success.

DGS-3620-28SC:admin#
```

## 22-4 config dhcp_relay option_60 add string

### Description

This command is used to configure the Option 60 relay rules. Note that different strings 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>** - Specify a string.

**relay** - Specify a relay server IP address.
  **<ipaddr>** - Enter the IP address here.

**exact-match** - The Option 60 string in the packet must fully match the specified string.
**partial-match** - The Option 60 string in the packet only need partially match the specified string.

### Restrictions

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

### Example

To configure DHCP Option 60 to decide to relay which DHCP server:

```
DGS-3620-28SC: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-3620-28SC:admin#
```

## 22-5 config dhcp_relay option_60 default

### Description

This command is used to configure DHCP relay Option 60 default relay servers. When there are no match servers found for the packet based on Option 60, the relay servers will be determined by the default relay server setting. When drop is specified, the packet with no matching rules found will be dropped without further processing. 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 a relay server IP for the packet that has matching Option 60 rules.
  **<ipaddr>** - Enter the server IP address here.

**mode** - Specify the mode to relay or drop packets.
  **relay** - The packet will be relayed based on the relay rules.
  **drop** - Specify to drop the packet that has no matching Option 60 rules.

### Restrictions

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

### Example

To configure a DHCP Option 60 default drop action:

```
DGS-3620-28SC:admin#config dhcp_relay option_60 default mode drop
Command: config dhcp_relay option_60 default mode drop

Success.

DGS-3620-28SC:admin#
```

## 22-6 config dhcp_relay option_60 delete

### Description

This command is used to delete a DHCP Option 60 entry. When all is specified, all rules excluding the default rules are deleted.

### Format

**config dhcp_relay option_60 delete [string <multiword 255> {relay <ipaddr>} | ipaddress <ipaddr> | all | default {<ipaddr>}]**

### Parameters

**string** - Delete all the entries whose string is equal to the string specified if the IP address is not specified.
**<multiword 255>** - The string value can be up to 255 characters long.

**relay** - (Optional) Delete one entry, whose string and IP address are equal to the string and IP address specified by the user.
**<ipaddr>** - Enter the IP address here.

**ipaddress** - Delete all the entries whose IP address are equal to the specified IP address.
**<ipaddr>** - Enter the IP address here.

**all** - Specify to have all rules, excluding the default rules, deleted.

**default** - Delete the default relay IP address that is specified by the user.
**<ipaddr>** - (Optional) Enter the IP address here.

### Restrictions

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

### Example

To delete a DHCP Option 60 entry:

```
DGS-3620-28SC: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-3620-28SC:admin#
```

## 22-7 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.

### Format

**config dhcp_relay option_60 state [enable | disable]**

### Parameters

**enable** - Specify to enable the DHCP relay function to use option 60 rules to relay DHCP packets.

**disable** - Specify to disable the DHCP relay function from using option 60 rules to relay DHCP packets.

### Restrictions

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

### Example

To configure the DHCP Option 60 state:

```
DGS-3620-28SC:admin#config dhcp_relay option_60 state enable
Command: config dhcp_relay option_60 state enable

Success.

DGS-3620-28SC:admin#
```

## 22-8 config dhcp_relay option_61 add

### Description

This command adds a rule to determine the relay server based on Option 61. The match rule can be based on either MAC address or a user-specified string. Only one relay server can be specified for a MAC address or a string. If relay servers are determined based on Option 60, and one relay server is determined based on Option 61, the final relay servers will be the union of these two sets of the servers.

### Format

**config dhcp_relay option_61 add [mac_address <macaddr> | string <desc_long 255>] [relay <ipaddr> | drop]**

### Parameters

**mac_address** - Specify the client's client-ID, which is the hardware address of the client.

**<macaddr>** - Specify the client's client-ID, which is the MAC address of the client.

**string** - Specify the client's client-ID, which is specified by administrator.
**<desc_long 255>** - Specify the client's client-ID, which is specified by administrator The client-ID string can be up to 255 characters long.

**relay** - Specify to relay the packet to an IP address.
**<ipaddr>** - Specify to relay the packet to an IP address by entering the IP address here.

**drop** - Specify to drop the packet.

### Restrictions

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

### Example

To configure DHCP Option 61 to decide how to process DHCP packets:

```
DGS-3620-28SC: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-3620-28SC:admin#
```

## 22-9 config dhcp_relay option_61 default

### Description

This command is used to determine the rule to process those packets that have no Option 61 matching rules. The default default-rule is drop.

### 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 here.

**drop** - Specify to drop the packet that have no Option 61 matching rules.

### Restrictions

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

### Example

To configure the DHCP Option 61 default action to drop:

```
DGS-3620-28SC:admin#config dhcp_relay option_61 default drop
Command: config dhcp_relay option_61 default drop

Success.

DGS-3620-28SC:admin#
```

## 22-10 config dhcp_relay option_61 delete

### Description

This command is used to delete Option 61 rules.

### 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<br>**<macaddr>** - Enter the MAC address here. |
| **string** - The entry with the specified string will be deleted.<br>**<desc_long 255>** - The string value can be up to 255 characters long. |
| **all** - All rules excluding the default rule will be deleted. |

### Restrictions

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

### Example

To delete a DHCP Option 61 entry:

```
DGS-3620-28SC: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-3620-28SC:admin#
```

## 22-11 config dhcp_relay option_61 state

### Description

This command is used to decide whether 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 DHCP relay function to use option 61 rules to relay DHCP packets.

**disable** - Specify to disable the DHCP relay function to use option 61 rules to relay DHCP packets.

### Restrictions

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

### Example

To configure the state of DHCP relay Option 61:

```
DGS-3620-28SC:admin#config dhcp_relay option_61 state enable
Command: config dhcp_relay option_61 state enable

Success.

DGS-3620-28SC:admin#
```

## 22-12 config dhcp_relay option_82 check

### Description

This command is used to configure the checking mechanism of the DHCP relay agent information Option 82 of the switch.

### Format

**config dhcp_relay option_82 check [enable | disable]**

### Parameters

**enable** - When the state is enabled, for a packet coming from the client side, the packet should not have the Option 82 field. If the packet has this option field, it will be dropped.

**disable** - The default setting is disabled.

### Restrictions

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

### Example

To configure the checking mechanism of the DHCP relay agent information Option 82:

```
DGS-3620-28SC:admin#config dhcp_relay option_82 check disable
Command: config dhcp_relay option_82 check disable
```

```
Success.

DGS-3620-28SC:admin#
```

## 22-13 config dhcp_relay option_82 policy

### Description

This option takes effect only when the check status is disabled. The relay agent does this operation because the packet cannot contain two Option 82s. The default setting is replace.

### Format

**config dhcp_relay option_82 policy [replace | drop | keep]**

### Parameters

**replace** - Replace the existing option 82 field in the packet.

**drop** - Specifies to discard if the packet has the Option 82 field. If the packet, that comes from the client side, contains an Option 82 value, then the packet will be dropped. If the packet, that comes from the client side doesn’t contain an Option 82 value, then insert it's own Option 82 value into the packet.

**keep** - Specifies to retain the existing Option 82 field in the packet. The default setting is replace. If the packet, that comes from the client side, and 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.

### Restrictions

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

### Example

To configure the policy of DHCP relay agent information Option 82:

```
DGS-3620-28SC:admin#config dhcp_relay option_82 policy replace
Command: config dhcp_relay option_82 policy replace

Success

DGS-3620-28SC:admin#
```

## 22-14 config dhcp_relay option_82 remote_id

### Description

This command is used to configure the remote ID string of the DHCP relay agent information Option 82 of the Switch.

### Format

**config dhcp_relay option_82 remote_id [default | user_define <desc 32>]**

### Parameters

**default** - Use the switch's system MAC address as remote ID.

**user_define** - Use the user-defined string as remote ID. Space characters are allowed in the string.
**<desc 32>** - The user-defined string can be up to 32 characters long.

### Restrictions

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

### Example

To configure the remote ID string of the DHCP relay agent information Option 82:

```
DGS-3620-28SC:admin#config dhcp_relay option_82 remote_id user_define D-Link
Switch
Command: config dhcp_relay option_82 remote_id user_define D-Link Switch

Success.

DGS-3620-28SC:admin#
```

## 22-15 config dhcp_relay option_82 state

### Description

This command is used to configure the state of the DHCP relay agent information Option 82 of the switch. The default settings is disabled.

### Format

**config dhcp_relay option_82 state [enable | disable]**

### Parameters

**enable** - When the state is enabled, the DHCP packet will be inserted with the Option 82 field before being relayed to server. The DHCP packet will be processed based on the behavior defined in the check and policy setting.

**disable** - When the state is disabled, the DHCP packet will be relayed directly to the server without further check and processing of the packet.

### Restrictions

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

### Example

To configure the state of the DHCP relay agent information Option 82:

```
DGS-3620-28SC:admin#config dhcp_relay option_82 state enable
Command: config dhcp_relay option_82 state enable

```

```
Success.

DGS-3620-28SC:admin#
```

## 22-16 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 Administrator, Operator and Power-User level users can issue this command.

### Example

To enable the DHCP relay function:

```
DGS-3620-28SC:admin#enable dhcp_relay
Command: enable dhcp_relay

Success.

DGS-3620-28SC:admin#
```

## 22-17 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 Administrator, Operator and Power-User level users can issue this command.

### Example

To disable the DHCP relay function:

```
DGS-3620-28SC:admin#disable dhcp_relay
Command: disable dhcp_relay

Success.

DGS-3620-28SC:admin#
```

## 22-18 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>** - Specify the IP interface name. The IP interface name can be up to 12 characters long.

**Note:** If no parameter is specified, the system will display all DHCP relay configurations.

### Restrictions

None.

### Example

To display the DHCP relay status:

```
DGS-3620-28SC:admin#show dhcp_relay
Command: show dhcp_relay

DHCP/BOOTP Relay Status         : Disabled
DHCP/BOOTP Hops Count Limit     : 4
DHCP/BOOTP Relay Time Threshold : 0
DHCP Vendor Class Identifier Option 60 State: Disabled
DHCP Client Identifier Option 61 State: Disabled
DHCP Relay Agent Information Option 82 State  : Disabled
DHCP Relay Agent Information Option 82 Check  : Disabled
DHCP Relay Agent Information Option 82 Policy : Replace
DHCP Relay Agent Information Option 82 Remote ID : D-Link Switch

Interface     Server 1        Server 2         Server 3       Server 4
------------- --------------- ---------------- --------------- --------------
```

```
System         10.1.1.1        192.168.0.1

DGS-3620-28SC:admin#
```

## 22-19 show dhcp_relay option_60

### Description

This command is used to display the DHCP relay option 60 entries.

### Format

**show dhcp_relay option_60 {[string <multiword 255> | ipaddress <ipaddr> | default]}**

### Parameters

| |
|---|
| **string** - (Optional) Display the entry whose string equals the string specified.<br>**<multiword 255>** - The string can be up to 255 characters long. |
| **ipaddress** - (Optional) Display the entry whose IP ipaddress equals the specified IP address.<br>**<ipaddr>** - Enter the IP address here. |
| **default** - (Optional) Display the default behaviour of DHCP relay option 60. |

**Note:** If no parameter is specified, all DHCP option 60 entries will be displayed.

### Restrictions

None.

### Example

To display the DHCP option 60 entries:

```
DGS-3620-28SC:admin#show dhcp_relay option_60
Command: show dhcp_relay option_60

Default Processing Mode: Drop

Default Servers:
   10.90.90.100
   10.90.90.101
   10.90.90.102

Matching Rules:

String                        Match Type               IP Address
-------                       ---------                ---------
abc                           Exact Match              10.90.90.1
abcde                         Partial Match            10.90.90.2
abcdefg                       Exact Match              10.90.90.3

Total Entries: 3
```

```

DGS-3620-28SC:admin#
```

## 22-20 show dhcp_relay option_61

### Description

This command is used to display all the DHCP relay option 61 rules.

### Format

**show dhcp_relay option_61**

### Parameters

None.

### Restrictions

None.

### Example

To display the DHCP option 61 entries:

```
DGS-3620-28SC:admin#show dhcp_relay option_61
Command: show dhcp_relay option_61

Default Relay Rule:Drop

Matching Rules:

Client-ID                         Type               Relay Rule
-----------                       ----               ---------
abc                               String             Drop
abcde                             String             10.90.90.1
00-11-22-33-44-55                 MAC Address        Drop

Total Entries: 3

DGS-3620-28SC:admin#
```

# Chapter 23 DHCP Server Commands

**create dhcp excluded_address** begin_address <ipaddr> end_address <ipaddr>

**delete dhcp excluded_address** [begin_address <ipaddr> end_address <ipaddr> | all]

**show dhcp excluded_address**

**create dhcp pool** <pool_name 12>

**delete dhcp pool** [<pool_name 12> | all]

**config dhcp pool network_addr** <pool_name 12> <network_address>

**config dhcp pool domain_name** <pool_name 12> {<domain_name 64>}

**config dhcp pool dns_server** <pool_name 12> {<ipaddr>} {<ipaddr>} {<ipaddr>}

**config dhcp pool netbios_name_server** <pool_name 12> {<ipaddr>} {<ipaddr>} {<ipaddr>}

**config dhcp pool netbios_node_type** <pool_name 12> [broadcast | peer_to_peer | mixed | hybrid]

**config dhcp pool default_router** <pool_name 12> {<ipaddr>} {<ipaddr>} {<ipaddr>}

**config dhcp pool lease** <pool_name 12> [<day 0-365> <hour 0-23> <minute 0-59> | infinite]

**config dhcp pool boot_file** <pool_name 12> {<file_name 64>}

**config dhcp pool next_server** <pool_name 12> {<ipaddr>}

**config dhcp ping_packets** <number 0-10>

**config dhcp ping_timeout** <millisecond 10-2000>

**create dhcp pool manual_binding** <pool_name 12> <ipaddr> hardware_address <macaddr> {type [ethernet | ieee802]}

**delete dhcp pool manual_binding** <pool_name 12> [<ipaddr> | all]

**clear dhcp binding** [<pool_name 12> [<ipaddr> | all] | all]

**show dhcp binding** {<pool_name 12>}

**show dhcp pool** {<pool_name 12>}

**show dhcp pool manual_binding** {<pool_name 12>}

**enable dhcp_server**

**disable dhcp_server**

**show dhcp_server**

**clear dhcp conflict_ip** [<ipaddr> | all]

**show dhcp conflict_ip** {<ipaddr>}

## 23-1 create dhcp excluded_address

### Description

This command is used to create a DHCP server exclude address. The DHCP server assumes that all IP addresses in a DHCP pool subnet are available for assigning to DHCP clients. Use this command to specify the IP address that the DHCP server should not assign to clients. This command can be used multiple times in order to define multiple groups of excluded addresses.

### Format

**create dhcp excluded_address begin_address <ipaddr> end_address <ipaddr>**

### Parameters

**begin_address** - Specify the starting address of the IP address range.
**<ipaddr> -** Specify the starting address of the IP address range.

**end_address** - Specify the ending address of the IP address range.
**<ipaddr>** - Specify the ending address of the IP address range.

### Restrictions

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

### Example

To specify the IP address that DHCP server should not assign to clients:

```
DGS-3620-28SC:admin#create dhcp excluded_address begin_address 10.10.10.1
end_address 10.10.10.10
Command: create dhcp excluded_address begin_address 10.10.10.1 end_address
10.10.10.10

Success.

DGS-3620-28SC:admin#
```

## 23-2 delete dhcp excluded_address

### Description

This command is used to delete a DHCP server exclude address.

### Format

**delete dhcp excluded_address [begin_address <ipaddr> end_address <ipaddr> | all]**

### Parameters

**begin_address** - Specify the starting address of the IP address range.
**<ipaddr>** - Specify the starting address of the IP address range.

**end_address** - Specify the ending address of the IP address range.
**<ipaddr>** - Specify the ending address of the IP address range.

**all** - Specify to delete all IP addresses.

### Restrictions

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

### Example

To delete a DHCP server exclude address:

```
DGS-3620-28SC:admin#delete dhcp excluded_address begin_address 10.10.10.1
end_address 10.10.10.10
Command: delete dhcp excluded_address begin_address 10.10.10.1 end_address
10.10.10.10

Success.
```

```
DGS-3620-28SC:admin#
```

## 23-3 show dhcp excluded_address

### Description

This command is used to display the groups of IP addresses which are excluded from being a legal assigned IP address.

### Format

**show dhcp excluded_address**

### Parameters

None.

### Restrictions

None.

### Example

To display the DHCP server excluded addresses:

```
DGS-3620-28SC:admin#show dhcp excluded_address
Command: show dhcp excluded_address

Index  Begin Address  End Address
-----  -------------  --------------
1      192.168.0.1    192.168.0.100
2      10.10.10.10    10.10.10.11

Total Entries : 2

DGS-3620-28SC:admin#
```

## 23-4 create dhcp pool

### Description

This command is used to create a DHCP pool by specifying a name. After creating a DHCP pool, use other DHCP pool configuration commands to configure parameters for the pool.

### Format

**create dhcp pool <pool_name 12>**

### Parameters

**<pool_name 12> -** Specify the name of the DHCP pool.

### Restrictions

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

### Example

To create a DHCP pool:

```
DGS-3620-28SC:admin#create dhcp pool nyknicks
Command: create dhcp pool nyknicks

Success.

DGS-3620-28SC:admin#
```

## 23-5 delete dhcp pool

### Description

This command is used to delete a DHCP pool.

### Format

**delete dhcp pool [<pool_name 12> | all]**

### Parameters

**<pool_name 12> -** Specify the name of the DHCP pool.

**all** - Specify to delete all the DHCP pools.

### Restrictions

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

### Example

To delete a DHCP pool:

```
DGS-3620-28SC:admin#delete dhcp pool nyknicks
Command: delete dhcp pool nyknicks

Success.

DGS-3620-28SC:admin#
```

## 23-6 config dhcp pool network_addr

### Description

This command is used to specify the network for the DHCP pool. The addresses in the network are free to be assigned to the DHCP client. The prefix length specifies the number of bits that comprise the address prefix. The prefix is an alternative way of specifying the network mask of the client. The prefix length must be preceded by a forward slash (/). When the DHCP server receives a request from the client, the server will automatically find a pool to allocate the address. If the request is relayed to the server by the intermediate device, the server will match the gateway IP address carried in the packet against the network of each DHCP pool. The pool which has the longest match will be selected. If the request packet is not through relay, then the server will match the IP address of the IPIF that received the request packet against the network of each DHCP pool.

### Format

**config dhcp pool network_addr <pool_name 12> <network_address>**

### Parameters

| |
|---|
| **<pool_name 12>** - Specify the DHCP pool name. |
| **<network_address>** - Specify the IP address that the DHCP server may assign to clients. |

### Restrictions

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

### Example

To configure the address range of the DHCP address pool:

```
DGS-3620-28SC:admin#config dhcp pool network_addr nyknicks 10.10.10.0/24
Command: config dhcp pool network_addr nyknicks 10.10.10.0/24

Success.

DGS-3620-28SC:admin#
```

## 23-7 config dhcp pool domain_name

### Description

This command is used to specify the domain name for the client if the server allocates the address for the client from this pool. The domain name configured here will be used as the default domain name by the client. By default, the domain name is empty. If the domain name is empty, the domain name information will not be provided to the client.

### Format

**config dhcp pool domain_name <pool_name 12> {<domain_name 64>}**

### Parameters

**<pool_name 12>** - Specify the DHCP pool name.

**<domain_name 64>** - (Optional) Specify the domain name of the client.

### Restrictions

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

### Example

To configure the domain name option of the DHCP pool:

```
DGS-3620-28SC:admin#config dhcp pool domain_name nyknicks nba.com
Command: config dhcp pool domain_name nyknicks nba.com

Success.

DGS-3620-28SC:admin#
```

## 23-8 config dhcp pool dns_server

### Description

This command is used to specify the IP address of a DNS server that is available to a DHCP client. Up to three IP addresses can be specified on one command line. If DNS server is not specified, the DNS server information will not be provided to the client. If this command is input twice for the same pool, the second command will overwrite the first command.

### Format

**config dhcp pool dns_server <pool_name 12> {<ipaddr>} {<ipaddr>} {<ipaddr>}**

### Parameters

**<pool_name 12>** - Specify the DHCP poll name.

**<ipaddr>** - (Optional) Specify the IP address of the DNS server. Up to three IP addresses can be specified on one command line.

### Restrictions

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

### Example

To configure the DNS server’s IP address:

```
DGS-3620-28SC:admin#config dhcp pool dns_server nyknicks 10.10.10.1
Command: config dhcp pool dns_server nyknicks 10.10.10.1

Success.

DGS-3620-28SC:admin#
```

## 23-9 config dhcp pool netbios_name_server

### Description

This command is used to specify the NetBIOS WINS server that is available to a Microsoft DHCP client. Up to three IP addresses can be specified on one command line.

Windows Internet Naming Service (WINS) is a name resolution service that Microsoft DHCP clients use to correlate host names to IP addresses within a general grouping of networks. If a NetBIOS name server is not specified, the NetBIOS name server information will not be provided to the client. If this command is input twice for the same pool, the second command will overwrite the first command.

### Format

**config dhcp pool netbios_name_server <pool_name 12> {<ipaddr>} {<ipaddr>} {<ipaddr>}**

### Parameters

| |
|---|
| **<pool_name 12>** - Specify the DHCP pool name. |
| **<ipaddr>** - (Optional) Specify the IP address of the WINS server. Up to three IP addresses can be specified on one command line. |

### Restrictions

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

### Example

To configure a WINS server IP address:

```
DGS-3620-28SC:admin#config dhcp pool netbios_name_server knicks 10.10.10.1
Command: config dhcp pool netbios_name_server knicks 10.10.10.1

Success.

DGS-3620-28SC:admin#
```

## 23-10 config dhcp pool netbios_node_type

### Description

This command is used to specify the NetBIOS node type for a Microsoft DHCP client.

The NetBIOS node type for Microsoft DHCP clients can be one of four settings: broadcast, peer-to-peer, mixed, or hybrid. Use this command to configure a NetBIOS over TCP/IP device that is described in RFC 1001/1002. By default, the NetBIOS node type is broadcast.

### Format

**config dhcp pool netbios_node_type <pool_name 12> [broadcast | peer_to_peer | mixed | hybrid]**

### Parameters

**<pool_name 12> -** Specify the DHCP pool name.

**broadcast** - Specify the NetBIOS node type for Microsoft DHCP clients as broadcast.

**peer_to_peer** - Specify the NetBIOS node type for Microsoft DHCP clients as peer_to_peer.

**mixed** - Specify the NetBIOS node type for Microsoft DHCP clients as mixed.

**hybrid -** Specify the NetBIOS node type for Microsoft DHCP clients as hybrid.

### Restrictions

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

### Example

To configure the NetBIOS node type:

```
DGS-3620-28SC:admin#config dhcp pool netbios_node_type knicks hybrid
Command: config dhcp pool netbios_node_type knicks hybrid

Success.

DGS-3620-28SC:admin#
```

## 23-11 config dhcp pool default_router

### Description

This command is used to specify the IP address of the default router for a DHCP client. Up to three IP addresses can be specified on one command line.

After a DHCP client has booted, the client begins sending packets to its default router. The IP address of the default router should be on the same subnet as the client. If the default router is not specified, the default router information will not be provided to the client. If this command is input twice for the same pool, the second command will overwrite the first command. The default router must be within the range the network defined for the DHCP pool.

### Format

**config dhcp pool default_router <pool_name 12> {<ipaddr>} {<ipaddr>} {<ipaddr>}**

### Parameters

**<pool_name 12>** - Specify the DHCP pool name.

**<ipaddr>** - (Optional) Specify the IP address of the default router. Up to three IP addresses can be specified on one command line.

### Restrictions

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

### Example

To configure the default router:

```
DGS-3620-28SC:admin#config dhcp pool default_router nyknicks 10.10.10.1
Command: config dhcp pool default_router nyknicks 10.10.10.1

Success.

DGS-3620-28SC:admin#
```

## 23-12 config dhcp pool lease

### Description

This command is used to specify the duration of the DHCP pool lease.

By default, each IP address assigned by a DHCP server comes with a one-day lease, which is the amount of time that the address is valid.

### Format

**config dhcp pool lease <pool_name 12> [<day 0-365> <hour 0-23> <minute 0-59> | infinite]**

### Parameters

| |
|---|
| **<pool_name 12>** - Specify the DHCP pool's name. |
| **<day 0-365>** - Specify the number of days of the lease. |
| **<hour 0-23>** - Specify the number of hours of the lease. |
| **<minute 0-59>** - Specify the number of minutes of the lease. |
| **infinite** - Specify a lease of unlimited duration. |

### Restrictions

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

### Example

To configure the lease of a pool:

```
DGS-3620-28SC:admin#config dhcp pool lease nyknicks infinite
Command: config dhcp pool lease nyknicks infinite

Success.

DGS-3620-28SC:admin#
```

## 23-13 config dhcp pool boot_file

### Description

This command is used to specify the name of the file that is used as a boot image.

The boot file is used to store the boot image for the client. The boot image is generally the operating system the client uses to load. If this command is input twice for the same pool, the second command will overwrite the first command. If the bootfile is not specified, the boot file information will not be provided to the client.

### Format

**config dhcp pool boot_file <pool_name 12> {<file_name 64>}**

### Parameters

**<pool_name 12>** - Specify the DHCP pool name.

**<file_name 64>** - (Optional) Specify the file name of the boot image.

### Restrictions

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

### Example

To configure the boot file:

```
DGS-3620-28SC:admin#config dhcp pool boot_file engineering boot.had
Command: config dhcp pool boot_file engineering boot.had

Success.

DGS-3620-28SC:admin#
```

## 23-14 config dhcp pool next_server

### Description

This command is used by the DHCP client boot process, typically a TFTP server. If next server information is not specified, it will not be provided to the client. If this command is input twice for the same pool, the second command will overwrite the first command.

### Format

**config dhcp pool next_server <pool_name 12> {<ipaddr>}**

### Parameters

**<pool_name 12>** - Specify the DHCP pool name.

**<ipaddr>** - (Optional) Specify the IP address of the next server.

### Restrictions

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

### Example

To configure the next server:

```
DGS-3620-28SC:admin#config dhcp pool next_server engineering 192.168.0.1
Command: config dhcp pool next_server engineering 192.168.0.1

Success.

DGS-3620-28SC:admin#
```

## 23-15 config dhcp ping_packets

### Description

This command is used to specify the number of ping packets the DHCP server sends to an IP address before assigning this address to a requesting client.

By default, the DHCP server pings a pool address twice before assigning the address to a DHCP client. If the ping is unanswered, the DHCP server assumes (with a high probability) that the address is not in use and assigns the address to the requesting client. If the ping is answered, the server will discard the current IP address and try another IP address.

### Format

**config dhcp ping_packets <number 0-10>**

### Parameters

**<number 0-10>** - Specify the number of ping packets. 0 means there is no ping test. The default value is 2.

### Restrictions

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

### Example

To configure ping packets:

```
DGS-3620-28SC:admin#config dhcp ping_packets 4
Command: config dhcp ping_packets 4

Success.

DGS-3620-28SC:admin#
```

## 23-16 config dhcp ping_timeout

### Description

This command is used to specify the amount of time the DHCP server must wait before timing out a ping packet.

By default, the DHCP server waits 100 milliseconds before timing out a ping packet.

### Format

**config dhcp ping_timeout <millisecond 10-2000>**

### Parameters

**<millisecond 10-2000>** - Specify the amount of time the DHCP server must wait before timing out a ping packet. The default value is 100.

### Restrictions

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

### Example

To configure the time out value for ping packets:

```
DGS-3620-28SC:admin#config dhcp ping_timeout 500
Command: config dhcp ping_timeout 500

Success.

DGS-3620-28SC:admin#
```

## 23-17 create dhcp pool manual_binding

### Description

This command is used to specify the distinct identification of the client in dotted-hexadecimal notation or hardware address.

An address binding is a mapping between the IP address and MAC address of a client. The IP address of a client can be assigned manually by an administrator or assigned automatically from a pool by a DHCP server.

The IP address specified in the manual binding entry must be in a range within that the network uses for the DHCP pool. If the user specifies a conflict IP address, an error message will be returned. If a number of manual binding entries are created, and the network address for the pool is changed such that conflicts are generated, those manual binding entries which conflict with the new network address will be automatically deleted.

### Format

**create dhcp pool manual_binding <pool_name 12> <ipaddr> hardware_address <macaddr> {type [ethernet | ieee802]}**

### Parameters

**<pool_name 12>** - Specify the DHCP pool name.

**<ipaddr>** - Specify the IP address which will be assigned to a specified client.

**hardware_address** - Specify the hardware MAC address.
  **<macaddr>** - Enter the MAC address here.

**type** - (Optional) Specify the DHCP pool manual binding type.
  **ethernet** - Specify Ethernet type.

**ieee802** -Specify IEEE802 type.

### Restrictions

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

### Example

To configure manual bindings:

```
DGS-3620-28SC:admin#create dhcp pool manual_binding engineering 10.10.10.1
hardware_address 00-80-C8-02-02-02 type ethernet
Command: create dhcp pool manual_binding engineering 10.10.10.1
hardware_address 00-80-C8-02-02-02 type ethernet


Success.


DGS-3620-28SC:admin#
```

## 23-18 delete dhcp pool manual_binding

### Description

This command is used to delete DHCP server manual binding.

### Format

**delete dhcp pool manual_binding <pool_name 12> [<ipaddr> | all]**

### Parameters

**<pool_name 12>** - Specify the DHCP pool name.

**<ipaddr>** - Specify the IP address which will be assigned to a specified client.
**all** - Specify to delete all IP addresses.

### Restrictions

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

### Example

To delete DHCP server manual binding:

```
DGS-3620-28SC:admin#delete dhcp pool manual_binding engineering 10.10.10.1
Command: delete dhcp pool manual_binding engineering 10.10.10.1


Success.


DGS-3620-28SC:admin#
```

## 23-19 clear dhcp binding

### Description

This command is used to clear a binding entry or all binding entries in a pool or clears all binding entries in all pools. Note that this command will not clear the dynamic binding entry which matches a manual binding entry.

### Format

**clear dhcp binding [<pool_name 12> [<ipaddr> | all] | all]**

### Parameters

**<pool_name 12>** - Specify the DHCP pool name to clear.
  **<ipaddr>** - Specify the IP address to clear.
  **all** - Specify to clear all IP addresses for the specified pool.

**all** - Specify to clear all binding entries in all pools

### Restrictions

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

### Example

To clear dynamic binding entries in the pool named “engineering”:

```
DGS-3620-28SC:admin#clear dhcp binding engineering 10.20.3.4
Command: clear dhcp binding engineering 10.20.3.4

Success.

DGS-3620-28SC:admin#
```

## 23-20 show dhcp binding

### Description

This command is used to display dynamic binding entries.

### Format

**show dhcp binding {<pool_name 12>}**

### Parameters

**<pool_name 12>** - (Optional) Specify a DHCP pool name.

### Restrictions

None.

### Example

To display dynamic binding entries for “engineering”:

```
DGS-3620-28SC:admin#show dhcp binding engineering
Command: show dhcp binding engineering

Pool Name     IP Addresss    Hardware Address   Type      Status   Lifetime
------------  -------------- ------------------ --------  -------  ---------
engineering   192.168.0.1    00-80-C8-08-13-88  Ethernet  Manual    86400
engineering   192.168.0.2    00-80-C8-08-13-99  Ethernet  Automatic 86400
engineering   192.168.0.3    00-80-C8-08-13-A0  Ethernet  Automatic 86400
engineering   192.168.0.4    00-80-C8-08-13-B0  Ethernet  Automatic 86400

Total Entries: 4

DGS-3620-28SC:admin#
```

## 23-21 show dhcp pool

### Description

This command is used to display the information for DHCP pool. If pool name is not specified, information for all pools will be displayed.

### Format

**show dhcp pool {<pool_name 12>}**

### Parameters

**<pool_name 12>** - (Optional) Specify the DHCP pool name.

### Restrictions

None.

### Example

To display the current DHCP pool information for “engineering”:

```
DGS-3620-28SC:admin#show dhcp pool engineering
Command: show dhcp pool engineering

Pool Name         : engineering
Network Address   : 10.10.10.0/24
Domain Name       : dlink.com
DNS Server        : 10.10.10.1
NetBIOS Name Server : 10.10.10.1
NetBIOS Node Type : Broadcast
Default Router    : 10.10.10.1
Pool Lease        : 10 Days, 0 Hours, 0 Minutes
Boot File         : boot.bin
```

```
Next Server       : 10.10.10.2

DGS-3620-28SC:admin#
```

## 23-22 show dhcp pool manual_binding

### Description

This command is used to display the configured manual binding entries.

### Format

**show dhcp pool manual_binding {<pool_name 12>}**

### Parameters

**<pool_name 12>** - (Optional) Specify the DHCP pool name.

### Restrictions

None.

### Example

To display the configured manual binding entries:

```
DGS-3620-28SC:admin#show dhcp pool manual_binding
Command: show dhcp pool manual_binding

Pool Name    IP Address    Hardware Address   Type
------------ ------------- ------------------ --------
p1           192.168.0.1   00-80-C8-08-13-88  Ethernet
p1           192.168.0.2   00-80-C8-08-13-99  Ethernet

Total Entries : 2

DGS-3620-28SC:admin#
```

## 23-23 enable dhcp_server

### Description

This command is used to enable the DHCP server function.

If DHCP relay is enabled, DHCP server cannot be enabled. The opposite is also true. For Layer 2 switches, if DHCP client is enabled on the only interface, then DHCP server cannot be enabled. For layer 3 switches, when the System interface is the only interface then can DHCP client be enabled. If the DHCP client is enabled, then the DHCP server cannot be enabled.

### Format

**enable dhcp_server**

### Parameters

None.

### Restrictions

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

### Example

To enable DHCP server:

```
DGS-3620-28SC:admin#enable dhcp_server
Command: enable dhcp_server

Success.

DGS-3620-28SC:admin#
```

## 23-24 disable dhcp_server

### Description

This command is used to disable the DHCP server function on the switch.

### Format

**disable dhcp_server**

### Parameters

None.

### Restrictions

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

### Example

To disable the Switch’s DHCP server:

```
DGS-3620-28SC:admin#disable dhcp_server
Command: disable dhcp_server

Success.

DGS-3620-28SC:admin#
```

## 23-25 show dhcp_server

### Description

This command is used to display the current DHCP server configuration.

### Format

**show dhcp_server**

### Parameters

None.

### Restrictions

None.

### Example

To display the DHCP server status:

```
DGS-3620-28SC:admin#show dhcp_server
Command: show dhcp_server

  DHCP Server Global State: Disabled
  Ping Packet Number      : 2
  Ping Timeout            : 100 ms

DGS-3620-28SC:admin#
```

## 23-26 clear dhcp conflict_ip

### Description

This command is used to clear an entry or all entries from the conflict IP database.

### Format

**clear dhcp conflict_ip [<ipaddr> | all]**

### Parameters

| |
|---|
| **<ipaddr>** - Specify the IP address to be cleared. |
| **all** - Specify that all IP addresses will be cleared. |

### Restrictions

None.

### Example

To clear an IP address 10.20.3.4 from the conflict database:

```
DGS-3620-28SC:admin#clear dhcp conflict_ip 10.20.3.4
Command: clear dhcp conflict_ip 10.20.3.4

Success.

DGS-3620-28SC:admin#
```

## 23-27 show dhcp conflict_ip

### Description

This command is used to display the IP address that has been identified as being in conflict.

The DHCP server will use ping packet to determine whether an IP address is conflicting with other hosts before binding this IP. The IP address which has been identified in conflict will be moved to the conflict IP database. The system will not attempt to bind the IP address in the conflict IP database unless the user clears it from the conflict IP database.

### Format

**show dhcp conflict_ip {<ipaddr>}**

### Parameters

**<ipaddr>** - (Optional) Specify the IP address to be displayed.

### Restrictions

None.

### Example

To display the entries in the DHCP conflict IP database:

```
DGS-3620-28SC:admin#show dhcp conflict_ip
Command: show dhcp conflict_ip

 IP Address    Detection Method   Detection Time
-----------   ----------------   --------------------
172.16.1.32   Ping               2007/08/30 17:06:59
172.16.1.32   Gratuitous ARP     2007/09/10 19:38:01

DGS-3620-28SC:admin#
```

# Chapter 24 DHCPv6 Relay Command List

| |
|---|
| **enable dhcpv6_relay** |
| **disable dhcpv6_relay** |
| **config dhcpv6_relay hop_count** <value 1-32> |
| **config dhcpv6_relay** [add \| delete] ipif <ipif_name 12> <ipv6addr> |
| **config dhcpv6_relay ipif** [<ipif_name 12> **\|** all] state [enable **\|** disable] |
| **show dhcpv6_relay** {ipif <ipif_name 12>} |

## 24-1 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 Administrator, Operator and Power-User level users can issue this command.

### Example

To configure the DHCPv6 relay global state to enable:

```
DGS-3620-28SC:admin# enable dhcpv6_relay
Command: enable dhcpv6_relay

Success.

DGS-3620-28SC:admin#
```

## 24-2 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 Administrator, Operator and Power-User level users can issue this command.

### Example

To configure the DHCPv6 relay global state to disable:

```
DGS-3620-28SC:admin# disable dhcpv6_relay
Command: disable dhcpv6_relay

Success.

DGS-3620-28SC:admin#
```

## 24-3 config dhcpv6_relay hop_count

### Description

Configure the DHCPv6 relay hop_count of the switch.

### Format

**config dhcpv6_relay hop_count <value 1-32>**

### Parameters

**hop_count** - Specifies the number of relay agents that have relayed this message. The default value is 4.

**<value 1-32>** - Enter the hop count number here. This value must be between 1 and 32.

### Restrictions

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

### Example

To configure the maximum hops of a DHCPv6 relay packet could be transferred to 4:

```
DGS-3620-28SC:admin# config dhcpv6_relay hop_count 4
Command: config dhcpv6_relay hop_count 4

Success.

DGS-3620-28SC:admin#
```

## 24-4 config dhcpv6_relay

### Description

The command could 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.<br>**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.<br>**<ipif_name 12>** - Enter the IP interface name here. This name can be up to 12 characters long. |
| **<ipv6addr>** - The DHCPv6 server IP address. |

### Restrictions

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

### Example

To add a DHCPv6 server to the relay table:

```
DGS-3620-28SC: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-3620-28SC:admin#
```

## 24-5 config dhcpv6_relay ipif

### Description

The 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** - Specifies the name of the IP interface.<br>**<ipif_name 12>** - Enter the IP interface name used here. This name can be up to 12 characters long.<br>**all** - Specifies that all the configured IP interfaces wil be used.. |
| **state** - Specifies 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 Administrator, Operator and Power-User level users can issue this command.

### Example

To configure the DHCPv6 relay state of the System interface to enable:

```
DGS-3620-28SC:admin#  config dhcpv6_relay ipif System state enable
Command: config dhcpv6_relay ipif System state enable

Success.

DGS-3620-28SC:admin#
```

## 24-6 show dhcpv6_relay

### Description

This command will 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 show the DHCPv6 relay configuration of all interfaces:

```
DGS-3620-28SC:admin# show dhcpv6_relay
Command: show dhcpv6_relay

DHCPv6 Relay Global State : Disabled
DHCPv6 Hops Count Limit   : 4
---------------------------------------------------------------
IP Interface              : n81
DHCPv6 Relay Status       : Enabled
Server Address            :

IP Interface              : n90
DHCPv6 Relay Status       : Enabled
Server Address            :

IP Interface              : n1000
DHCPv6 Relay Status       : Enabled
Server Address            :

Total Entries : 3

DGS-3620-28SC:admin#
```

To show the DHCPv6 relay configuration of System interface:

```
DGS-3620-28SC:admin# show dhcpv6_relay ipif System
Command: show dhcpv6_relay ipif System

DHCPv6 Relay Global State : Disabled
DHCPv6 Hops Count Limit   : 4
---------------------------------------------------------------
IP Interface              : System
DHCPv6 Relay Status       : Enabled
Server Address            : 2001:DB8:1234::218:FEFF:FEFB:CC0E
Server Address            : 3000:90:1::6

DGS-3620-28SC:admin#
```

# Chapter 25 DHCPv6 Server Commands

| |
|---|
| **create dhcpv6 pool** <pool_name 12> |
| **delete dhcpv6 pool** [<pool_name 12> \| all] |
| **show dhcpv6 pool** {<pool_name 12>} |
| **config dhcpv6 pool ipv6network_addr** <pool_name 12> begin <ipv6networkaddr> end <ipv6networkaddr> |
| **config dhcpv6 pool domain_name** <pool_name 12> <domain_name 255> |
| **config dhcpv6 pool dns_server** <pool_name 12> <ipv6addr> {<ipv6addr>} |
| **config dhcpv6 pool lifetime** <pool_name 12> preferred_lifetime <sec 60-4294967295> valid_lifetime <sec 60-4294967295> |
| **config dhcpv6 pool manual_binding** <pool_name 12> [add <ipv6addr> client_duid <string 28> \| delete [<ipv6addr> \| all]] |
| **show dhcpv6 manual_binding** {<pool_name 12>} |
| **show dhcpv6 binding** {<pool_name 12>} |
| **clear dhcpv6 binding** {<pool_name 12>} |
| **enable dhcpv6_server** |
| **disable dhcpv6_server** |
| **show dhcpv6_server** {ipif <ipif_name 12>} |
| **config dhcpv6 pool excluded_address** <pool_name 12> [add begin <ipv6addr> end <ipv6addr> \| delete [begin <ipv6addr> end <ipv6addr> \| all]] |
| **show dhcpv6 excluded_address** {<pool_name 12>} |
| **config dhcpv6_server ipif** [<ipif_name 12> \| all] state [enable \| disable] |

## 25-1 create dhcpv6 pool

### Description

This command is used to create a DHCPv6 pool for the DHCPv6 server.

### Format

**create dhcpv6 pool <pool_name 12>**

### Parameters

**pool** - Specifies the pool to be created with this command.
**<pool_name 12>** - Enter the pool name here. This name can be up to 12 characters long.

### Restrictions

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

### Example

To create a DHCPv6 pool pool1:

```
DGS-3620-28SC:admin# create dhcpv6 pool pool1
Command : create dhcpv6 pool pool1

success

DGS-3620-28SC:admin#
```

## 25-2 delete dhcpv6 pool

### Description

This command is used to delete one or all DHCPv6 pools.

### Format

**delete dhcpv6 pool [<pool_name 12> | all]**

### Parameters

**pool** - Specifies the DHCPv6 pool to be removed.
**<pool_name 12>** - Enter the DHCPv6 pool name to be removed here. This name can be up to 12 characters long.
**all** - Specifies that all the DHCPv6 pools will be removed.

### Restrictions

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

### Example

To delete the DHCPv6 pool by specifying the pool name pool1:

```
DGS-3620-28SC:admin# delete dhcpv6 pool pool1
Command: delete dhcpv6 pool pool1

Success.

DGS-3620-28SC:admin#
```

## 25-3 show dhcpv6 pool

### Description

This command is used to display one or all DHCPv6 pools configuration.

### Format

**show dhcpv6 pool {<pool_name 12>}**

### Parameters

**pool** – Specifies the DHCPv6 pool to be displayed.

**<pool_name 12>** - (Optional) Enter the DHCPv6 pool name to be displayed here. This name can be up to 12 characters long.

If no parameters are specified, all the DHCPv6 pools will be displayed.

### Restrictions

None.

### Example

To show the DHCPv6 pool by specifying the pool name pool1:

```
DGS-3620-28SC:admin# show dhcpv6 pool pool1
Command: show dhcpv6 pool pool1

Pool Name               : pool1
Begin Network Address   : 2000::1/64
End Network Address     : 2000::200/64
Domain Name             : domain.com
DNS Server Address      : 2000::ff
                        : 2000::fe
Preferred Lifetime      : 604800 (sec)
Valid Lifetime          : 2592000 (sec)

Total Pool Entry: 1

DGS-3620-28SC:admin#
```

## 25-4 config dhcpv6 pool ipv6network_addr

### Description

This command is used to configure the range of IPv6 network addresses for the DHCPv6 pool. The IPv6 addresses in the range are free to be assigned to any DHCPv6 client. When the DHCPv6 server receives a request from the client, the server will automatically find an available pool to allocate an IPv6 address.

The begin_networkaddr and end_networkaddr must observer some rules as followed:

The prefix of the begin_networkaddr and end_networkaddr are not consistence, otherwise, the switch will print an error message: The prefix of begin_networkaddr and end_networkaddr must be consistence.(e.g.: the begin_networkaddr is 2000::1/64, and the end_networkaddr is 3000::100/64)

The begin address must not be large than end address, otherwise, the switch will print an error message: The begin IPv6 address must be lower than or equal to the end IPv6 address.(e.g.: the begin_networkaddr is 2000::200/64, and the end_networkaddr is 2000::100/64)

There must not be intersection between the IPv6 address ranges of two pools, otherwise, the Switch will print an error message: IPv6network address collision. (e.g.: pool1: 2000::1/64 --- 2000::100/64, pool2: 2000::50/64 --- 2000::200/64)

The IPv6 network address can’t be Link-local address and Multicast address, otherwise, the Switch will print an error message: “The IPv6 network address can’t be Link-local address or Multicast address. “ (e.g.:: pool1: FE80::1/64 --- FE80::100/64, pool2: FE80::200/64 --- FE80::300/64

### Format

**config dhcpv6 pool ipv6network_addr <pool_name 12> begin <ipv6networkaddr> end <ipv6networkaddr>**

### Parameters

**<pool_name 12>** - Enter the DHCPv6 pool name used here. This name can be up to 12 characters long.

**begin** - Specifies the beginning IPv6 network address of the DHCPv6 pool.
**<ipv6networkaddr>** - Enter the beginning IPv6 network address of the DHCPv6 pool here.

**end** - Specifies the ending IPv6 network address of the DHCPv6 pool.
**<ipv6networkaddr>** - Enter the ending IPv6 network address of the DHCPv6 pool here.

### Restrictions

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

### Example

To configure the range of ipv6network address for the DHCPv6 pool pool1:

```
DGS-3620-28SC:admin# config dhcpv6 pool ipv6network_addr pool1 begin 2000::1/64
end 2000::32/64
Command: config dhcpv6 pool ipv6network_addr pool1 begin 2000::1/64 end
2000::32/64


success


DGS-3620-28SC:admin#
```

## 25-5 config dhcpv6 pool domain_name

### Description

This command is used to configure the domain name for the DHCPv6 pool of the Switch. The domain name configured here will be used as the default domain name by the client.

By default, the domain name is empty. If domain name is empty, the domain name information will not be provided to the client.

### Format

**config dhcpv6 pool domain_name <pool_name 12> <domain_name 255>**

### Parameters

**<pool_name 12>** - Enter the DHCPv6 pool name used here. This name can be up to 12 characters long.

**<domain_name 255>** - Enter the domain name used here. This name can be up to 255 characters long.

### Restrictions

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

### Example

To configure the domain name for the DHCPv6 pool pool1:

```
DGS-3620-28SC:admin# config dhcpv6 pool domain_name pool1 dlink.com
Command: config dhcpv6 pool domain_name pool1 dlink.com

Success.

DGS-3620-28SC:admin#
```

## 25-6 config dhcpv6 pool dns_server

### Description

This command is used to configure the DNS server's IPv6 addresses for a specific DHCPv6 pool. Users may add up to two DNS Server addresses. If DNS server is not specified, the DNS server information will not be provided to the client. Users could delete a DNS server address in the method of setting the DNS server address to zero.

### Format

**config dhcpv6 pool dns_server <pool_name 12> <ipv6addr> {<ipv6addr>}**

### Parameters

**<pool_name 12>** - Enter the DHCPv6 pool name used here. This name can be up to 12 characters long.

**<ipv6addr>** - Enter the primary DNS Server IPv6 address used for this pool here.

**<ipv6addr>** - (Optional) Enter the secondary DNS Server IPv6 address used for this pool here.

### Restrictions

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

### Example

To configure the DNS server address for a DHCPv6 pool:

```
DGS-3620-28SC:admin# config dhcpv6 pool dns_server pool1 2000::200 2000::201
Command: config dhcpv6 pool dns_server pool1 2000::200 2000::201

Success.

DGS-3620-28SC:admin#
```

## 25-7 config dhcpv6 pool lifetime

### Description

This command is used to configure the preferred-lifetime and valid-lifetime of IPv6 address within a DHCPv6 pool.

**Preferred lifetime** - the length of time that a valid address is preferred (i.e., the time until deprecation). When the preferred lifetime expires, the address becomes deprecated.

**Valid lifetime -** the length of time an address remains in the valid state (i.e., the time until invalidation). When the valid lifetime expires, the address becomes invalid.

The valid lifetime must be greater than or equal to the preferred lifetime.

### Format

**config dhcpv6 pool lifetime <pool_name 12> preferred_lifetime <sec 60-4294967295> valid_lifetime <sec 60-4294967295>**

### Parameters

**<pool_name 12>** - Enter the DHCPv6 pool name used here. This name can be up to 12 characters long.

**preferred_lifetime** - Specifies the length of time that a valid address is preferred to.
- **<sec 60-4294967295>** - Enter the preferred lifetime value here. This value must be between 60 and 4294967295 seconds.

**valid_lifetime** - Specifies the length of time an address remains in the valid state.
- **<sec 60-4294967295>** - Enter the valid lifetime value here. This value must be between 60 and 4294967295 seconds.

### Restrictions

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

### Example

To configure the preferred-lifetime and valid-lifetime for the DHCPv6 pool:

```
DGS-3620-28SC:admin# config dhcpv6 pool lifetime pool1 preferred_lifetime 80
valid_lifetime 100
Command: config dhcpv6 pool lifetime pool1 preferred_lifetime 80 valid_lifetime
100

Success.

DGS-3620-28SC:admin#
```

## 25-8 config dhcpv6 pool manual_binding

### Description

This command is used to configure a DHCPv6 pool manual binding entry. An address binding is a mapping between the IPv6 address and DUID (A DHCPv6 Unique Identifier for a DHCPv6 participant) of a client. The IPv6 address specified in the manual binding entry must be in the range of the DHCPv6 pool.

### Format

**config dhcpv6 pool manual_binding <pool_name 12> [add <ipv6addr> client_duid <string 28> | delete [<ipv6addr> | all]]**

### Parameters

**<pool_name 12>** - Enter the DHCPv6 pool name used here. This name can be up to 12 characters long.

**add** - Specifies the IPv6 address that will statically be bound to a device.
**<ipv6addr>** - Enter the IPv6 address used for the static bind here.

**client_duid** - Specifies the DUID of the device that will statically be bound to the IPv6 address entered in the previous field.
**<string 28>** - Enter the client DUID used here. This string can be up to 28 characters long.

**delete** - Specifies to delete the manual binding entry.
**<ipv6addr>** - Enter the IPv6 address of the manual binding entry to be deleted here.
**all** - Specifies that all manual binding entries will be deleted.

### Restrictions

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

### Example

To add a manual binding DHCPv6 entry:

```
DGS-3620-28SC:admin# config dhcpv6 pool manual_binding pool1 add 2000::3
client_duid 00010006124dd5840021918d4d9f
Command: config dhcpv6 pool manual_binding pool1 add 2000::3 client_duid
00010006124dd5840021918d4d9f


success


DGS-3620-28SC:admin#
```

## 25-9 show dhcpv6 manual_binding

### Description

This command will display the manual binding entries for the selected or all DHCPv6 pools.

### Format

**show dhcpv6 manual_binding {<pool_name 12>}**

### Parameters

**<pool_name 12>** - (Optional) Enter the DHCPv6 pool name used here. This name can be up to 12 characters long.

If no parameter is specified, then all the entries will be displayed.

### Restrictions

None.

### Example

To display the manual binding entries of the DHCPv6 pool:

```
DGS-3620-28SC:admin# show dhcpv6 manual_binding
Command: show dhcpv6 manual_binding

 Pool Name :net100
   Entry  1
     IPv6 Address: 3000:100:1::ABCD
     DUID        : 00030006001572200700

 Pool Name :net91
   Entry  1
     IPv6 Address: 3000:91:1::100
     DUID        : 00030006aabbcc000000

   Entry  2
     IPv6 Address: 3000:91:1::101
     DUID        : 00030006aabbcc000001

Total Entries: 3

DGS-3620-28SC:admin#
```

## 25-10 show dhcpv6 binding

### Description

This command is used to show the DHCPv6 dynamic binding information. Entering the command without the pool name will display all information regarding DHCPv6 dynamic binding on the switch. This command only displays the dynamic binding information, not including manual binding information.

### Format

**show dhcpv6 binding {<pool_name 12>}**

### Parameters

**<pool_name 12>** - (Optional) Enter the DHCPv6 pool name used here. This name can be up to 12 characters long.

### Restrictions

None.

### Example

To display the DHCPv6 dynamic binding information on the Switch:

```
DGS-3620-28SC:admin# show dhcpv6 binding
Command: show dhcpv6 binding

 Pool Name: net90        IPv6 Address: 3000:90:1::7
                         DUID        : 0003000600cd14517000
                         Preferred(s): 120          Valid(s): 240

 Pool Name: net100-2     IPv6 Address: 3000:100:1::1
                         DUID        : 00030006001572200300
                         Preferred(s): 120          Valid(s): 240

Total Entries : 2

DGS-3620-28SC:admin#
```

## 25-11 clear dhcpv6 binding

### Description

This command is used to clear the DHCPv6 dynamic binding information.

### Format

**clear dhcpv6 binding {<pool_name 12>}**

### Parameters

**<pool_name 12>** - (Optional) Enter the DHCPv6 pool name used here. This name can be up to 12 characters long.

### Restrictions

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

### Example

To clear the DHCPv6 dynamic binding information on the Switch:

```
DGS-3620-28SC:admin# clear dhcpv6 binding
Command: clear dhcpv6 binding

Success.

DGS-3620-28SC:admin#
```

## 25-12 enable dhcpv6_server

### Description

This command is used to enable the DHCPv6 server function on the Switch

### Format

**enable dhcpv6_server**

### Parameters

None.

### Restrictions

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

### Example

To configure the DHCPv6 server global state to enable:

```
DGS-3620-28SC:admin# enable dhcpv6_server
Command: enable dhcpv6_server

Success.

DGS-3620-28SC:admin#
```

## 25-13 disable dhcpv6_server

### Description

This command is used to disable the DHCPv6 server function on the Switch

### Format

**disable dhcpv6_server**

### Parameters

None.

### Restrictions

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

### Example

To configure the DHCPv6 server global state to disable:

```
DGS-3620-28SC:admin# disable dhcpv6_server
Command: disable dhcpv6_server

Success.

DGS-3620-28SC:admin#
```

## 25-14 show dhcpv6_server

### Description

This command is used to display the DHCPv6 server setting.

### Format

**show dhcpv6_server {ipif <ipif_name 12>}**

### Parameters

**ipif** - (Optional) Specifies the IP interface name to be displayed.

**<ipif_name 12>** - Enter the IP interface name to be displayed here. This name can be up to 12 characters long.

### Restrictions

None.

### Example

To display the DHCPv6 server setting:

```
DGS-3620-28SC:admin# show dhcpv6_server
Command: show dhcpv6_server

DHCPv6 Server Global State: Disabled
---------------------------------------------------------------
IP Interface              : System
DHCPv6 Server State       : Enabled

IP Interface              : ipif1
DHCPv6 Server State       : Enabled

Total Entries   : 2

DGS-3620-28SC:admin#
```

## 25-15 config dhcpv6 pool excluded_address

### Description

This command is used to configure the reserved IPv6 addresses on the DHCPv6 server.

### Format

**config dhcpv6 pool excluded_address <pool_name 12> [add begin <ipv6addr> end <ipv6addr> | delete [begin <ipv6addr> end <ipv6addr> | all]]**

### Parameters

| |
|---|
| **<pool_name 12>** - Enter the DHCPv6 pool name used here. This name can be up to 12 characters long. |
| **add** - Specifies to add an excluded address range for a specified pool.<br>**begin** - Specifies the beginning IPv6 address of the range of IPv6 addresses to be excluded from the DHCPv6 pool.<br>**<ipv6addr>** - Enter the beginning IPv6 address used here.<br>**end** - Specifies the ending IPv6 address of the range of IPv6 addresses to be excluded from the DHCPv6 pool.<br>**<ipv6addr>** - Enter the ending IPv6 address used here. |
| **delete** - Specifies to delete one or all excluded address ranges of a specified pool.<br>**begin** - Specifies the beginning IPv6 address of the range of IPv6 addresses to be excluded from the DHCPv6 pool.<br>**<ipv6addr>** - Enter the beginning IPv6 address used here.<br>**end** - Specifies the ending IPv6 address of the range of IPv6 addresses to be excluded from the DHCPv6 pool.<br>**<ipv6addr>** - Enter the ending IPv6 address used here.<br>**all** - Specifies to delete all excluded address ranges of a specified pool. |

### Restrictions

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

### Example

To add the IPv6 addresses range that DHCPv6 server should not assign to clients:

```
DGS-3620-28SC:admin# config dhcpv6 pool excluded_address pool1 add begin
2000::3 end 2000::8
Command: config dhcpv6 pool excluded_address pool1 add begin 2000::3 end
2000::8


Success.


DGS-3620-28SC:admin#
```

## 25-16 show dhcpv6 excluded_address

### Description

This command is used to display the groups of IPv6 addresses which are excluded from the legal assigned IPv6 address

### Format

**show dhcpv6 excluded_address {<pool_name 12>}**

### Parameters

**<pool_name 12> -** (Optional) Enter the DHCPv6 pool name used here. This name can be up to 12 characters long.

### Restrictions

None.

### Example

To display the excluded address information:

```
DGS-3620-28SC:admin# show dhcpv6 excluded_address
Command: show dhcpv6 excluded_address

Pool Name: net100
   Range  1
     Begin Address: 3000:100:1::1
     End Address  : 3000:100:1::7

 Pool Name: net110
   Range  1
     Begin Address: 3000:110:1::1
     End Address  : 3000:110:1::7

   Range  2
     Begin Address: 3000:110:1::9
     End Address  : 3000:110:1::9

   Range  3
     Begin Address: 3000:110:1::11
     End Address  : 3000:110:1::11

   Range  4
     Begin Address: 3000:110:1::13
     End Address  : 3000:110:1::13

Total Entries : 5

DGS-3620-28SC:admin#
```

## 25-17 config dhcpv6_server ipif

### Description

This command is used to configure the DHCPv6 Server state per interface.

### Format

**config dhcpv6_server ipif [<ipif_name 12> | all] state [enable | disable]**

## Parameters

**ipif** - Specifies the IP interface used.

- **<ipif_name 12>** - Enter the IP interface name used. This name can be up to 12 characters long.
- **all** - Specifies that all the IP interfaces will used.

**state** - Specifies the DHCPv6 server state for the specified interface.

- **enable** - Specifies that the DHCPv6 server state for the specified interface will be enabled.
- **disable** - Specifies that the DHCPv6 server state for the specified interface will be disabled.

## Restrictions

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

## Example

To configure the DHCPv6 Server state of System Interface to enable:

```
DGS-3620-28SC:admin# config dhcpv6_server ipif System state enable
Command: config dhcpv6_server ipif System state enable

Success.

DGS-3620-28SC:admin#
```

# Chapter 26 Distance Vector Multicast Routing Protocol (DVMRP) Commands

| |
|---|
| **config dvmrp** [ipif <ipif_name 12> \| all] {metric <value 1-31> \| probe <sec 1-65535> \| neighbor_timeout <sec 1-65535> \| state [enable \| disable]}(1) |
| **enable dvmrp** |
| **disable dvmrp** |
| **show dvmrp** {ipif <ipif_name 12>} |
| **show dvmrp neighbor** {ipif <ipif_name 12> \| ipaddress <network_address>} |
| **show dvmrp nexthop** {ipaddress <network_address> \| ipif <ipif_name 12>} |
| **show dvmrp routing_table** {ipaddress <network_address>} |

## 26-1 config dvmrp

### Description

This command is used to configure DVMRP configurations.

### Format

**config dvmrp [ipif <ipif_name 12> | all] {metric <value 1-31> | probe <sec 1-65535> | neighbor_timeout <sec 1-65535> | state [enable | disable]}(1)**

### Parameters

| |
|---|
| **ipif** - Specifies the IP interface name used.<br>**<ipif_name 12>** - Enter the IP interface name used here. This name can be up to 12 characters long.<br>**all** - Specifies that all the IP interfaces will be used. |
| **metric** - (Optional) Allows the assignment of a DVMRP route cost to the above IP interface. A DVMRP route cost is a relative number that represents the real cost of using this route in the construction of a multicast delivery tree. It is similar to, but not defined as, the hop count in RIP.<br>**<value 1-31>** - Enter the metric value used here. This value must be between 1 and 31. The default value is 1. |
| **probe** - (Optional) Specifies the time in seconds between the DVMRP Probe message transmissions.<br>**<sec 1-65535>** - Enter the probe value used here. This value must be between 1 and 65535 seconds. The default value is 10 seconds. |
| **neighbor_timeout** - (Optional) Specifies the time period for DVMRP will hold Neithbor Router reports before issuing poison route messages.<br>**<sec 1-65535>** - Enter the neighbor timeout value used here. This value must be between 1 and 65535 seconds. The default value is 35 seconds. |
| **state** - (Optional) Specifies the DVMRP state of the IP interface.<br>**enable** - Specifies that DVMRP of the specified IP interface will be enabled. |

**disable** - Specifies that DVMRP of the specified IP interface will be disabled.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

To configure DVMRP configurations of IP interface called ‘System’:

```
DGS-3620-28SC:admin# config dvmrp ipif System neighbor_timeout 30 metric 1
probe 5
Command: config dvmrp ipif System neighbor_timeout 30 metric 1 probe 5

Success

DGS-3620-28SC:admin#
```

## 26-2 enable dvmrp

### Description

This command is used to enable the DVMRP global state on the Switch.

### Format

**enable dvmrp**

### Parameters

None.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

To enable DVMRP:

```
DGS-3620-28SC:admin# enable dvmrp
Command: enable dvmrp

Success.

DGS-3620-28SC:admin#
```

## 26-3 disable dvmrp

### Description

This command is used to disable the DVMRP global state on the Switch.

### Format

**disable dvmrp**

### Parameters

None.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

To disable DVMRP:

```
DGS-3620-28SC:admin# disable dvmrp
Command: disable dvmrp

Success.

DGS-3620-28SC:admin#
```

## 26-4 show dvmrp

### Description

This command is used to display DVMRP configurations.

### Format

**show dvmrp {ipif <ipif_name 12>}**

### Parameters

| |
|---|
| **ipif** - (Optional) Specifies the IP interface name used for the display.<br>**<ipif_name 12>** - Enter the IP interface name used for the display here. This name can be up to 12 characters long. |
| If no parameter is specified, then all the IP interfaces will be displayed. |

### Restrictions

None. (EI Mode Only Command)

### Example

To display DVMRP configurations:

```
DGS-3620-28SC:admin#show dvmrp
Command: show dvmrp

DVMRP Global State : Disabled

Interface     IP Address         Neighbor Timeout   Probe  Metric  State
------------  -----------------  ----------------   -----  ------  --------
System        192.168.69.123     35                 10     1       Disabled

Total Entries: 1

DGS-3620-28SC:admin#
```

## 26-5 show dvmrp neighbor

### Description

This command is used to display the DVMRP neighbor table.

### Format

**show dvmrp neighbor {ipif <ipif_name 12> | ipaddress <network_address>}**

### Parameters

| |
|---|
| **ipif** - (Optional) Specifies the IP interface name used for the display.<br>**<ipif_name 12>** - Enter the IP interface name used for the display here. This name can be up to 12 characters long. |
| **ipaddress** - (Optional) Specifies the IP address and netmask of the destination used.<br>**<network_address>** - Enter the IP address and netmask of the destination used here. |
| If no parameter is specified, the system will display the whole DVMRP neighbor table. |

### Restrictions

None. (EI Mode Only Command)

### Example

To display DVMRP neighbor table:

```
DGS-3620-28SC:admin# show dvmrp neighbor
Command: show dvmrp neighbor

DVMRP Neighbor Address Table
Interface         Neighbor Address  Generation ID  Expire Time
---------------   ----------------  -------------  -----------
System            10.48.74.123      86             32

Total Entries : 1

DGS-3620-28SC:admin#
```

## 26-6 show dvmrp nexthop

### Description

This command is used to display the DVMRP routing next hop table.

### Format

**show dvmrp nexthop {ipaddress <network_address> | ipif <ipif_name 12>}**

### Parameters

**ipaddress** - (Optional) Specifies the IP address and netmask of the destination used.
**<network_address>** - Enter the IP address and netmask of the destination used here.

**ipif** - (Optional) Specifies the IP interface name used for the display.
**<ipif_name 12>** - Enter the IP interface name used for the display here. This name can be up to 12 characters long.

If no parameter is specified, the system will display all the DVMRP routing next hop tables.

### Restrictions

None. (EI Mode Only Command)

### Example

To display DVMRP routing next hop table:

```
DGS-3620-28SC:admin# show dvmrp nexthop
Command: show dvmrp nexthop

Source Address/NetMask  Interface Name   Type
----------------------  ---------------  ------
10.0.0.0/8              ip2              Leaf
10.0.0.0/8              ip3              Leaf
20.0.0.0/8              System           Leaf
20.0.0.0/8              ip3              Leaf
30.0.0.0/8              System           Leaf
30.0.0.0/8              ip2              Leaf

Total Entries : 6

DGS-3620-28SC:admin#
```

## 26-7 show dvmrp routing_table

### Description

This command is used to display the DVMRP routing table.

### Format

**show dvmrp routing_table {ipaddress <network_address>}**

### Parameters

| |
|---|
| **ipaddress** - (Optional) Specifies the IP address and netmask of the destination used.<br>**<network_address>** - Enter the IP address and netmask of the destination used here. |
| If no parameter is specified, the system will display the whole DVMRP routing table. |

### Restrictions

None. (EI Mode Only Command)

### Example

To display DVMRP routing table:

```
DGS-3620-28SC:admin# show dvmrp routing_table
Command: show dvmrp routing_table

DVMRP Routing Table
Source Address/Netmask  Upstream Neighbor  Metric  Learned  Interface   Expire
----------------------  -----------------  ------  -------  ----------  ------
10.0.0.0/8              10.90.90.90        2       Local    System      -
20.0.0.0/16             20.1.1.1           2       Local    ip2         -
30.0.0.0/24             30.1.1.1           2       Local    ip3         -

Total Entries : 3

DGS-3620-28SC:admin#
```

# Chapter 27 D-Link License Management System (DLMS)

**install dlms activation_code** <string 25> {unit <unit_id>}

**show dlms license**

## 27-1 install dlms activation_code

### Description

This command is used to install an activation code. The activation code is a set of codes which activates/ unlocks functions on the switch.

### Format

**install dlms activation_code <string 25> {unit <unit_id>}**

### Parameters

**<string 25>** Specifies an activation code. The length should be 25 string characters

**unit** - Specifies the unit to display.

**<unit_id>** Specifies the switch in the switch stack.

### Restrictions

Only Administrator level users can issue this command.

### Example

To input a legal activation code:

```
DGS-3620-28SC:admin# install dlms activation_code xBc7vNWsSpchuQkGZsTfPwcfa
Command: install dlms activation_code xBc7vNWsSpchuQkGZsTfPwcfa

Success.

Please reboot the device to active the license.

DGS-3620-28SC:admin#
```

## 27-2 show dlms license

### Description

This command will display the license information.

### Format

**show dlms license {unit <unit_id>}**

### Parameters

**unit** - Specifies the unit to display.
**<unit_id>** Specifies the switch in the switch stack.

### Restrictions

None.

### Example

To display license information:

```
DGS-3620-28SC:admin# show dlms license
Command: show dlms license

Device Default License : EI

DGS-3620-28SC:admin#
```

# Chapter 28 Domain Name System (DNS) Relay Commands

**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 add or delete a static entry into the Switch’s DNS resolution table, or set up the relay server.

### Format

**config dnsr [[primary | secondary] nameserver <ipaddr> | [add | delete] static <domain_name 32> <ipaddr>]**

### Parameters

**primary** - Specify to indicate that the IP address below is the address of the primary DNS server.

**secondary** - Specify to indicate that the IP address below is the address of the secondary DNS server.

**nameserver** - Specify the IP address of the DNS nameserver.
**<ipaddr>** - Specify the IP address of the DNS nameserver.

**add** - Specify to add the DNS relay function.

**delete** - Specify to delete the DNS relay function.

**static** - Specify the domain name of the entry.
**<domain_name32>** - Specify the domain name.
**<ipaddr>** - Specify the IP address of the entry.

### Restrictions

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

### Example

To set IP address 10.24.22.5 as the primary DNS server:

```
DGS-3620-28SC:admin# config dnsr primary nameserver 10.24.22.5
Command: config dnsr primary nameserver 10.24.22.5

Success.
```

```
DGS-3620-28SC:admin#
```

To add the entry “dns1” with IP address 10.24.22.5 to the DNS static table:

```
DGS-3620-28SC:admin#config dnsr add static dns1 10.24.22.5
Command: config dnsr add static dns1 10.24.22.5

Success.

DGS-3620-28SC:admin#
```

To delete the entry “dns1” with IP address 10.24.22.5 from the DNS static table:

```
DGS-3620-28SC:admin#config dnsr delete static dns1 10.24.22.5
Command: config dnsr delete static dns1 10.24.22.5

Success.

DGS-3620-28SC:admin#
```

## 28-2 enable dnsr

### Description

This command is used to enable DNS relay.

### Format

**enable dnsr {[cache | static]}**

### Parameters

**cache** - Specify to enable the cache lookup for the DNS relay on the switch.

**static** - Specify to enable the static table lookup for the DNS relay on the switch.

### Restrictions

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

### Example

To enable DNS relay:

```
DGS-3620-28SC:admin#enable dnsr
Command: enable dnsr

Success.

DGS-3620-28SC:admin#
```

To enable cache lookup for DNS relay:

```
DGS-3620-28SC:admin#enable dnsr cache
Command: enable dnsr cache

Success.

DGS-3620-28SC:admin#
```

To enable static table lookup for DNS relay:

```
DGS-3620-28SC:admin#enable dnsr static
Command: enable dnsr static

Success.

DGS-3620-28SC:admin#
```

## 28-3 disable dnsr

### Description

This command is used to disable DNS relay on the switch.

### Format

**disable dnsr {[cache | static]}**

### Parameters

| |
|---|
| **cache** - (Optional) Specify to disable the cache lookup for the DNS relay on the switch. |
| **static** - (Optional) Specify to disable the static table lookup for the DNS relay on the switch. |

### Restrictions

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

### Example

To disable the status of DNS relay:

```
DGS-3620-28SC:admin#disable dnsr
Command: disable dnsr

Success.

DGS-3620-28SC:admin#
```

To disable cache lookup for DNS relay:

```
DGS-3620-28SC:admin#disable dnsr cache
Command: disable dnsr cache

Success.
```

```

DGS-3620-28SC:admin#
```

To disable static table lookup for DNS relay:

```
DGS-3620-28SC:admin#disable dnsr static
Command: disable dnsr static

Success.

DGS-3620-28SC:admin#
```

## 28-4 show dnsr

### Description

This command is used to display the current DNS relay configuration and static entries.

### Format

**show dnsr {static}**

### Parameters

**static** - (Optional) Specify to display the static entries in the DNS relay table. If this parameter is omitted, the entire DNS relay table will be displayed.

### Restrictions

None.

### Example

To display the DNS relay status:

```
DGS-3620-28SC: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
----------------------------------------- ---------------
www.123.com.tw                            10.12.12.123

Total Entries: 1

DGS-3620-28SC:admin#
```

# Chapter 29 Domain Name System (DNS) Resolver Commands

**config name_server add** <ipaddr> {primary}

**config name_server delete** <ipaddr> {primary}

**config name_server timeout** <second 1-60>

**show name_server**

**create host_name** <name 255> <ipaddr>

**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> {primary}**

### Parameters

**<ipaddr>** - Enter the DNS Resolver name server IP address used here.

**primary** – (Optional) Specifies that the name server is a primary name server.

### Restrictions

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

### Example

To add DNS Resolver primary name server 10.10.10.10:

```
DGS-3620-28SC:admin# config name_server add 10.10.10.10 primary
Command: config name_server add 10.10.10.10 primary

Success.

DGS-3620-28SC: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> {primary}**

### Parameters

**<ipaddr> -** Enter the DNS Resolver name server IP address used here.

**primary** – (Optional) Specifies that the name server is a primary name server.

### Restrictions

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

### Example

To delete DNS Resolver name server 10.10.10.1:

```
DGS-3620-28SC:admin# config name_server delete 10.10.10.10
Command: config name_server delete 10.10.10.10

Success.

DGS-3620-28SC: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 <second 1-60>**

### Parameters

**timeout** - Specifies the maximum time waiting for a responce from a specified name server.

**<second 1-60>** - Enter the timeout value used here. This value must be between 1 and 60 seconds.

### Restrictions

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

### Example

To configure DNS Resolver name server time out to 10 seconds:

```
DGS-3620-28SC:admin# config name_server timeout 10
Command: config name_server timeout 10

Success.

DGS-3620-28SC: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-3620-28SC:admin# show name_server
Command: show name_server

Name Server Time Out: 3 seconds

Static Name Server Table:
Server IP Address     Priority
--------------------- --------------
20.20.20.20           Secondary
10.1.1.1              Primary

Dynamic Name Server Table:
Server IP Address     Priority
--------------------- --------------
10.48.74.122          Primary

DGS-3620-28SC: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>**

### Parameters

**<name 255>** - Enter the hostname used here. This name can be up to 255 characters long.

**<ipaddr>** - Enter the host IP address used here.

### Restrictions

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

### Example

To create static host name “www.example.com”:

```
DGS-3620-28SC:admin# create host_name www.example.com 10.10.10.10
Command: create host_name www.example.com 10.10.10.10

Success.

DGS-3620-28SC: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 used here. This name can be up to 255 characters long.

**all** - Specifies that all the hostnames will be deleted.

### Restrictions

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

### Example

To delete the static host name entry “www.example.com”:

```
DGS-3620-28SC:admin# delete host_name www.example.com
Command: delete host_name www.example.com

Success.

DGS-3620-28SC: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) Specifies to display the static host name entries. | |
| **dynamic** – (Optional) Specifies to display the dynamic host name entries. | |

### Restrictions

None.

### Example

To display the static and dynamic host name entries:

```
DGS-3620-28SC:admin# show host_name
Command: show host_name

Static Host Name Table
Host Name                            IP Address
------------------------------   ---------------
www.example.com                     10.10.10.10
www.exampla.com                     20.20.20.20

Total Static Entries: 2

Dynamic Host Name Table
Host Name                            IP Address       TTL
------------------------------   --------------- --------
www.examplc.com                     30.30.30.30      60 minutes
www.exampld.com                     40.40.40.40      10 minutes

Total Dynamic Entries: 2

DGS-3620-28SC: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 Administrator, Operator and Power-User level users can issue this command.

### Example

To configure the DNS Resolver state to enabled:

```
DGS-3620-28SC:admin# enable dns_resolver
Command: enable dns_resolver

Success.

DGS-3620-28SC: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 Administrator, Operator and Power-User level users can issue this command.

### Example

To configure the DNS Resolver state to disabled:

```
DGS-3620-28SC:admin# disable dns_resolver
Command: disable dns_resolver

Success.

DGS-3620-28SC:admin#
```

# Chapter 30 D-Link Unidirectional Link Detection (DULD) Commands

| |
|---|
| **config duld ports** [<portlist> \| all] {state [enable \| disable] \| mode [shutdown \| normal] \| discovery_time <sec 5-65535>} |
| **show duld ports** {<portlist>} |

## 30-1 config duld ports

### Description

The command 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>}**

### Parameters

| |
|---|
| **ports** - Specify a range of ports to be used.<br>**<portlist>** - Enter the list of ports used for this configuration here.<br>**all** – Specifies that all the ports will be used for this configuration. |
| **state** - (Optional) Specifies these ports unidirectional link detection status. The default state is disabled.<br>**enable** - Specifies that the unidirectional link detection status will be enabled.<br>**disable** - Specifies that the unidirectional link detection status will be disabled. |
| **mode** - (Optional) Specifies the mode the unidirectional link detection will be set to.<br>**shutdown** - If any unidirectional link is detected, disable the port and log an event.<br>**normal** - Only log an event when a unidirectional link is detected. |
| **discovery_time** - (Optional) Specifies these ports neighbor discovery time. If the discovery is timeout, the unidirectional link detection will start. The default discovery time is 5 seconds.<br>**<sec 5-65535>** - Enter the discovery time value here. This value must be between 5 and 65535. |

### Restrictions

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

### Example

To enable unidirectional link detection on port 1:

```
DGS-3620-28SC:admin# config duld ports 1 state enable
Commands: config duld ports 1 state enable

Success

DGS-3620-28SC:admin#
```

## 30-2 show duld ports

### Description

This command is used to show unidirectional link detection information.

### Format

**show duld ports {<portlist>}**

### Parameters

| |
|---|
| **ports** - (Optional) Specify a range of ports to be display.<br>**<portlist>** - Enter the list of ports to be displayed here. |
| If no ports are specified, all the ports will be displayed. |

### Restrictions

None.

### Example

To show ports 1-4 unidirectional link detection information:

```
DGS-3620-28SC:admin#config duld ports 1,2,4 state enable
Commands: config duld ports 1,2,4 state enable

Success

DGS-3620-28SC:admin#show duld ports 1-4
Commands: show duld ports 1-4

port   Admin State  Oper Status  Mode            Link Status        Discovery
Time(Sec)
----   -----------  -----------  ----------     --------------     ------------
-------
1       Enabled       Enabled       Shutdown       Bidirectional      5
2       Enabled       Enabled       Normal         RX Fault             5
3       Enabled       Enabled       Normal         TX Fault             5
4       Disabled      Disabled      Normal         Unknown              5
5       Enabled       Enabled       Normal         Link Down            5

DGS-3620-28SC:admin#
```

# Chapter 31 Ethernet Ring Protection Switching (ERPS) Commands

**enable erps**

**disable erps**

**create erps raps_vlan** <vlanid>

**delete erps raps_vlan** <vlanid>

**config erps raps_vlan** <vlanid> [state [enable | disable] | ring_mel <value 0-7> | ring_port [west [<port> | 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> tc_propagation state [enable | disable] | [add | delete] sub_ring raps_vlan <vlanid> | revertive [enable | disable] | timer {holdoff_time <millisecond 0-10000> | guard_time <millisecond 10-2000> | wtr_time <min 5-12>}(1)]

**config erps log** [enable | disable]

**config erps trap** [enable | disable]

**show erps** {raps_vlan <vlanid> {sub_ring}}

## 31-1 enable erps

### Description

This command is used to enable the ERPS function on a switch. STP and LBD should be disabled on the ring ports before enabling ERPS. ERPS cannot be enabled before the R-APS VLAN is created, and ring ports, an RPL port, an RPL owner, are configured. In order to guarantee correct operation, the following integrity will be checked when ERPS is enabled:

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.

### Format

**enable erps**

### Parameters

None.

### Restrictions

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

### Example

To enable ERPS:

```
DGS-3620-28SC:admin#enable erps
Command: enable erps

Success.

DGS-3620-28SC:admin#
```

## 31-2 disable erps

### Description

This command is used to disable the ERPS function on the switch.

### Format

**disable erps**

### Parameters

None. The ERPS is disabled by default.

### Restrictions

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

### Example

To disable ERPS:

```
DGS-3620-28SC:admin#disable erps
Command: disable erps

Success.

DGS-3620-28SC:admin#
```

## 31-3 create erps raps_vlan

### Description

This command is used to create an R-APS VLAN on the switch. There should be only one R-APS VLAN used to transfer R-APS messages. Note that the R-APS VLAN must already have been created by the create vlan command. This command can only be issued when ERPS is disabled.

### Format

**create erps raps_vlan <vlanid>**

### Parameters

| |
|---|
| **<vlanid>** - Specify the VLAN which will be the R-APS VLAN. |

### Restrictions

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

### Example

To create an ERPS RAPS VLAN:

```
DGS-3620-28SC:admin#create erps raps_vlan 4094
Command: create erps raps_vlan 4094

Success.

DGS-3620-28SC:admin#
```

## 31-4 delete erps raps_vlan

### Description

This command is used to delete an R-APS VLAN on the 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 ERPS is disabled.

### Format

**delete erps raps_vlan <vlanid>**

### Parameters

| |
|---|
| **<vlanid>** - Specify the VLAN which will be the R-APS VLAN. |

### Restrictions

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

### Example

To delete an R-APS VLAN:

```
DGS-3620-28SC:admin#delete erps raps_vlan 4094
Command: delete erps raps_vlan 4094

Success.

DGS-3620-28SC:admin#
```

## 31-5 config erps raps_vlan

### Description

This command is used to set the R-APS VLAN parameters. The **ring_mel** command is used to configure the ring MEL for an R-APS VLAN. 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, 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 ring MEL is not higher than the highest MEL of the MEPs on the ring ports, the R-APS PDU cannot be forwarded on the ring.

The **ring_port** command is used to configure the port that participates in the ERPS 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.

The **rpl** command is used to configure the RPL port and the RPL owner.

**RPL port** - Specifies one of the R-APS VLAN ring ports as the RPL port. To remove an RPL port from an R-APS VLAN, use the **none** designation for **rpl_port**.

**RPL owner** - Specifies the node as the RPL owner.

The **protected_vlan** command is used to configure the VLANs that are protected by the ERPS function.

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.

The **timer** commands are used to configure the protocol timers:

**Holdoff timer** - Hold-off timer is used to filter out intermittent link faults when link failure occurs. This timer is used during the protection switching process when link failure occurs. When a ring node detects a link’s failure, it will start the hold off timer. It will report the link failure event (R-APS BPDU with SF flag) after the link failure is confirmed within this period of time.

**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 when link failure recovers. When the link node detects that the link failure is recovered, 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. Therefore, the blocking state of the recovered link will not be recovered within this period of time. This time 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. This timer 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.

## Format

**config erps raps_vlan <vlanid> [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> tc_propagation state [enable | disable] | [add |delete] sub_ring raps_vlan <vlanid> | revertive [enable | disable] | timer {holdoff_time <millisecond 0-10000> | guard_time <millisecond 10-2000> | wtr_time <min 5-12>}(1)]**

## Parameters

**<vlanid>** - The VLAN ID associated with the R-APS VLAN.

**state** - Specifies the ERPS R-APS VLAN state.
**enable** - Specifies that the ERPS R-APS VLAN state will be enabled.
**disable** - Specifies that the ERPS R-APS VLAN state will be disabled.

**ring_mel** - Specify the ring MEL of the R-APS function. The default ring MEL is 1.
**<value 0-7>** - Specify a value between 0 and 7.
**ring_port** - Specify a port participating in the ERPS ring.
**west** - Specify the port as the west ring port.
**<port>** - Specify a port.
**virtual_channel** - Specify the port as a west port on the virtual channel.
**east** - Specify the port as the east ring port.
**<port>** - Specify a port.
**virtual_channel** - Specify the port as an east port on the virtual channel.

**rpl_port** - By default, the node has no RPL port.
**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.

**rpl_owner** - By default, the RPS owner is disabled.
**enable** - Specify the device as an RPL owner node.
**disable** - This node is not an RPL owner.

**protected_vlan** - Specify VLANs that are protected by the ERPS function. 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.
**add** - Add VLANs to the protected VLAN group
**delete** - Delete VLANs from the protected VLAN group.
**vlanid** - Specify a VLAN ID list.
**<vidlist>** - Specify a range of VLAN IDs.

**sub_ring** - Specifies the sub-ring configuration.
**raps_vlan** - Specify the R-APS VLAN.
**<vlanid>** - Enter the R-APS VLAN ID used here.
**tc_propagation** - Specifies to configure the state of the topology change propagation for the sub-ring.
**state** - Specifies the propagation state of the topology change for the sub-ring.
**enable** - 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** - Specifies the add a topology change propagation rule.
**sub_ring** - Specifies the sub-ring configuration information.
**raps_vlan** - Specify the R-APS VLAN
**<vlanid>** - Enter the R-APS VLAN ID used here.

**delete** - Specifies the delete a topology change propagation rule.
**sub_ring** - Specifies the sub-ring configuration information.
**raps_vlan** - Specify the R-APS VLAN.
**<vlanid>** - Enter the R-APS VLAN ID used here.

**revertive** - Specifies the revertive mode state.
**enable** - Specifies that the revertive mode will be enabled.
**disable** - Specifies that the revertive mode will be disabled.

**timer** - Configure the ERPS timers for a specific R-APS VLAN.

**holdoff_time** - Specify the holdoff time of the R-APS function.
**<value 0-10000>** - Specify the time between 0 and 10000. The default hold off time is 0 milliseconds.
**guard_time** - Specify the guard time of the R-APS function.
**<value 10-2000>** - Specify the time between 10 and 2000. The default guard time is 500 milliseconds.
**wtr_time** - Specify the WTR time of the R-APS function.
**<value 5-12>** - Specify the time between 5 and 12. The default WTR time is 5 minutes.

## Restrictions

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

## Example

To set the R-APS west ring port parameter to 5:

```
DGS-3620-28SC:admin#config erps raps_vlan 4094 ring_port west 5
Command: config erps raps_vlan 4094 ring_port west 5

Success.

DGS-3620-28SC:admin#
```

To set the R-APS east ring port parameter to 7:

```
DGS-3620-28SC:admin#config erps raps_vlan 4094 ring_port east 7
Command: config erps raps_vlan 4094 ring_port east 7

Success.

DGS-3620-28SC:admin#
```

To set the R-APS RPL parameter:

```
DGS-3620-28SC:admin#config erps raps_vlan 4094 rpl_port west
Command: config erps raps_vlan 4094 rpl_port west

Success.

DGS-3620-28SC:admin#config erps raps_vlan 4094 rpl_owner enable
Command: config erps raps_vlan 4094 rpl_owner enable

Success.

DGS-3620-28SC:admin#
```

To set the R-APS protected VLAN parameter:

```
DGS-3620-28SC: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-3620-28SC:admin#
```

To set the R-APS timer parameter:

```
DGS-3620-28SC: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_time 10

Success.

DGS-3620-28SC:admin#
```

## 31-6 config erps log

### Description

This command is used to configure the ERPS log state.

### Format

**config erps log [enable | disable]**

### Parameters

**enable** - Enable the log state. The default value is disabled.

**disable** - Disable the log state.

### Restrictions

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

### Example

To set the log state:

```
DGS-3620-28SC:admin#config erps log enable
Command: config erps log enable

Success.

DGS-3620-28SC:admin#
```

## 31-7 config erps trap

### Description

This command is used to configure trap state of ERPS events.

### Format

**config erps trap [enable | disable]**

### Parameters

**trap** - Specifies to enable or disable the ERPS trap state.
    **enable** - Enter enable to enable the trap state.
    **disable** - Enter disable to disable the trap state. The default value is disabled.

### Restrictions

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

### Example

To configure the trap state of the ERPS:

```
DGS-3620-28SC:admin# config erps trap enable
Command: config erps trap enable

Success.

DGS-3620-28SC:admin#
```

## 31-8 show erps

### Description

This command is used to display ERPS configuration and operation information. The port state of the ring port may be as Forwarding, Blocking, or Signal Fail. Forwarding indicates that traffic is able to be forwarded. Blocking indicates that traffic is blocked by ERPS and a signal failure is not detected on the port. Signal Fail indicates that a signal failure is detected on the port and traffic is blocked by ERPS.

### Format

**show erps {raps_vlan <vlanid> {sub_ring}}**

### Parameters

**raps_vlan** - Specifies the R-APS VLAN.
    **<vlanid>** - Enter the R-APS VLAN ID used here.

**sub_ring** - Display the sub-ring configuration information.

### Restrictions

None.

### Example

To display ERPS information:

```
DGS-3620-28SC:admin#show erps
Command: show erps

 Global Status            : Enabled
 Log Status               : Enabled
 Trap Status              : Disabled
 ------------------------------------
 R-APS VLAN               : 4094
 ERPS Status              : Disabled
 Admin West Port          : 1:5
 Operational West Port    : 1:5  (Forwarding)
 Admin East Port          : 1:7
 Operational East Port    : 1:7  (Forwarding)
 Admin RPL Port           : West port
 Operational RPL Port     : West port
 Admin Owner              : Enabled
 Operational Owner        : Enabled
 Protected VLANs          : 10-20
 Ring MEL                 : 1
 Holdoff Time             : 100 milliseconds
 Guard Time               : 1000 milliseconds
 WTR Time                 : 10 minutes
 Revertive mode           : Enabled
 Current Ring State       : -

 ------------------------------------
 Total Rings: 1

DGS-3620-28SC:admin#
```

# Chapter 32 External Alarm Commands

| |
|---|
| **config external_alarm {unit < unit_id>} channel <value 1-2> message <sentence 1-128>** |
| **show external_alarm {unit <unitlist>}** |

## 32-1 config external_alarm

### Description

This command is used to configure external alarm message for a channel.

The source of alarm is located outside of the switch. They are monitored via pre-defined connection channels, with each channel representing a specific alarm event. This command allows the user to define the alarm event associated with each channel.

### Format

**config external_alarm {unit < unit_id>} channel <value 1-2> message <sentence 1-128>**

### Parameters

| |
|---|
| **unit** - Specifies the unit to display.<br>**<unit_id> -** Specifies the switch in the switch stack. |
| **channel** - Specifies which channel is selected to configure.<br>**<value 1-2>** - Enter the value of the channel number to be used here. |
| **message** - Alarm messages to display on console, log and trap.<br>**<sentence 1-128>** - Enter up to 128 characters here for the message to be displayed. |

### Restrictions

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

### Example

To configure an alarm message for channel 1 of unit 2:

```
DGS-3620-28SC:admin# config external_alarm unit 2 channel 1 message External
Alarm: UPS is exhausted!
Command: config external_alarm unit 2 channel 1 message External Alarm: UPS is
exhausted!


Success.


DGS-3620-28SC:admin#
```

## 32-2 show external_alarm

### Description

This command is used to display the real-time status of external alarm.

### Format

**show external_alarm {unit <unitlist>}**

### Parameters

**unit** - Specifies the unit(s) to display.
**<unitlist>** - Enter the number of the unit(s) here.

### Restrictions

None.

### Example

To display the real-time status of external alarm when the switch is not support stacking:

```
DGS-3620-28SC:admin# show external_alarm
Command: show external_alarm

Unit      Channel     Status       Message
------   ---------   --------      --------------------------------------------
1          1         Normal        External Alarm 1
1          2         Normal        External Alarm 2

DGS-3620-28SC:admin#
```

# Chapter 33 FDB Commands

| |
|---|
| **create fdb** <vlan_name 32> <macaddr> [port <port> \| drop] |
| **create fdb vlanid** <vidlist> <macaddr> [port <port> \| drop] |
| **create multicast_fdb** <vlan_name 32> <macaddr> |
| **config multicast_fdb** <vlan_name 32> <macaddr> [add \| delete] <portlist> |
| **config fdb aging_time** <sec 10-1000000> |
| **config multicast vlan_filtering_mode** [vlanid <vidlist> \| vlan <vlan_name 32> \| all] [forward_all_groups \| forward_unregistered_groups \| filter_unregistered_groups] |
| **delete fdb** <vlan_name 32> <macaddr> |
| **clear fdb** [vlan <vlan_name 32> \| port <port> \| all] |
| **show multicast_fdb** {[vlan <vlan_name 32> \| vlanid <vidlist>] \| mac_address <macaddr>} |
| **show fdb** {[port <port> \| vlan <vlan_name 32> \| vlanid <vidlist> \| mac_address <macaddr> \| static \| aging_time \| security]} |
| **show multicast vlan_filtering_mode** {[vlanid <vidlist> \| vlan <vlan_name 32>]} |

## 33-1 create fdb

### Description

This command is used to make an entry into the switch's unicast MAC address forwarding database.

### Format

**create fdb <vlan_name 32> <macaddr> [port <port> | drop]**

### Parameters

| |
|---|
| **<vlan_name 32>** - Specify a VLAN name associated with a MAC address. The maximum length is 32 characters. |
| **<macaddr>** - Specify the MAC address to be added to the static forwarding table. |
| **port** - The switch will always forward traffic to the specified device through this port.<br>**<port>** - Specify the port number corresponding to the MAC destination address.<br>**drop** - Specify to have the switch drop traffic. |

### Restrictions

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

### Example

To create an unicast MAC forwarding:

```
DGS-3620-28SC:admin#create fdb default 00-00-00-00-01-02 port 1:5
Command: create fdb default 00-00-00-00-01-02 port 1:5

Success.
DGS-3620-28SC:admin#
```

## 33-2 create fdb vlanid

### Description

This command is used to create an entry into the switch’s unicast MAC address forwarding database using the VLAN ID.

### Format

**create fdb vlanid <vidlist> <macaddr> [port <port> | drop]**

### Parameters

**<vidlist>** - Enter the VLAN ID used here.

**<macaddr>** - Specify the MAC address to be added to the static forwarding table.

**port** - The switch will always forward traffic to the specified device through this port.
- **<port>** - Specify the port number corresponding to the MAC destination address.
- **drop** - Specify to have the switch drop traffic.

### Restrictions

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

### Example

To create an unicast MAC forwarding:

```
DGS-3620-28SC:admin#create fdb vlanid 1 00-11-22-33-44-55 port 1:5
Command: create fdb vlanid 1 00-11-22-33-44-55 port 1:5

Success.

DGS-3620-28SC:admin#
```

## 33-3 create multicast_fdb

### Description

This command is used to make an entry into the switch’s multicast MAC address forwarding database.

### Format

**create multicast_fdb <vlan_name 32> <macaddr>**

### Parameters

**<vlan_name 32>** - Specify the name of the VLAN on which the MAC address resides. The maximum length is 32 characters.

**<macaddr>** - Specify the multicast MAC address to be added to the static forwarding table.

### Restrictions

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

### Example

To create multicast MAC forwarding:

```
DGS-3620-28SC:admin# create multicast_fdb default 01-00-00-00-01-01
Command: create multicast_fdb default 01-00-00-00-01-01

Success.

DGS-3620-28SC:admin#
```

## 33-4 config multicast_fdb

### Description

This command is used to configure the multicast MAC address forwarding table.

### Format

**config multicast_fdb <vlan_name 32> <macaddr> [add | delete] <portlist>**

### Parameters

**<vlan_name 32>** - Specify the name of the VLAN on which the MAC address resides. The maximum name length is 32 characters.

**<macaddr>** - Specify the MAC address that will be added or deleted to the forwarding table.

**add** - Specify to add ports.
**delete** - Specify to delete ports.

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

### Restrictions

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

### Example

To add multicast MAC forwarding:

```
DGS-3620-28SC:admin# config multicast_fdb default 01-00-00-00-01-01 add 1-5
Command: config multicast_fdb default 01-00-00-00-01-01 add 1-5

Success.

DGS-3620-28SC:admin#
```

## 33-5 config fdb aging_time

### Description

This command is used to set the age-out timer for the switch's dynamic unicast MAC address forwarding tables.

### Format

**config fdb aging_time <sec 10-1000000>**

### Parameters

**<sec 10-1000000>** - Specify the time in seconds that a dynamically learned MAC address will remain in the switch's MAC address forwarding table without being accessed, before being dropped from the database. The range of the value is 10 to 1000000. The default value is 300.

### Restrictions

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

### Example

To configure MAC address aging time:

```
DGS-3620-28SC:admin#config fdb aging_time 300
Command: config fdb aging_time 300

Success.

DGS-3620-28SC:admin#
```

## 33-6 config multicast vlan_filtering_mode

### Description

This command is used to configure the multicast packet filtering mode for VLANs.

### 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 the VLAN ID list to set.
**<vidlist>** - Specify the VLAN ID list to set.

**vlan** - Specify the VLAN to set.
**<vlan_name 32>** - The maximum length is 32 characters.

**all** - Specify to set all VLANs.

**forward_all_groups** - Specifies that all multicast groups will be forwarded based on the VLAN.

**forward_unregistered_groups** - Specify the filtering mode as forward_unregistered_groups. This is the default.

**filter_unregistered_groups** - Specify the filtering mode as filter_unregistered_groups.

### Restrictions

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

### Example

To configure the the multicast packet filtering mode for all VLANs:

```
DGS-3620-28SC:admin#config multicast vlan_filtering_mode all
forward_unregistered_groups
Command: config multicast port filtering_mode all forward_unregistered_groups

Success.

DGS-3620-28SC:admin#
```

## 33-7 delete fdb

### Description

This command is used to delete a permanent FDB entry.

### Format

**delete fdb <vlan_name 32> <macaddr>**

### Parameters

**<vlan_name 32>** - Specify the name of the VLAN on which the MAC address resides. The maximum length is 32 characters.

**<macaddr>** - Specify the MAC address to be deleted from the static forwarding table.

### Restrictions

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

### Example

To delete a permanent FDB entry:

```
DGS-3620-28SC:admin#delete fdb default 00-00-00-00-01-02
Command: delete fdb default 00-00-00-00-01-02

Success.

DGS-3620-28SC:admin#
```

## 33-8 clear fdb

### Description

This command is used to clear the switch's forwarding database of all dynamically learned MAC addresses.

### Format

**clear fdb [vlan <vlan_name 32> | port <port> | all ]**

### Parameters

| |
|---|
| **vlan** - Specify the name of the VLAN on which the MAC address resides.<br>**<vlan_name 32>** - The maximum length is 32 characters. |
| **port** - Specify the port number corresponding to the dynamically learned MAC address.<br>**<port>** - Specify the port number corresponding to the dynamically learned MAC address. |
| **all** - Specify to clear all VLANs and ports. |

### Restrictions

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

### Example

To clear all FDB dynamic entries:

```
DGS-3620-28SC:admin#clear fdb all
Command: clear fdb all

Success.

DGS-3620-28SC:admin#
```

## 33-9 show multicast_fdb

### Description

This command is used to display the contents of the switch's multicast forwarding database.

### Format

**show multicast_fdb {[vlan <vlan_name 32> | vlanid <vidlist>] | mac_address <macaddr>}**

### Parameters

| |
|---|
| **vlan** - (Optional) Specify the name of the VLAN on which the MAC address resides.<br>**<vlan_name 32>** - The maximum length is 32 characters. |
| **vlanid** – (Optional) Specifies the VLAN ID on which the MAC address resides.<br>**<vidlist>** - Enter the VLAN ID used here. |
| **mac_address** - (Optional) Specify a MAC address, for which FDB entries will be displayed.<br>**<macaddr>** - Specify a MAC address, for which FDB entries will be displayed. |

**Note:** If no parameter is specified, all multicast FDB entries will be displayed.

### Restrictions

None.

### Example

To display multicast MAC address table:

```
DGS-3620-28SC:admin#show multicast_fdb
Command: show multicast_fdb

VLAN Name      : default
MAC Address    : 01-00-00-00-01-01
Egress Ports   : 1-5,26
Mode           : Static

Total Entries : 1

DGS-3620-28SC:admin#
```

## 33-10 show fdb

### Description

This command is used to display the current unicast MAC address forwarding database.

### Format

**show fdb {[port <port> | vlan <vlan_name 32> | vlanid <vidlist> | mac_address <macaddr> | static | aging_time | security]}**

### Parameters

**port** - (Optional) Specify the entries for one port.
    <**port**> - Specify the entries for one port.

**vlan** - (Optional) Specify to display the entries for a specific VLAN.
    **<vlan_name 32>** - The maximum length is 32 characters.

**vlanid** - (Optional) Specify to display the entries by VLAN ID list.
    **<vidlist>** - Specify to display the entries by VLAN ID list.

**mac_address** - (Optional) Specify the MAC address.
    **<macaddr>** - Specify the MAC address.

**static** - (Optional) Specify to display all permanent entries.

**aging_time** - Specify to display the unicast MAC address aging time.

**security** – Specify to display the security settings.

**Note:** If no parameter is specified, all unicast FDB entries will be displayed.

### Restrictions

None.

### Example

To display unicast MAC address table:

```
DGS-3620-28SC: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                          00-26-5A-AE-CA-1C 21    Dynamic Forward

Total Entries: 2

DGS-3620-28SC:admin#
```

## 33-11 show multicast vlan_filtering_mode

### Description

This command is used to display the multicast packet filtering mode for VLANs.

### Format

**show multicast vlan_filtering_mode {[vlanid <vidlist> | vlan <vlan_name 32>]}**

### Parameters

**vlanid** - (Optional) Specify to display the entries by VLAN ID list.
**<vidlist>** - Specify to display the entries by VLAN ID list.

**vlan** - (Optional) Specify to display the entries for a specific VLAN.
**<vlan_name 32>** - The maximum length is 32 characters.

### Restrictions

None.

### Example

To show multicast filtering mode for ports:

```
DGS-3620-28SC:admin#show multicast vlan_filtering_mode
Command: show multicast filtering_mode

VLAN ID/VLAN Name                 Multicast Filter Mode
-------------------------------  -----------------------------
default                          forward_unregistered_groups
```

```

DGS-3620-28SC:admin#
```

# Chapter 34 File System Management Commands

| |
|---|
| **show storage_media_info** {[unit <unit_id> \| all]} |
| **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> |
| **erase** {{unit <unit_id>} <drive_id>} <pathname> |
| **format** {unit <unit_id>} <drive_id> {[fat16 \| fat32]} {<label_name>} |
| **del** {{unit <unit_id>} <drive_id>} <pathname> {recursive} |
| **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> |
| **change drive** {unit <unit_id>} <drive_id> |

## 34-1 show storage_media_info

### Description

This command is used to display storage media information.

### Format

**show storage_media_info {[unit <unit_id> | all]}**

### Parameters

| |
|---|
| **unit** - Specifies the unit ID in the stacking system. If not specified, it refers to the master unit.<br>**<unit_id>** - Enter the unit ID value here. |
| **all** – Specifies that all the units, in the stacking system's storage media information will be displayed. |

### Restrictions

None.

### Example

To display storage media information:

```
DGS-3620-28SC:admin#show storage_media_info
Command: show storage_media_info

Unit  Drive  Media Type      Size  Label        FS Type  Version
----  -----  ----------  --------  -----------  -------  -------
   1  c:     Flash         123 MB               FFS

DGS-3620-28SC:admin#
```

## 34-2 md

### Description

This command is used to create a directory.

### Format

**md {{unit <unit_id>} <drive_id>} <pathname>**

### Parameters

**unit** - Specifies the unit ID in the stacking system. If not specified, it refers to the master unit.
**<unit_id>** - Enter the unit ID value here.
**<drive_id>** - Specifies the drive ID. If not specified, it refers to the current drive.

**<pathname>** - Specify the directory to be created. The path name can be specified either as a full path name or partial name. For a partial path name, it indicates the directory is in the current directory.

### Restrictions

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

### Example

To create a directory:

```
DGS-3620-28SC:admin#md c:/abc
Command: md c:/abc

Success.

DGS-3620-28SC:admin#
```

## 34-3 rd

### Description

This command is used to remove a directory. If there are files and directories still existing in the directory, this command will fail and return an error message.

### Format

**rd {{unit <unit_id>} <drive_id>} <pathname>**

### Parameters

**unit** - Specifies the unit ID in the stacking system. If not specified, it refers to the master unit.
**<unit_id>** - Enter the unit ID value here.
**<drive_id>** - Specifies the drive ID. If not specified, it refers to the current drive.

**<pathname>** - Specify the directory to be removed. The path name can be specified either as a full path name or partial name. For a partial path name, it indicates the file is in the current directory.

### Restrictions

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

### Example

To delete an empty directory:

```
DGS-3620-28SC:admin#rd c:/abc
Command: rd c:/abc

Success.

DGS-3620-28SC:admin#
```

## 34-4 cd

### Description

This command is used to change the current directory. The user can change the current directory to another drive using this command. The current drive and current directory will be displayed if the **<pathname>** is not specified.

### Format

**cd {<pathname>}**

### Parameters

**<pathname>** - (Optional) Specify the directory to be changed. The path name can be specified either as a full path name or partial name. For a partial path name, it indicates the file is in the current directory.

### Restrictions

None.

### Example

To change a work directory:

```
DGS-3620-28SC:admin#cd d1
Command: cd d1
```

```
Current work directory: "c:/d1"

DGS-3620-28SC:admin#
```

## 34-5 dir

### Description

This command is used to list all of the files located in a directory of a drive. If a path name 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 directory will be displayed. If a user lists the system directory, the used space will be shown.

### Format

**dir {{unit <unit_id>} <drive_id>} {<pathname>}**

### Parameters

| |
|---|
| **unit** - Specifies the unit ID in the stacking system. If not specified, it refers to the master unit.<br>**<unit_id>** - Enter the unit ID value here.<br>**<drive_id>** - Specifies the drive ID. If not specified, it refers to the current drive. |
| **<pathname>** - (Optional) Specify the directory to be listed. The path name can be specified either as a full path name or partial name. For a partial path name, it indicates the file is in the current directory. The drive ID also included in this parameter, for example: d:/config/bootup.cfg. |

### Restrictions

None.

### Example

To list a directory:

```
DGS-3620-28SC:admin#dir
Command: dir

Directory of c:/
Idx Info    Attr Size     Update Time          Name
--- ------- ---- -------- -------------------- ----
  1 RUN(*)  -rw- 4796564  2000/01/22 03:52:03  runtime.had
  2 CFG(*)  -rw- 24120    2000/01/22 23:22:58  config.cfg
  3 CFG(b)  -rw- 24120    2000/01/23 06:59:39  1
  4         d---          2000/01/23 22:52:50  system
30608 KB total (25700 KB free)

 (*) -with boot up info         (b) -with backup info

DGS-3620-28SC:admin#
```

To list a system directory:

```
DGS-3620-28SC:admin#dir c:/system
Command: dir c:/system

System reserved directory. Used space 89KB.

DGS-3620-28SC:admin#
```

## 34-6 rename

### Description

This command is used to rename a file in the file system. The pathname specifies the file (in path form) to be renamed and the file name specifies the new file name. If the path name 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** - Specifies the unit ID in the stacking system. If not specified, it refers to the master unit.
**<unit_id>** - Enter the unit ID value here.
**<drive_id>** - Specifies the drive ID. If not specified, it refers to the current drive.

**<pathname>** - Specify the file (in path form) to be renamed.

**<filename>** - Specify the new name of the file.

### Restrictions

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

### Example

To rename a file or directory:

```
DGS-3620-28SC:admin#rename run.had run1.had
Command: rename run.had run1.had

Success.

DGS-3620-28SC:admin#
```

## 34-7 erase

### Description

This command is used to delete a file stored in the file system. The system will prompt if the target file is a bootup image/configuration or the last image.

### Format

**erase {{unit <unit_id>} <drive_id>} <pathname>**

### Parameters

**unit** - Specifies the unit ID in the stacking system. If not specified, it refers to the master unit.
    **<unit_id>** - Enter the unit ID value here.
    **<drive_id>** - Specifies the drive ID. If not specified, it refers to the current drive.

**<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 Administrator and Operator-level users can issue this command.

### Example

To delete a file:

```
DGS-3620-28SC:admin#erase cfg
Command: erase cfg

Are you sure to remove the boot up Configuration from this device? (y/n)y

Success.

DGS-3620-28SC:admin#
```

## 34-8 format

### Description

This command is used to format a specific drive.

### Format

**format {unit <unit_id>} <drive_id> {[fat16 | fat32]} {<label_name>}**

### Parameters

**unit** - Specifies the unit ID in the stacking system. If not specified, it refers to the master unit.
    **<unit_id>** - Enter the unit ID value here.
    **<drive_id>** - Specifies the drive ID.

**fat16** - (Optional) Specifies that the drive will be formatted to support a FAT16 file system.
**fat32** - (Optional) Specifies that the drive will be formatted to support a FAT32 file system.

**<label_name>** - (Optional) Enter the label name used for this drive here.

### Restrictions

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

### Example

To format media:

```
DGS-3620-28SC:admin#format d: fat32
Command: format d: fat32

 Formatting.......................... Done!

DGS-3620-28SC:admin#
```

## 34-9 del

### Description

This command is used to delete a file. It is also used to delete a directory and its contents. The system will prompt if the target file is a bootup image/configuration or the last image.

### Format

**del {{unit <unit_id>} <drive_id>} <pathname> {recursive}**

### Parameters

**unit** - Specifies the unit ID in the stacking system. If not specified, it refers to the master unit.
**<unit_id>** - Enter the unit ID value here.
**<drive_id>** - Specifies the drive ID. If not specified, it refers to the current drive.

**<pathname>** - Specify 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) Used on the directory, to delete a directory and its contents even if it is not empty.

### Restrictions

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

### Example

To delete a file:

```
DGS-3620-28SC:admin#del cfg
Command: del cfg

Are you sure to remove the boot up Configuration from this device? (y/n)y

Success.

DGS-3620-28SC:admin#
```

To delete a a directory with the parameter “recursive”:

```
DGS-3620-28SC:admin# del d1 recursive
Command: del d1 recursive

Success.

DGS-3620-28SC:admin#
```

## 34-10 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 be renamed at the same time.

### Format

**move {{unit <unit_id>} <drive_id>} <pathname> {{unit <unit_id>} <drive_id>} <pathname>**

### Parameters

| |
|---|
| **unit** - Specifies the unit ID in the stacking system. If not specified, it refers to the master unit.<br>**<unit_id>** - Enter the unit ID value here.<br>**<drive_id>** - Specifies the drive ID. If not specified, it refers to the current drive. |
| **<pathname>** - Specify the file to be moved. The path name can be specified either as a full path name or partial name. For a partial path name, it indicates the file is in the current directory. |
| **unit** - Specifies the unit ID in the stacking system. If not specified, it refers to the master unit.<br>**<unit_id>** - Enter the unit ID value here.<br>**<drive_id>** - Specifies the drive ID. If not specified, it refers to the current drive. |
| **<pathname>** - Specify the new path where the file will be moved. The path name can be specified either as a full path name or partial name. For a partial path name, it indicates the file is in the current directory. |

### Restrictions

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

### Example

To move a file or directory:

```
DGS-3620-28SC:admin#move c:/log.txt c:/abc/log1.txt
Command: move c:/log.txt c:/abc/log1.txt

Success.

DGS-3620-28SC:admin#
```

## 34-11 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** - Specifies the unit ID in the stacking system. If not specified, it refers to the master unit.
**<unit_id>** - Enter the unit ID value here.
**<drive_id>** - Specifies the drive ID. If not specified, it refers to the current drive.
**<pathname>** - Specify the file to be copied. If it is specified in the associated form, then it is related to the current directory.

**unit** - Specifies the unit ID in the stacking system. If not specified, it refers to the master unit.
**<unit_id>** - Enter the unit ID value here.
**<drive_id>** - Specifies the drive ID. If not specified, it refers to the current drive.
**<pathname>** - Specify the file to copy to. If it is specified in the associated form, then it is related to the current directory

### Restrictions

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

### Example

To copy a file:

```
DGS-3620-28SC:admin#copy c:/log.txt c:/log1.txt
Command: copy c:/log.txt c:/log1.txt

Copying........................... Done!

DGS-3620-28SC:admin#
```

## 34-12 change drive

### Description

This command is used to change the current drive.

### Format

**change drive {unit <unit_id>} <drive_id>**

### Parameters

**unit** - (Optional) Specifies a unit ID if in the stacking system. If not specified, it refers to the master unit.
**<unit_id>** - Enter the unit ID here.

**<drive_id>** - Specifies the drive ID. The format of drive_id is ‘c:’, or ‘d:’.

### Restrictions

None.

### Example

To display the storage media’s information:

```
DGS-3620-28SC:admin# change drive unit 3 c:
Command: change drive unit 3 c:

Current work directory: "/unit3:/c:".

DGS-3620-28SC:admin#
```

# Chapter 35 Filter Commands

**config filter dhcp_server** [add permit server_ip <ipaddr> {client_mac <macaddr>} ports [<portlist> | all] | delete permit server_ip <ipaddr> {client_mac <macaddr>} ports [<portlist> | all] | ports [<portlist> | all] state [enable | disable] | illegal_server_log_suppress_duration [1min | 5min | 30min] | trap_log [enable | disable]]

**show filter dhcp_server**

**config filter extensive_netbios** [<portlist> | all] state [enable | disable]

**show filter extensive_netbios**

**config filter netbios** [<portlist> | all] state [enable | disable]

**show filter netbios**

## 35-1 config filter dhcp_server

### Description

This command has two purposes: to specify to filter all DHCP server packets on the specific port and to specify to allow some DHCP server packets with pre-defined server IP addresses and client MAC addresses. With this function, we can restrict the DHCP server to service specific DHCP clients. This is useful when two DHCP servers are present on the network; one of them can provide the private IP address and the other can provide the public IP address.

Enabling filter DHCP server port state will create one access profile and create one access rule per port (UDP port = 67). Filter commands in this file will share the same access profile. Addition of a permit DHCP entry will create one access profile and create one access rule. Filter commands in this file will share the same access profile.

### Format

**config filter dhcp_server [add permit server_ip <ipaddr> {client_mac <macaddr>} ports [<portlist> | all] | delete permit server_ip <ipaddr> {client_mac <macaddr>} ports [<portlist> | all] | ports [<portlist> | all] state [enable | disable] | illegal_server_log_suppress_duration [1min | 5min | 30min] | trap_log [enable | disable]]**

### Parameters

**add permit server_ip** - Specify the IP address of the DHCP server to be permitted.
  **<ipaddr>** - Specify the IP address.
  **client_mac** - (Optional) Specify the MAC address of the DHCP client.
    **<macaddr>** - Specify the MAC address.
  **ports** - Specify the ports.
    **<portlist>** - Specify the range of ports to be configured.
    **all** - Specify to configure all ports.

**delete permit server_ip** - Specify the delete permit server IP address.
  **<ipaddr>** - Specify the IP address.
  **client_mac** - (Optional) Specify the MAC address of the DHCP client.
    **<macaddr>** - Specify the MAC address.
  **ports** - Specify the ports.
    **<portlist>** - Specify the range of ports to be configured.
    **all** - Specify to configure all ports.

**ports** - Specify the ports.
  **<portlist>** - Specify the range of ports to be configured.

**all** - Specify to configure all ports.
**state** - Specify the port status.
**enable** - Enable the state.
**disable** - Disable the state.

**illegal_server_log_suppress_duration** - Specify the illegal server log suppression duration.
**1min** - Specify an illegal server log suppression duration of 1 minute.
**5min** - Specify an illegal server log suppression duration of 5 minutes.
**30min** - Specify an illegal server log suppression duration of 30 minutes.

**trap_log** - Specify the trap log status.
**enable** - Enable the trap log feature.
**disable** - Disable the trap log feature.

### Restrictions

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

### Example

To add an entry from the DHCP server/client filter list in the switch's database:

```
DGS-3620-28SC:admin#config filter dhcp_server add permit server_ip 10.1.1.1
client_mac 00-00-00-00-00-01 port 1-26
Command: config filter dhcp_server add permit server_ip 10.1.1.1 client_mac 00-
00-00-00-00-01 port 1-26

Success.

DGS-3620-28SC:admin#
```

To configure the filter DHCP server state:

```
DGS-3620-28SC:admin#config filter dhcp_server ports 1-10 state enable
Command: config filter dhcp_server ports 1-10 state enable

Success.

DGS-3620-28SC:admin#
```

## 35-2 show filter dhcp_server

### Description

This command is used to display the DHCP server/client filter list created on the switch.

### Format

**show filter dhcp_server**

### Parameters

None.

### Restrictions

None.

### Example

To display the DHCP server/client filter list created on the switch:

```
DGS-3620-28SC:admin#show filter dhcp_server
Command: show filter dhcp_server

Enabled Ports: 1,28
Trap & Log State: Enabled
Illegal Server Log Suppress Duration: 1 minutes
Permit DHCP Server/Client Table
Server IP Address Client MAC Address  Port
----------------- ------------------- ---------------
 Total Entries: 0

DGS-3620-28SC:admin#
```

## 35-3 config filter extensive_netbios

### Description

This command is used to configure the switch to deny NetBIOS packets over 802.3 frames on the network. Enabling the filterNetBIOS packets over 802.3 frames will create one access profile and one access rule per port automatically. Filter commands in this file will share the same access profile.

### Format

**config filter extensive_netbios [<portlist> | all] state [enable | disable]**

### Parameters

| |
|---|
| **<portlist>** - Specify the port or range of ports to configure. |
| **all** - Specify to configure all ports. |
| **state** - Specify the status of the filter to block the NetBIOS packets over 802.3 frames.<br>**enable** - Enable the filter to block the NetBIOS packets over 802.3 frames.<br>**disable** - Disable the filter to block the NetBIOS packets over 802.3 frames. |

### Restrictions

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

### Example

To configure the extensive NetBIOS filter state on ports 1 to 10:

```
DGS-3620-28SC:admin#config filter extensive_netbios 1-10 state enable
Command: config filter extensive_netbios 1-10 state enable

```

```
Success.

DGS-3620-28SC:admin#
```

## 35-4 show filter extensive_netbios

### Description

This command is used to display the extensive NetBIOS filter state on the switch.

### Format

**show filter extensive_netbios**

### Parameters

None.

### Restrictions

None.

### Example

To display the extensive NetBIOS filter state on the switch:

```
DGS-3620-28SC:admin#show filter extensive_netbios
Command: show filter extensive_netbios

Enabled Ports: 1-3

DGS-3620-28SC:admin#
```

## 35-5 config filter netbios

### Description

This command is used to configure the Switch to deny NetBIOS packets on the network. Enabling of the filter NetBIOS state will create one access profile and three access rules per port automatically (UDP ports 137 and138 and TCP port 139). Filter commands in this file will share the same access profile.

### Format

**config filter netbios [<portlist> | all] state [enable | disable]**

### Parameters

| |
|---|
| **<portlist>** - Specify the port or range of ports to configure. |
| **all** - Specify to configure all ports. |
| **state** - Specify the status of the filter to block NetBIOS packets.<br>**enable** - Enable the filter to block NetBIOS packets. |

**disable** - Disable the filter to block NetBIOS packets.

### Restrictions

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

### Example

To configure the NetBIOS filter state:

```
DGS-3620-28SC:admin#config filter netbios 1-10 state enable
Command: config filter netbios 1-10 state enable

Success.

DGS-3620-28SC:admin#
```

## 35-6 show filter netbios

### Description

This command is used to display the NetBIOS filter state on the switch.

### Format

**show filter netbios**

### Parameters

None.

### Restrictions

None.

### Example

To display the NetBIOS filter state:

```
DGS-3620-28SC:admin#show filter netbios
Command: show filter netbios

Enabled Ports: 1-3

DGS-3620-28SC:admin#
```

# Chapter 36 Gratuitous ARP Commands

**enable gratuitous_arp** {ipif <ipif_name 12>} {trap | log}(1)

**disable gratuitous_arp** {ipif <ipif_name 12>} {trap | log}(1)

**config gratuitous_arp learning** [enable | disable]

**config gratuitous_arp send dup_ip_detected** [enable | disable]

**config gratuitous_arp send ipif_status_up** [enable | disable]

**config gratuitous_arp send periodically ipif** <ipif_name 12> interval <value 0-65535>

**show gratuitous_arp** {ipif <ipif_name 12>}

## 36-1 enable gratuitous_arp

### Description

This command is used to enable the gratuitous ARP trap and log state. The switch can trap and log the IP conflict event to inform the administrator.

### Format

**enable gratuitous_arp {ipif <ipif_name 12>} {trap | log}(1)**

### Parameters

**ipif** - (Optional) The interface name of the L3 interface.
**<ipif_name 12>** - Specify the interface name. The maximum length is 12 characters.

**trap** - Specify trap. The trap is disabled by default.

**log** - Specify log. The even log is enabled by default.

### Restrictions

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

### Example

To enable gratuitous ARP:

```
DGS-3620-28SC:admin#enable gratuitous_arp ipif System trap log
Command: enable gratuitous_arp ipif System trap log

Success.

DGS-3620-28SC:admin#
```

## 36-2 disable gratuitous_arp

### Description

This command is used to disable the gratuitous ARP trap and log state.

### Format

**disable gratuitous_arp {ipif <ipif_name 12>} {trap | log}(1)**

### Parameters

**ipif** - (Optional) The interface name of the L3 interface.
  **<ipif_name 12>** - Specify the interface name. The maximum length is 12 characters.

**trap** - Specify trap. The trap is disabled by default.

**log** - Specify log. The even log is enabled by default.

### Restrictions

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

### Example

To disable gratuitous ARP, the trap, and the log state:

```
DGS-3620-28SC:admin#disable gratuitous_arp ipif System trap log
Command: disable gratuitous_arp ipif System trap log

Success.

DGS-3620-28SC:admin#
```

## 36-3 config gratuitous_arp learning

### Description

This command is used to enable or disable learning of ARP entries in the ARP cache based on the received gratuitous ARP packets.

### Format

**config gratuitous_arp learning [enable | disable]**

### Parameters

**enable** - Enable learning of ARP entries based on the received gratuitous ARP packets.

**disable** - Disable learning of ARP entries based on the received gratuitous ARP packets.

### Restrictions

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

### Example

To enable learning of ARP entries in the ARP cache based on the received gratuitous ARP packets:

```
DGS-3620-28SC:admin# config gratuitous_arp learning enable
```

```
Command: config gratuitous_arp learning enable

Success.

DGS-3620-28SC:admin#
```

## 36-4 config gratuitous_arp send dup_ip_detected

### Description

This command is used to enable or disable the sending of gratuitous ARP requests when a duplicate IP address is detected. By default, the state is disabled. For this command, 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 somebody out there is using an IP address that conflicts with that of 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** - Enable the sending of gratuitous ARP requests when a duplicate IP is detected.

**disable** - Disable the sending of gratuitous ARP requests when a duplicate IP is detected.

### Restrictions

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

### Example

To enable the sending of gratuitous ARP requests when a duplicate IP address is detected:

```
DGS-3620-28SC:admin#config gratuitous_arp send dup_ip_detected enable
Command: config gratuitous_arp send dup_ip_detected enable

Success.

DGS-3620-28SC:admin#
```

## 36-5 config gratuitous_arp send ipif_status_up

### Description

This command is used to enable or disable the sending of gratuitous ARP requests when the IP interface status becomes up. This is used to automatically announce the interface's IP address to other nodes. By default, the state is disabled. When the state is enabled and IP interface is linked up, one gratuitous ARP packet will be broadcast.

### Format

**config gratuitous_arp send ipif_status_up [enable | disable]**

### Parameters

**enable** - Enable the sending of gratuitous ARP requests when the IPIF status becomes up.

**disable** - Disable the sending of gratuitous ARP requests when the IPIF status becomes up.

### Restrictions

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

### Example

To enable the sending of gratuitous ARP requests when the IP interface status becomes up:

```
DGS-3620-28SC:admin#config gratuitous_arp send ipif_status_up enable
Command: config gratuitous_arp send ipif_status_up enable

Success.

DGS-3620-28SC:admin#
```

## 36-6 config gratuitous_arp send periodically ipif

### Description

This command is used to configure the interval for the periodical sending of gratuitous ARP request packets.

### Format

**config gratuitous_arp send periodically ipif <ipif_name 12> interval <value 0-65535>**

### Parameters

**<ipif_name 12>** - Specify the interface name of the L3 interface. The maximum length is 12 characters.

**interval** - The periodically send gratuitous ARP interval time, in seconds.
**<value 0-65535>** - Specify the value between 0 and 65535. 0 (zero) means not to send gratuitous ARP request packets periodically. By default, the interval is 0 (zero).

### Restrictions

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

### Example

To configure the gratuitous ARP interval to 5 for the IPIF System:

```
DGS-3620-28SC:admin#config gratuitous_arp send periodically ipif System
interval 5
```

```
Command: config gratuitous_arp send periodically ipif System interval 5

Success.

DGS-3620-28SC:admin#
```

## 36-7 show gratuitous_arp

### Description

This command is used to display gratuitous ARP configuration.

### Format

**show gratuitous_arp {ipif <ipif_name 12>}**

### Parameters

**ipif** - (Optional) The interface name of the L3 interface.
**<ipif_name 12>** - Specify the interface name. The maximum length is 12 characters.

### Restrictions

None.

### Example

To display the gratuitous ARP log and trap state:

```
DGS-3620-28SC:admin#show gratuitous_arp
Command: show gratuitous_arp

Send on IPIF Status Up        : Disabled
Send on Duplicate IP Detected : Disabled
Gratuitous ARP Learning       : Disabled

IP Interface Name : System
        Gratuitous ARP Trap                    : Disabled
        Gratuitous ARP Log                     : Enabled
        Gratuitous ARP Periodical Send Interval : 0

Total Entries: 1

DGS-3620-28SC:admin#
```

# Chapter 37 Internet Group Management Protocol (IGMP) Commands

| |
|---|
| **config igmp** [ipif <ipif_name 12> \| all] {version <value 1-3> \| query_interval <sec 1-31744> \| max_response_time <sec 1-25> \| robustness_variable <value 1-7> \| last_member_query_interval <value 1-25> \| state [enable \| disable]} (1) |
| **show igmp** {ipif <ipif_name 12>} |
| **show igmp group** {group <group> \| ipif <ipif_name 12>} |
| **config igmp check_subscriber_source_network** [ipif <ipif_name 12> \| all] [enable \| disable] |
| **show igmp check_subscriber_source_network** {ipif <ipif_name 12>} |
| **create igmp static_group ipif** <ipif_name 12> group <ipaddr> |
| **delete igmp static_group ipif** <ipif_name 12> [group <ipaddr> \| all] |
| **show igmp static_group** {ipif <ipif_name 12>} |

## 37-1 config igmp

### Description

This command is used to configure IGMP on the Switch.

### Format

**config igmp [ipif <ipif_name 12> | all] {version <value 1-3> | query_interval <sec 1-31744> | max_response_time <sec 1-25> | robustness_variable <value 1-7> | last_member_query_interval <value 1-25> | state [enable | disable]} (1)**

### Parameters

| |
|---|
| **ipif** - Specifies the IP interface name used for this configuration.<br>**<ipif_name 12>** - Enter the IP interface name used for this configuration here. This name can be up to 12 characters long.<br>**all** - Specifies that all the IP interfaces will be used. |
| **version** - (Optional) Specifies the IGMP version used.<br>**<value 1-3>** - Enter the IGMP version number used here. This value must be between 1 and 3. The default value is 3. |
| **query_interval** - (Optional) Specifies the time in seconds between general query transmissions.<br>**<sec 1-31744>** - Enter the query interval time here. This value must be between 1 and 31744 seconds. The default value is 125. |
| **max_response_time** - (Optional) Specifies the maximum time in seconds to wait for reports from members.<br>**<sec 1-25>** - Enter the maximum response time here. This value must be between 1 and 25 seconds. The default value is 10. |
| **robustness_variable** - (Optional) Specifies the permitted packet loss that guarantees IGMP.<br>**<value 1-7>** - Enter the robustness variable here. This value must be between 1 and 7. The default value is 2. |
| **last_member_query_interval** - (Optional) Specifies the maximum Response Time inserted into the Group-Specific Queries that are sent in response to Leave Group messages, which is also the amount of time between Group-Specific Query messages. |

**<value 1-25>** - Enter the last member query interval value here. This value must be between 1 and 25. The default value is 1.

**state** - (Optional) Specifies the IGMP state on a router interface.

**enable** - Specifies that the IGMP state will be enabled.

**disable** - Specifies that the IGMP state will be disabled.

### Restrictions

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

### Example

To enable IGMP version 1 for the IP interface “System”:

```
DGS-3620-28SC:admin# config igmp ipif System version 1 state enable
Command: config igmp ipif System version 1 state enable

Success.

DGS-3620-28SC:admin#
```

To configure IGMPv2 for all IP interfaces:

```
DGS-3620-28SC:admin# config igmp all version 2
Command: config igmp all version 2

Success.

DGS-3620-28SC:admin#
```

## 37-2 show igmp

### Description

This command is used to display the IGMP configuration.

### Format

**show igmp {ipif <ipif_name 12>}**

### Parameters

**ipif** - (Optional) Specifies the IP interface name used for this configuration.

**<ipif_name 12>** - Enter the IP interface name used for this configuration here. This name can be up to 12 characters long.

**all** - Specifies that all the IP interfaces will be used.

If no parameter is specified, the system will display all IGMP configurations.

### Restrictions

None.

### Example

To display the IGMP configuration for all interfaces:

```
DGS-3620-28SC:admin#show igmp
Command: show igmp

IGMP Interface Configurations

Interface    IP Address/Netmask  Ver- Query  Maximum  Robust- Last     State
                                 sion        Response ness    Member
                                             Time     Value   Query
                                                              Interval
------------ ------------------  ---- ------ -------- ------- -------- --------
System       10.90.90.90/8       3    125    10       2       1        Disabled

Total Entries: 1

DGS-3620-28SC:admin#
```

## 37-3 show igmp group

### Description

This command is used to display the switch’s IGMP group table.

### Format

**show igmp group {group <group> | ipif <ipif_name 12>}**

### Parameters

| |
|---|
| **group** - (Optional) Specifies the multicast group ID.<br>**<group>** - Enter the multicast group ID value here. |
| **ipif** - (Optional) Specifies the IP interface name used for this configuration.<br>**<ipif_name 12>** - Enter the IP interface name used for this configuration here. This name can be up to 12 characters long.<br>**all** - Specifies that all the IP interfaces will be used. |
| If no parameter is specified, the system will display all IGMP group tables. |

### Restrictions

None.

### Example

To display the IGMP group table:

```
DGS-3620-28SC:admin# show igmp group
Command: show igmp group

Interface      Multicast Group  Last Reporter   IP Querier          IP Expire
------------  ---------------  --------------- ------------------- ---------
System         224.0.0.2        10.42.73.111    10.48.74.122        260
System          224.0.0.9         10.20.53.1       10.48.74.122        260
System          224.0.1.24        10.18.1.3        10.48.74.122        259
System          224.0.1.41        10.1.43.252      10.48.74.122        259
System          224.0.1.149       10.20.63.11      10.48.74.122        259

Total Entries : 5

DGS-3620-28SC:admin#
```

## 37-4 config igmp check_subscriber_source_network

### Description

This command is used to configure the flag that determines whether or not to check the subscriber source IP when an IGMP report or leave message is received. When this command is enabled on an interface, any IGMP report or leave messages received by the interface will be checked to determine whether its source IP is in the same network as the interface. If the check failed for a received report or leave message, the message won't be processed by IGMP protocol. If the check is disabled, the IGMP report or leave message with any source IP will be processed by the IGMP protocol.

### Format

**config igmp check_subscriber_source_network [ipif <ipif_name 12> | all] [enable | disable]**

### Parameters

**ipif** - Specifies the IP interface name used for this configuration.
  **<ipif_name 12>** - Enter the IP interface name used for this configuration here. This name can be up to 12 characters long.
  **all** - Specifies that all the IP interfaces will be used.

**enable** - Specifies that the check state will be enabled.
**disable** - Specifies that the check state will be disabled.

### Restrictions

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

### Example

To enable the checking of subscriber source IP addresses when an IGMP report or leave message is received on the interface called 'System':

```
DGS-3620-28SC:admin# config igmp check_subscriber_source_network ipif System
enable
Command: config igmp check_subscriber_source_network ipif System enable

Success.

DGS-3620-28SC:admin#
```

## 37-5 show igmp check_subscriber_source_network

### Description

This command is used to display the status of the IGMP report/leave message source IP check.

### Format

**show igmp check_subscriber_source_network {ipif <ipif_name 12>}**

### Parameters

| | |
|---|---|
| **ipif** – (Optional) Specifies the IP interface name used for this configuration.<br>**<ipif_name 12>** - Enter the IP interface name used for this configuration here. This name can be up to 12 characters long. |
| If no parameter is specified, the system will display all interfaces. |

### Restrictions

None.

### Example

To show the status of the check subscriber for the received IGMP report/leave messages on interface “n20”:

```
DGS-3620-28SC:admin# show igmp check_subscriber_source_network ipif n20
Command: show igmp check_subscriber_source_network ipif n20

Interface    IP Address/Netmask  Check Subscriber Source Network
------------ ------------------  -------------------------------
n20          20.1.1.1/8          Disabled

Total Entries: 1

DGS-3620-28SC:admin#
```

To show the status of the check subscriber for the received IGMP report/leave messages on all interfaces:

```
DGS-3620-28SC:admin# show igmp check_subscriber_source_network
Command: show igmp check_subscriber_source_network

Interface    IP Address/Netmask  Check Subscriber Source Network
------------ ------------------  -------------------------------
System       10.90.90.90/8       Enabled
n1           1.1.1.1/8           Disabled
n11          11.1.1.1/8          Disabled
n20          20.1.1.1/8          Disabled
n100         100.3.2.2/8         Disabled

Total Entries: 5
```

```
DGS-3620-28SC:admin#
```

## 37-6 create igmp static_group

### Description

This command is used to create an IGMP static group on the Switch.

### Format

**create igmp static_group ipif <ipif_name 12> group <ipaddr>**

### Parameters

**ipif** – Specifies the IP interface name used for this configuration.
  **<ipif_name 12>** - Enter the IP interface name used for this configuration here. This name can be up to 12 characters long.

**group** - Specifies the multicast IP address used.
  **<ipaddr>** - Enter the multicast IP address used here.

### Restrictions

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

### Example

To create an IGMP static group, with the multicast IP address 225.0.0.2 on the IP interface "System":

```
DGS-3620-28SC:admin# create igmp static_group ipif System group 225.0.0.2
Command: create igmp static_group ipif System group 225.0.0.2

Success.

DGS-3620-28SC:admin#
```

## 37-7 delete igmp static_group

### Description

This command is used to delete IGMP static group(s) on the switch.

### Format

**delete igmp static_group ipif <ipif_name 12> [group <ipaddr> | all]**

### Parameters

**ipif** – Specifies the IP interface name used for this configuration.
  **<ipif_name 12>** - Enter the IP interface name used for this configuration here. This name can be up to 12 characters long.

**group** - Specifies the multicast IP address used.
  **<ipaddr>** - Enter the multicast IP address used here.

**all** – Specifies that all the multicast IP addresses will be deleted.

### Restrictions

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

### Example

To delete the IGMP static group, with the multicast IP address 225.0.0.2 on the IP interface “System”.

```
DGS-3620-28SC:admin# delete igmp static_group ipif System group 225.0.0.2
Command: delete igmp static_group ipif System group 225.0.0.2

Success.

DGS-3620-28SC:admin#
```

To delete all IGMP static groups on the IP interface “n2”.

```
DGS-3620-28SC:admin# delete igmp static_group ipif n2 all
Command: delete igmp static_group ipif n2 all

Success.

DGS-3620-28SC:admin#
```

## 37-8 show igmp static_group

### Description

This command is used to display IGMP static groups on the Switch.

### Format

**show igmp static_group {ipif <ipif_name 12>}**

### Parameters

**ipif** – (Optional) Specifies the IP interface name used for this configuration.
**<ipif_name 12>** - Enter the IP interface name used for this configuration here. This name can be up to 12 characters long.

### Restrictions

None.

### Example

To display all IGMP static groups on the interface “n20”:

```
DGS-3620-28SC:admin# show igmp static_group ipif n20
Command: show igmp static_group ipif n20

Interface       Multicast Group
------------    ---------------
n20             239.0.0.3

Total Entries: 1

DGS-3620-28SC:admin#
```

To display all IGMP static groups on all interfaces:

```
DGS-3620-28SC:admin# show igmp static_group
Command: show igmp static_group

Interface        Multicast Group
------------     ---------------
System           225.0.0.1
System           225.0.0.2
n20              239.0.0.3

Total Entries: 3

DGS-3620-28SC:admin#
```

# Chapter 38 IGMP Proxy Commands

**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 <vlanid 1-4094>] **|** router_ports [add | delete] <portlist> **|** source_ip <ipaddr> **|** unsolicited_report_interval <sec 0-25>}(1)

**show igmp_proxy** {group}

## 38-1 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-3620-28SC:admin#enable igmp_proxy
Command: enable igmp_proxy

Success.

DGS-3620-28SC:admin#
```

## 38-2 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-3620-28SC:admin#disable igmp_proxy
Command: disable igmp_proxy

Success.

DGS-3620-28SC:admin#
```

## 38-3 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-3620-28SC:admin#config igmp_proxy downstream_if add vlan vlanid 2-7
```

```
Command: config igmp_proxy downstream_if add vlan vlanid 2-7

Success.

DGS-3620-28SC:admin#
```

## 38-4 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-3620-28SC:admin#config igmp_proxy upstream_if vlan default router_ports add
3
Command: config igmp_proxy upstream_if vlan default router_ports add 3

```

```
Success.

DGS-3620-28SC:admin#
```

## 38-5 show igmp_proxy

### Description

This command displays IGMP proxy configuration information or group information on the switch. The display status item means group entry is determined by whether or not the chip is inserted.

### Format

**show igmp_proxy {group}**

### Parameters

**group** - (Optional) Specify the group information.

**Note:** If the **group** is not specified, the IGMP proxy configuration will be displayed.

### Restrictions

None.

### Example

To display IGMP proxy information:

```
DGS-3620-28SC:admin#show igmp_proxy
Command: show igmp_proxy

IGMP Proxy Global State          : Enabled

Upstream Interface
 VLAN ID                         : 1
 Dynamic Router Ports            : 1-4
 Static Router Ports             : 5-6
 Unsolicited Report Interval     : 10
 Source IP Address               : 0.0.0.0

Downstream Interface
 VLAN List                       : 2-4

DGS-3620-28SC:admin#
```

To display the IGMP proxy's group information:

```
DGS-3620-28SC:admin#show igmp_proxy group
Command: show igmp_proxy group

```

```
Dest-V : The destination VLAN.
A      : Active
I      : Inactive

Dest IP         Source IP    Dest-V     Member Ports     Status
----------- -------------    ------     ---------------- ---------
224.2.2.2       NULL            4            3,6            A
                                2            2-4            I
227.3.1.5       NULL            2            2,5,8          I
                                3            5,7,9          A
Total Entries: 2

DGS-3620-28SC:admin#
```

# Chapter 39 IGMP Snooping Commands

**config igmp_snooping** [vlan_name <vlan_name 32> | vlanid <vlanid_list> | all] {state [enable | disable] | fast_leave [enable | disable] | proxy_reporting {state [enable | disable] | source_ip <ipaddr>}(1)}(1)

**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**

**show igmp_snooping** {[vlan <vlan_name 32> | vlanid <vlanid_list>]}

**show igmp_snooping group** {[vlan <vlan_name 32> | vlanid <vlanid_list> | ports <portlist>] {<ipaddr>}}

**config igmp_snooping rate_limit** [ports <portlist> | vlanid <vlanid_list>] [<value 1-1000> | no_limit]

**show igmp_snooping rate_limit** [ports <portlist> | vlanid <vlanid_list>]

**create 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>

**delete igmp_snooping static_group** [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipaddr>

**show igmp_snooping static_group** {[vlan <vlan_name 32> | vlanid <vlanid_list>] <ipaddr>}

**show igmp_snooping statistic counter** [vlan <vlan_name 32> | vlanid <vlanid_list> | ports <portlist>]

**clear igmp_snooping statistics counter**

**show igmp_snooping forwarding** {[vlan <vlan_name 32> | vlanid <vlanid_list>]}

**show router_ports** [vlan <vlan_name 32> | vlanid <vlanid_list> | all] {[static | dynamic | forbidden]}

## 39-1 config igmp_snooping

### Description

This command is used to configure IGMP snooping on the switch.

### Format

**config igmp_snooping [vlan_name <vlan_name 32> | vlanid <vlanid_list> | all] {state [enable | disable] | fast_leave [enable | disable] | 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>** - Specify the VLAN name. The maximum length is 32 characters.

**vlanid** - Specify the VLAN ID list.
**<vlanid_list>** - Specify the VLAN ID list.

**all** - Specify to configure all VLANs.

**state** - Enable or disable IGMP snooping for the chosen VLAN.
**enable** - Enable IGMP snooping for the chosen VLAN.
**disable** - Disable IGMP snooping for the chosen VLAN.

**fast_leave** - Enable or disable the IGMP snooping fast leave function. If enabled, the membership is immediately removed when the system receive the IGMP leave message.
**enable** - Enable the IGMP snooping fast leave function.
**disable** - Disable the IGMP snooping fast leave function.

**proxy_reporting** - Specifies the proxy reporting option.
**state** - Specifies the proxy reporting state.
**enable** - Specifies that the proxy reporting option will be enabled.
**disable** - Specifies that the proxy reporting option will be disabled.

**source_ip** - Specifies the source IP address used.
**<ipaddr>** - Enter the source IP addres used here.

### Restrictions

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

### Example

To configure IGMP snooping:

```
DGS-3620-28SC:admin#config igmp_snooping vlan_name default state enable
fast_leave enable
Command: config igmp_snooping vlan_name default state enable fast_leave enable

Success.

DGS-3620-28SC:admin#
```

## 39-2 config igmp_snooping querier

### Description

This command is used to configure the IGMP snooping querier.

### 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>** - Specify the VLAN name. The maximum length is 32 characters.

**vlanid** - Specify the VLAN ID list.
**<vlanid_list>** - Specify the VLAN ID list.

**all** - Specify to configure all VLANs and VLAN IDs.

**query_interval** - Specify the amount of time in seconds between general query transmissions.
**<sec 1-65535>** - Specify the amount of time in seconds between general query transmissions. The default setting is 125 seconds.

**max_response_time** - Specify the maximum time in seconds to wait for reports from members.
**<sec 1-25>** - Specify the maximum time in seconds to wait for reports from members. The

default setting is 10 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:

1. 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).
2. 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).
3. 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.

**<value 1-7>** - Specify the value between 1 and 7. Increase the value if you expect a subnet to be lossy. The robustness variable is set to 2 by default.

**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.

**<sec 1-25>** - Specify the time between 1 and 25 seconds.

**state** - If the state is enable, it allows the switch to be selected as a IGMP Querier (sends IGMP query packets). If the state is disabled, then the switch can not play the role as a querier. Note that if the Layer 3 router connected to the switch provides only the IGMP proxy function but does not provide the multicast routing function, then this state must be configured as disabled. Otherwise, if the Layer 3 router is not selected as the querier, it will not send the IGMP query packet. Since it will not also send the multicast-routing protocol packet, the port will be timed out as a router port.

**enable** - Allows the switch to be selected as an IGMP Querier (sends IGMP query packets).

**disable** - When disabled, the switch can not play the role as a querier.

**version** - Specify the version of IGMP packet that will be sent by this port. If a IGMP packet received by the interface has a version higher than the specified version, this packet will be forward from the router's ports or VLAN flooding.

**<value 1-3>** - Specify the values between 1 and 3.

## Restrictions

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

## Example

To configure the IGMP snooping querier:

```
DGS-3620-28SC: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-3620-28SC:admin#
```

## 39-3 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.

### Format

**config router_ports [<vlan_name 32> | vlanid <vlanid_list>] [add | delete] <portlist>**

### Parameters

**<vlan_name 32>** - Specify the name of the VLAN on which the router port resides.

**vlanid** - Specify the VLAN ID list.
  **<vlanid_list>** - Specify the VLAN ID list.

**add** - Specify to add the router ports.

**delete** - Specify to delete the router ports.

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

### Restrictions

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

### Example

To set up static router ports:

```
DGS-3620-28SC:admin#config router_ports default add 1-10
Command: config router_ports default add 1-10

Success.

DGS-3620-28SC:admin#
```

## 39-4 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>** - Specify the name of the VLAN on which the router port resides.

**vlanid** - Specify the VLAN ID list.
  **<vlanid_list>** - Specify the VLAN ID list.

**add** - Specify to add the router ports.

**delete** - Specify to delete the router ports.

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

### Restrictions

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

### Example

To set up port range 1 to 7 to be forbidden router ports of the default VLAN:

```
DGS-3620-28SC:admin#config router_ports_forbidden default add 1-7
Command: config router_ports_forbidden default add 1-7

Success.

DGS-3620-28SC:admin#
```

## 39-5 enable igmp_snooping

### Description

This command allows you to enable IGMP snooping on the switch.

### Format

**enable igmp_snooping**

### Parameters

None.

### Restrictions

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

### Example

To enable IGMP snooping on the switch:

```
DGS-3620-28SC:admin#enable igmp_snooping
Command: enable igmp_snooping

Success.

DGS-3620-28SC:admin#
```

## 39-6 disable igmp_snooping

### Description

This command is used to disable IGMP snooping on the switch. IGMP snooping can be disabled only if IP multicast routing is not being used. Disabling IGMP snooping allows all IGMP and IP multicast traffic to flood within a given IP interface.

### Format

**disable igmp_snooping**

### Parameters

None.

### Restrictions

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

### Example

To disable IGMP snooping:

```
DGS-3620-28SC:admin#disable igmp_snooping
Command: disable igmp_snooping

Success.

DGS-3620-28SC:admin#
```

## 39-7 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 to display the IGMP snooping configuration.<br>**<vlan_name 32>** - Specify the name of the VLAN. The maximum length is 32 characters. |
| **vlanid** - (Optional) Specify the VLAN ID to display the IGMP snooping configuration.<br>**<vlanid_list>** - Specify a range of VLAN IDs. |

**Note:** If no parameter is specified, the system will display all current IGMP snooping configuration.

### Restrictions

None.

### Example

To show IGMP snooping:

```
DGS-3620-28SC:admin#show igmp_snooping
Command: show igmp_snooping

IGMP Snooping Global State               : Disabled

 VLAN Name                          : default
 Query Interval                     : 125
 Max Response Time                  : 10
 Robustness Value                   : 2
 Last Member Query Interval         : 1
 Querier State                      : Disabled
 Querier Role                       : Non-Querier
 Querier IP                         : 0.0.0.0
 Querier Expiry Time                : 0 secs
 State                              : Disabled
 Fast Leave                         : Disabled
 Rate Limit                         : No Limitation
 Proxy Reporting                    : Disabled
 Proxy Reporting Source IP          : 0.0.0.0
 Version                            : 3

Total Entries: 1

DGS-3620-28SC:admin#
```

## 39-8 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>}}**

### Parameters

**vlan** - (Optional) Specify the name of the VLAN for which you want to view IGMP snooping group configuration information.
**<vlan_name 32>** - Specify the VLAN name. The maximum length is 32 characters.

**vlanid** - (Optional) Specify the ID of the VLAN for which to view IGMP snooping group information.
**<vlanid_list>** - Specify the VLAN ID list.

**ports** - (Optional) Specify the list of ports for which to view IGMP snooping group information.

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

**<ipaddr>** - (Optional) Specify the group IP address for which to view IGMP snooping group information.

**Note:** If no parameter is specified, the system will display all of the current IGMP snooping group configuration of the switch.

### Restrictions

None.

### Example

To display IGMP snooping groups:

```
DGS-3620-28SC:admin#show igmp_snooping group
Command: show igmp_snooping group

 Source/Group   : NULL  / 224.106.0.211
 VLAN Name/VID  : default/1
 Member Ports   : 1
 UP Time        : 223
 Expiry Time    : 37
 Filter Mode    : EXCLUDE


 Source/Group   : NULL  / 234.54.163.75
 VLAN Name/VID  : default/1
 Member Ports   : 1
 UP Time        : 223
 Expiry Time    : 37
 Filter Mode    : EXCLUDE


 Source/Group   : 110.56.32.100 / 235.10.160.5
 VLAN Name/VID  : default/1
 Member Ports   : 2
 UP Time        : 221
 Expiry Time    : 10
 Filter Mode    : EXCLUDE


  Total Entries : 3

DGS-3620-28SC:admin#
```

## 39-9 config igmp_snooping rate_limit

### Description

This command is used to configure the upper limit per second for ingress IGMP control packets.

### 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>** - Specify a range of ports to be configured.

**vlanid** - Specify a range of VLANs to be configured.
**<vlanid_list>** - Specify the VLAN ID list.

**<value 1-1000>** - Specify the rate of IGMP control packets that the switch can process on a specific port/VLAN. The rate is specified in packet per second. The packets that exceed the limited rate will be dropped.

**no_limit** - The default setting is no limit.

### Restrictions

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

### Example

To configure the IGMP snooping rate limit for ports 1-2 to have no limit:

```
DGS-3620-28SC:admin#config igmp_snooping rate_limit ports 1-2 no_limit
Command: config igmp_snooping rate_limit ports 1-2 no_limit

Success.

DGS-3620-28SC:admin#
```

## 39-10 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 a range of ports to be displayed.
**<portlist>** - Specify a range of ports to be displayed.

**vlanid** - Specify a range of VLANs to be displayed.
**<vlanid_list>** - Specify the VLAN ID list.

### Restrictions

None.

### Example

To display the IGMP snooping rate limit for ports 1-2:

```
DGS-3620-28SC:admin#show igmp_snooping rate_limit ports 1-2
Command: show igmp_snooping rate_limit ports 1-2

Port      Rate Limit
--------  ------------
1              No Limit
2              No Limit

Total Entries: 2
DGS-3620-28SC:admin#
```

## 39-11 create igmp_snooping static_group

### Description

This command allows users to create an IGMP snooping static group. Member ports can be added to the static group. The static member and the dynamic member port form the member ports of a group. The static group will only take effect when IGMP snooping is enabled on the VLAN. For those static member ports, the device needs to emulate the IGMP protocol operation to the querier, and forward the traffic destined to the multicast group to the member ports. For a layer 3 device, the device is also responsible to route the packet destined for this specific group to static member ports. The static member port will only affect V2 IGMP operation. The Reserved IP multicast address 224.0.0.X must be excluded from the configured group.The VLAN must be created first before a static group can be created.

### Format

**create igmp_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipaddr>**

### Parameters

**vlan** - Specify the name of the VLAN on which the router port resides.
  **<vlan_name 32>** - Specify the VLAN name. The maximum length is 32 characters.

**vlanid** - Specify the VLAN ID list.
  **<vlanid_list>** - Specify the VLAN ID list.

**<ipaddr>** - Specify the multicast group IP address (for Layer 3 switch).

### Restrictions

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

### Example

To create an IGMP snooping static group on default VLAN, group 239.1.1.1:

```
DGS-3620-28SC: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-3620-28SC:admin#
```

## 39-12 config igmp_snooping static_group

### Description

This command is used to configure an IGMP snooping static group on the switch. When a port is configured as a static member port, the IGMP protocol will not operate on this port. Therefore, 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.<br>**<vlan_name 32>** - Specify the VLAN name. The maximum length is 32 characters. |
| **vlanid** - Specify the ID of the VLAN on which the static group resides.<br>**<vlanid_list>** - Specify the VLAN ID list. |
| **<ipaddr>** - Specify the multicast group IP address (for Layer 3 switch). |
| **add** - Specify to add the member ports. |
| **delete** - Specify to delete the member ports. |
| **<portlist>** - Specify a range of ports to be configured. |

### Restrictions

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

### Example

To add port 9 to 10 to be IGMP snooping static member ports for group 239.1.1.1 on default VLAN:

```
DGS-3620-28SC:admin#config igmp_snooping static_group vlan default 239.1.1.1
add 9-10
Command: config igmp_snooping static_group vlan default 239.1.1.1 add 9-10

Success.

DGS-3620-28SC:admin#
```

## 39-13 delete igmp_snooping static_group

### Description

This command is used to delete an IGMP snooping static group on the switch. 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 router port resides.
**<vlan_name 32>** - Specify the VLAN name. The maximum length is 32 characters.

**vlanid** - Specify the VLAN ID list on which the router port resides.
**<vlanid_list>** - Specify the VLAN ID list.

**<ipaddr>** - Specify the multicast group IP address (for Layer 3 switch).

### Restrictions

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

### Example

To delete an IGMP snooping static group from the default VLAN, group 239.1.1.1:

```
DGS-3620-28SC: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-3620-28SC:admin#
```

## 39-14 show igmp_snooping static_group

### Description

This command is used to display the IGMP snooping static multicast group.

### Format

**show igmp_snooping static_group {[vlan <vlan_name 32> | vlanid <vlanid_list>] <ipaddr>}**

### Parameters

**vlan** - Specify the name of the VLAN on which the router port resides.
**<vlan_name 32>** - Specify the VLAN name. The maximum length is 32 characters.

**vlanid** - Specify the VLAN ID list on which the router port resides.
**<vlanid_list>** - Specify the VLAN ID list.

**<ipaddr>** - Specify the multicast group IP address (for Layer 3 switch).

### Restrictions

None.

### Example

To display all the IGMP snooping static groups:

```
DGS-3620-28SC:admin#show igmp_snooping static_group
```

```
Command: show igmp_snooping static_group

VLAN ID/Name                            IP Address      Static Member Ports
---------------------------------------  --------------  --------------------
1/Default                               239.1.1.1       9-10

Total Entries : 1

DGS-3620-28SC:admin#
```

## 39-15 show igmp_snooping statistic counter

### Description

This command is used to display the IGMP snooping statistics counter for IGMP protocol packets that are transmitted or received by the switch since IGMP snooping was enabled.

### Format

**show igmp_snooping statistic counter [vlan <vlan_name 32> | vlanid <vlanid_list> | ports <portlist>]**

### Parameters

**vlan** - Specify a VLAN to be displayed.
  **<vlan_name 32>** - Specify the VLAN name. The maximum length is 32 characters.

**vlanid** - Specify a list of VLANs to be displayed.
  **<vlanid_list>** - Specify the VLAN ID list.

**ports** – Specify a list of ports to be displayed.
  **<portlist>** - Specify a list of ports.

### Restrictions

None.

### Example

To display the IGMP snooping statistics counter for port 1:

```
DGS-3620-28SC: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                    : 8
      Total                            : 8

    Report & Leave
      IGMP v1 Report                   : 0
      IGMP v2 Report                   : 0
      IGMP v3 Report                   : 0
      IGMP v2 Leave                    : 0
      Total                            : 0

 Total Entries : 1
DGS-3620-28SC:admin#
```

## 39-16 clear igmp_snooping statistics counter

### Description

This command is used to clear the IGMP snooping statistics counter on the switch.

### Format

**clear igmp_snooping statistics counter**

### Parameters

None.

### Restrictions

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

### Example

To clear the IGMP snooping statistic counter:

```
DGS-3620-28SC:admin#clear igmp_snooping statistics counter
Command: clear igmp_snooping statistics counter

Success.

DGS-3620-28SC:admin#
```

## 39-17 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 comes from in terms of specific sources. The packets come from the source VLAN. They will be forwarded to the forwarding ports.

### Format

**show igmp_snooping forwarding {[vlan <vlan_name 32> | vlanid <vlanid_list>]}**

### Parameters

**vlan** - (Optional) Specify a VLAN to be displayed.
**<vlan_name 32>** - Specify the VLAN name. The maximum length is 32 characters.

**vlanid** - (Optional) Specify a list of VLANs to be displayed.
**<vlanid_list>** - Specify the VLAN ID list.

**Note:** If no parameter is specified, the system will display all current IGMP snooping forwarding table entries of the switch.

### Restrictions

None.

### Example

To display all IGMP snooping forwarding entries located on the switch:

```
DGS-3620-28SC:admin#show igmp_snooping forwarding
Command: show igmp_snooping forwarding

VLAN Name      : default
Source IP      : 10.90.90.114
Multicast Group: 225.0.0.0
Port Member    : 2,7

VLAN Name      : default
Source IP      : 10.90.90.10
Multicast Group: 225.0.0.1
Port Member    : 2,5

Total Entries : 2
```

```
DGS-3620-28SC:admin#
```

## 39-18 show router_ports

### Description

This command is used to display the current 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>** - Specify the VLAN name. The maximum length is 32 characters.

**vlanid** - Specify the ID of the VLAN on which the router port resides.
    **<vlanid_list>** - Specify the VLAN ID list.
    **all** – Specifies that all the VLAN's will be displayed.

**static** - (Optional) Display router ports that have been statically configured.

**dynamic** - (Optional) Display router ports that have been dynamically registered.

**forbidden** - (Optional) Display forbidden router ports that have been statically configured.

✎ **Note:** If no parameter is specified, the system will display all the current router ports on the Switch.

### Restrictions

None.

### Example

To display the router ports on the default VLAN:

```
DGS-3620-28SC:admin#show router_ports vlan default
Command: show router_ports vlan default

VLAN Name                : default
Static Router Port       :
Dynamic Router Port      :
Router IP                :
Forbidden Router Port    :

Total Entries: 1

DGS-3620-28SC:admin#
```

# Chapter 40 IGMP Snooping Multicast (ISM) VLAN Commands

| |
|---|
| **create igmp_snooping multicast_vlan** <vlan_name 32> <vlanid 2-4094> {remap_priority [<value 0-7> \| none] {replace_priority}} |
| **config igmp_snooping multicast_vlan** <vlan_name 32> {[add \| delete] [member_port <portlist> \| [source_port <portlist> \| untag_source_port <portlist>] \| tag_member_port <portlist>] \| state [enable \| disable] \| replace_source_ip <ipaddr> \| remap_priority [<value 0-7> \| none] {replace_priority}}(1) |
| **create igmp_snooping multicast_vlan_group_profile** <profile_name 1-32> |
| **config igmp_snooping multicast_vlan_group_profile** <profile_name 1-32> [add \| delete] <mcast_address_list> |
| **delete igmp_snooping multicast_vlan_group_profile** [profile_name <profile_name 1-32> \| all] |
| **show igmp_snooping multicast_vlan_group_profile** {<profile_name 1-32>} |
| **config igmp_snooping multicast_vlan_group** <vlan_name 32> [add \| delete] profile_name <profile_name 1-32> |
| **show igmp_snooping multicast_vlan_group** {<vlan_name 32>} |
| **delete igmp_snooping multicast_vlan** <vlan_name 32> |
| **enable igmp_snooping multicast_vlan** |
| **disable igmp_snooping multicast_vlan** |
| **show igmp_snooping multicast_vlan** {<vlan_name 32>} |
| **config igmp_snooping multicast_vlan forward_unmatched** [disable \| enable] |

## 40-1 create igmp_snooping multicast_vlan

### Description

This command is used to create an IGMP snooping multicast VLAN and implements relevant parameters as specified. More than one multicast VLAN can be configured. 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 and 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>** - Specify 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>** - Specify the VLAN ID of the multicast VLAN to be created. The range is from 2 to 4094. |
| **remap_priority** - (Optional) Specify the remap priority that will be used.<br>**<value 0-7>** - Specify 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 Administrator, Operator and Power-User level users can issue this command.

### Example

To create an IGMP snooping multicast VLAN with the VLAN name mv1 and the VID 2:

```
DGS-3620-28SC:admin#create igmp_snooping multicast_vlan mv1 2
Command: create igmp_snooping multicast_vlan mv1 2

Success.

DGS-3620-28SC:admin#
```

## 40-2 config igmp_snooping multicast_vlan

### Description

This command is used to configure IGMP 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 igmp_snooping multicast_vlan** command before the multicast VLAN can be configured.

### Format

**config igmp_snooping multicast_vlan <vlan_name 32> {[add | delete] [member_port <portlist> | [source_port <portlist> | untag_source_port <portlist>] | tag_member_port <portlist>] | state [enable | disable] | replace_source_ip <ipaddr> | remap_priority [<value 0-7> | none] {replace_priority}} (1)**

### Parameters

**<vlan_name 32>** - Specify 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>** - Specify a range of ports to be configured.

**source_port** - Specify source port where the multicast traffic is entering the Switch.
**<portlist>** - Specify 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>** - Specify a range of ports to be configured.

**tag_member_port** - Specify the tagged member port of the multicast VLAN.

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

**state** - (Optional) 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_ip** - With the IGMP snooping function, the IGMP 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 use “0” IP address.
**<ipaddr>** - Enter the IP address here.

**remap_priority** - Specify the remap priority here.
**<value 0-7>** - The remap priority value (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 is used. The default setting is 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 Administrator, Operator and Power-User level users can issue this command.

### Example

To configure an IGMP snooping multicast VLAN with the name “v1”, make ports 1 and 3 members of the VLAN, and set the state to enable:

```
DGS-3620-28SC:admin#config igmp_snooping multicast_vlan v1 add member_port 1,3
state enable
Command: config igmp_snooping multicast_vlan v1 add member_port 1,3 state
enable

Success.

DGS-3620-28SC:admin#
```

## 40-3 create igmp_snooping multicast_vlan_group_profile

### Description

This command is used to create a multicast group profile. The profile name for IGMP snooping must be unique.

### Format

**create igmp_snooping multicast_vlan_group_profile <profile_name 1-32>**

### Parameters

**<profile_name 1-32>** - Specifies the multicast VLAN profile name. The maximum length is 32 characters.

### Restrictions

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

### Example

To create an IGMP snooping multicast group profile with the name “Knicks”:

```
DGS-3620-28SC:admin#create igmp_snooping multicast_vlan_group_profile Knicks
Command: create igmp_snooping multicast_vlan_group_profile Knicks

Success.

DGS-3620-28SC:admin#
```

## 40-4 config igmp_snooping multicast_vlan_group_profile

### Description

This command is used to configure an IGMP snooping multicast group profile on the switch and to add or delete multicast addresses for a profile.

### Format

**config igmp_snooping multicast_vlan_group_profile <profile_name 1-32> [add | delete] <mcast_address_list>**

### Parameters

**<profile_name 32>** - Specify 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.

**<mcast_address_list>** - Specify a multicast address list. This 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 types, such as 225.1.1.1, 225.1.1.18-225.1.1.20.

### Restrictions

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

### Example

To add the single multicast address 225.1.1.1 and multicast range 225.1.1.10-225.1.1.20 to the IGMP snooping multicast VLAN profile named “Knicks”:

```
DGS-3620-28SC:admin#config igmp_snooping multicast_vlan_group_profile Knicks
add 225.1.1.1, 225.1.1.10-225.1.1.20
Command: config igmp_snooping multicast_vlan_group_profile Knicks add
225.1.1.1, 225.1.1.10-225.1.1.20

Success.

DGS-3620-28SC:admin#
```

## 40-5 delete igmp_snooping multicast_vlan_group_profile

### Description

This command is used to delete an existing IGMP snooping multicast group profile on the switch. Specify a profile name to delete it.

### Format

**delete igmp_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>** - The profile file can be up to 32 characters long.
**all** - Specify to delete all the profiles.

If no parameter is specified, the system will display all multicast VLAN group profiles.

### Restrictions

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

### Example

To delete an IGMP snooping multicast group profile named “Knicks”:

```
DGS-3620-28SC:admin#delete igmp_snooping multicast_vlan_group_profile
profile_name Knicks
Command: delete igmp_snooping multicast_vlan_group_profile profile_name Knicks

Success.

DGS-3620-28SC:admin#
```

## 40-6 show igmp_snooping multicast_vlan_group_profile

### Description

This command is used to display an IGMP snooping multicast group profile.

### Format

**show igmp_snooping multicast_vlan_group_profile {<profile_name 1-32>}**

### Parameters

**<profile_name 1-32>** - (Optional) Specify the multicast VLAN profile name. The maximum length is 32 characters.

If no parameter is specified, the system will display all multicast VLAN group profiles.

### Restrictions

None.

### Example

To display all IGMP snooping multicast VLAN profiles:

```
DGS-3620-28SC:admin#show igmp_snooping multicast_vlan_group_profile
Command: show igmp_snooping multicast_vlan_group_profile

Profile Name              Multicast Addresses
-----------------------  --------------------------------
Knicks                   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-3620-28SC:admin#
```

## 40-7 config igmp_snooping multicast_vlan_group

### Description

This command is used to configure the multicast group which will be learned with the specific multicast VLAN. There are two cases that need to be considered. For the first case, suppose that a multicast group is not configured and multicast VLANs do not have overlapped member ports. That means the join packets received by the member port will only be learned with the multicast VLAN that this port belongs to. If not, which is the second case, the join packet will be learned with the multicast VLAN that contains the destination multicast group. If the destination multicast group of the join packet can not be classified into any multicast VLAN that this port belongs to, then the join packet will be learned with the natural VLAN of the packet. Please note that the same profile can not overlap different multicast VLANs. Multiple profiles can be added to a multicast VLAN, however.

### Format

**config igmp_snooping multicast_vlan_group <vlan_name 32> [add | delete] profile_name <profile_name 1-32>**

### Parameters

| |
|---|
| **<vlan_name 32>** - Specify the name of the multicast VLAN to be configured. Each multicast VLAN is given a name that can be up to 32 characters.<br>**add** - Specify to associate a profile to a multicast VLAN.<br>**delete** - Specify to de-associate a profile from a multicast VLAN. |
| **profile_name** - Specifies the multicast VLAN profile name. The maximum length is 32 characters.<br>**<profile_name>** - The profile name can be up to 32 characters long. |

### Restrictions

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

### Example

To add an IGMP snooping profile to a multicast VLAN group with the name “v1”:

```
DGS-3620-28SC: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-3620-28SC:admin#
```

## 40-8 show igmp_snooping multicast_vlan_group

### Description

This command allows group profile information for a specific multicast VLAN to be displayed.

### Format

**show igmp_snooping multicast_vlan_group {<vlan_name 32>}**

### Parameters

**<vlan_name 32>** - (Optional) Specify the name of the group profile’s multicast VLAN to be displayed.

If no parameter is specified, the system will display all multicast VLAN groups.

### Restrictions

None.

### Example

To display all IGMP snooping multicast VLANs’group profile information:

```
DGS-3620-28SC:admin#show igmp_snooping multicast_vlan_group
Command: show igmp_snooping multicast_vlan_group


VLAN Name                         VLAN ID        Multicast Group Profiles
-------------------------------   -------   ---------------------------------
test2                             20

test1                             100


DGS-3620-28SC:admin#
```

## 40-9 delete igmp_snooping multicast_vlan

### Description

This command is used to delete an IGMP snooping multicast VLAN.

### Format

**delete igmp_snooping multicast_vlan <vlan_name 32>**

### Parameters

**<vlan_name 32>** - Specify the name of the multicast VLAN to be deleted.

### Restrictions

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

### Example

To delete an IGMP snooping multicast VLAN called “v1”:

```
DGS-3620-28SC:admin#delete igmp_snooping multicast_vlan v1
Command: delete igmp_snooping multicast_vlan v1

Success.

DGS-3620-28SC:admin#
```

## 40-10 enable igmp_snooping multicast_vlan

### Description

This command is used to enable the IGMP snooping multicast VLAN function. By default, the multicast VLAN is disabled.

### Format

**enable igmp_snooping multicast_vlan**

### Parameters

None.

### Restrictions

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

### Example

To enable IGMP snooping multicast VLAN:

```
DGS-3620-28SC:admin#enable igmp_snooping multicast_vlan
Command: enable igmp_snooping multicast_vlan

Success.

DGS-3620-28SC:admin#
```

## 40-11 disable igmp_snooping multicast_vlan

### Description

This command is used to disable the IGMP snooping multicast VLAN function. By default, the multicast VLAN is disabled.

### Format

**disable igmp_snooping multicast_vlan**

### Parameters

None.

### Restrictions

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

### Example

To disable IGMP snooping multicast VLAN:

```
DGS-3620-28SC:admin#disable igmp_snooping multicast_vlan
Command: disable igmp_snooping multicast_vlan

Success.

DGS-3620-28SC:admin#
```

## 40-12 show igmp_snooping multicast_vlan

### Description

This command allows information for a specific multicast VLAN to be displayed.

### Format

**show igmp_snooping multicast_vlan {<vlan_name 32>}**

### Parameters

**<vlan_name 32>** - (Optional) Specify the name of the multicast VLAN to be displayed.

If no parameter is specified, the system will display all multicast VLANs.

### Restrictions

None.

### Example

To display all IGMP snooping multicast VLANs:

```
DGS-3620-28SC:admin#show igmp_snooping multicast_vlan
Command: show igmp_snooping multicast_vlan

IGMP Multicast VLAN Global State        : Disabled
IGMP Multicast VLAN Forward Unmatched   : Disabled

VLAN Name                 :test
VID                       :100

Member(Untagged) Ports     :1
Tagged Member Ports        :
Source Ports               :3
Untagged Source Ports      :
Status                     :Disabled
Replace Source IP          :0.0.0.0
Remap Priority             :None

Total Entries: 1

DGS-3620-28SC:admin#
```

## 40-13 config igmp_snooping multicast_vlan forward_unmatched

### Description

This command is used to configure the forwarding mode for IGMP snooping 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

**enable** - The packet will be flooded on the VLAN.

**disable** - The packet will be dropped.

## Restrictions

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

## Example

To configure the forwarding mode for IGMP snooping multicast VLAN unmatched packets:

```
DGS-3620-28SC:admin#config igmp_snooping multicast_vlan forward_unmatched
enable
Command: config igmp_snooping multicast_vlan forward_unmatched enable

Success.

DGS-3620-28SC:admin#
```

# Chapter 41 IP Multicasting Commands

|  |
|---|
| **show ipmc** {ipif <ipif_name 12> \| protocol [inactive \| dvmrp \| pim]} |
| **show ipmc cache** {group <group>} {ipaddress <network_address>} |

## 41-1 show ipmc

### Description

This command is used to display the IP Multicast interface table.

### Format

**show ipmc {ipif <ipif_name 12> | protocol [inactive | dvmrp | pim]}**

### Parameters

|  |
|---|
| **ipif** - (Optional) Specifies the IP interface name used.<br>**<ipif_name 12>** - Enter the IP interface name used here. This name can be up to 12 characters long. |
| **protocol** - (Optional) Specifies which kind of routing protocol interface table will be displayed.<br>**inactive** - Specifies that the protocol display will be inactive.<br>**dvmrp** - Specifies that the DVMRP protocol will be displayed.<br>**pim** - Specifies that the PIM protocol will be displayed. |

If no parameter is specified, the system will display all IP multicast interfaces.

### Restrictions

None.

### Example

To display the IP Multicast interface table:

```
DGS-3620-28SC:admin# show ipmc
Command: show ipmc

Interface    IP Address         Multicast Routing
-----------  -----------------  -----------------
System       10.90.90.90        INACT
n1           1.3.2.3            PIM-SM
n2           2.3.2.3            PIM-SM-DM
n3           3.3.2.3            PIM-DM
n4           4.3.2.3            DVMRP

Total Entries : 5

DGS-3620-28SC:admin#
```

## 41-2 show ipmc cache

### Description

This command is used to display the IP multicast forwarding cache.

### Format

**show ipmc cache {group <group>} {ipaddress <network_address>}**

### Parameters

| |
|---|
| **group** - (Optional) Specifies the multicast group.<br>**<group>** - Enter the multicast group used here. |
| **ipaddress** - (Optional) Specifies the IP address used.<br>**<network_address>** - Enter the IP address used here. |

If no parameter is specified, the system will display all IP multicast forwarding cache entries.

### Restrictions

None.

### Example

To display the IP multicast forwarding cache:

```
DGS-3620-28SC:admin# show ipmc cache
Command: show ipmc cache

Multicast        Source             Upstream     Expire   Routing
Group            Address/Netmask    Neighbor     Time     Protocol
---------------  -----------------  -----------  -------  -----------
224.1.1.1        10.48.74.121/8     10.48.75.63  30       DVMRP
224.1.1.1        20.48.74.25/8      20.48.75.25  20       PIM-DM
224.1.2.3        10.48.75.3/8       10.48.76.6   30       DVMRP

Total Entries : 3

DGS-3620-28SC:admin#
```

# Chapter 42 IP Route Filter Commands

**create ip prefix_list** <list_name 16>

**config ip prefix_list** <list_name 16> [[add | delete] {sequence <value 1-65535>} <network_address> {ge <value 1-32>} {le <value 1-32>} [deny | permit] | [description <desc 80> | clear_description]]

**delete ip prefix_list** [list_name <list_name 16> | all]

**show ip prefix_list** {<list_name 16>}

**create ip standard access_list** <list_name 16>

**config ip standard access_list** <list_name 16> [add | delete] <network_address> [deny | permit]

**delete ip standard access_list** [list_name <list_name 16> | all]

**show ip standard access_list** {<list_name 16>}

**clear ip prefix_list counter** [<list_name 16> {<network_address>} | all]

**create route_map** <map_name 16>

**config route_map** <map_name 16> [[add | delete] sequence <value 1-65535> {[deny | permit]} | sequence <value 1-65535> [match [add | delete] [as_path <list_name 16> | community_list <list_name 16> {exact} | ip [next_hop | address] {prefix_list} <list_name 16> | metric <uint 0-4294967294>] | set [add | delete] [next_hop [<ipaddr> | peer_address] | metric <uint 0-4294967294> | local_preference <uint 0-4294967295> | weight <value 0-65535> | as_path <aspath_list> | community {community_set <community_set 80> | internet | no_export | no_advertise | local_as} {additive} | origin [egp | igp | incomplete] | dampening <min 1-45> <value 1-20000> <value 1-20000> <min 1-255> <min 1-45>]]]

**delete route_map** [map_name <map_name 16> {all_seqence} | all]

**show route_map** {<map_name 16>}

## 42-1 create ip prefix_list

### Description

This command is used to create an IP prefix list that can be further applied to routes as a filter list.

### Format

**create ip prefix_list <list_name 16>**

### Parameters

**<list_name 16> -** Specifies the name to identify the prefix list.

### Restrictions

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

### Example

To creates one IP prefix list named 1:

```
DGS-3620-28SC:admin# create ip prefix_list 1
Command:  create ip prefix_list 1

Success.

DGS-3620-28SC:admin#
```

## 42-2 config ip prefix_list

### Description

This command defines the rule entry for an IP route prefix list.

A prefix list can have multiple rule entries; each is represented by a sequence number. The rule with the lower sequence number will be evaluated first. If the sequence number is not specified for the defined rule entry, the sequence number will be automatically given. The automatically given sequence number will be a multiple of 5. Therefore, if the defined rule is the first rule in the prefix list, the automatically given sequence number will be 5. If the defined rule is not the first rule in the prefix list, the sequence number will be the number that is a multiple of 5 and larger than the largest sequence number of an existing rule in the prefix list.

A prefix list consists of an IP address and a bit mask. The bit mask is entered as a number from 1 to 32. An implicit denial is applied to traffic that does not match any prefix list entry.

The IP route prefix list rule entry is defined to either permit or deny specific routes. Prefix lists are configured to match an exact prefix length or a prefix range. The prefix list is processed using an exact match when neither the **ge** nor **le** keyword is entered. If only the **ge** value is entered, the range is the value entered for the **ge** ge-length argument to a full 32-bit length. If only the **le** value is entered, the range is from the value entered for the network/length argument to the **le** le-length argument. If both the **ge** ge-length and **le** le-length keywords and arguments are entered, the range falls between the values used for the ge-length and le-length arguments.

The following formula is a restriction for the specified ge-length and le-length.

***network/length < ge ge-length < le le-length <= 32***

As an example, if the configured network address is 10.1.2.3/16, only the route 10.1.0.0/16 will match the rule. The route 10.1.2.0/24 will not match the rule.

As another example, if 10.1.0.0/16 ge 24 is configured, then the route 10.1.0.0/16 will not match the rule. The route 10.1.2.0/24 will match the rule. The route 10.1.2.3/32 will also match the rule.

### Format

**config ip prefix_list <list_name 16> [[add | delete] {sequence <value 1-65535>} <network_address> {ge <value 1-32>} {le <value 1-32>} [deny | permit] | [description <desc 80> | clear_description]]**

### Parameters

| |
|---|
| **<list_name 16>** - Specifies the name for the prefix list. |
| **add** - Specifies to add a rule entry.<br>**delete** - Specifies to delete a rule entry. |
| **sequence** - (Optional) Specifies the sequence number for the rule entry.<br>**<value 1-65535>** - Enter the sequence number for the rule entry here. This value must be between 1 and 65535. |

**<network_address>** - Specifies the network address used.

**ge** - (Optional) Specifies the minimum prefix length to be matched.
**<value 1-32>** - Enter the 'ge' value used here. This value must be between 1 and 32.

**le** - (Optional) Specifies the maximum prefix length to be matched.
**<value 1-32>** - Enter the 'le' value used here. This value must be between 1 and 32.

**deny** - Specifies that the network will be denied.
**permit** - Specifies that the network will be permitted.

**description** - Specifies the description for the prefix list used.
**<desc 80>** - Enter the description used here. This value can be up to 80 characters long.
**clear_description** - Specifies that the description for the prefix list will be cleared.

### Restrictions

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

### Example

The following example configures a prefix list 1 to permit routes from the 10.0.0.0/8 network that have a mask length that is less than or equal to 24 bits:

```
DGS-3620-28SC:admin# config ip prefix_list 1 add 10.0.0.0/8 le 24 permit
Command:  config ip prefix_list 1 add 10.0.0.0/8 le 24 permit

Success.

DGS-3620-28SC:admin#
```

## 42-3 delete ip prefix_list

### Description

This command is used to delete the IP prefix list

### Format

**delete ip prefix_list [list_name <list_name 16> | all]**

### Parameters

**list_name** - Specifies the prefix list name that will be deleted.
**<list_name 16>** - Enter the prefix list name that will be deleted here. This name must be 16 characters long.
**all** - Specifies that all the entries will be deleted.

### Restrictions

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

### Example

To delete an IP prefix list named “list1”:

```
DGS-3620-28SC:admin# delete ip prefix_list list_name list1
Command: delete ip prefix_list list_name list1

Success.

DGS-3620-28SC:admin#
```

## 42-4 show ip prefix_list

### Description

This command is used to show an IP prefix list.

### Format

**show ip prefix_list {<list_name 16>}**

### Parameters

**<list_name 16>** - (Optional) Enter the prefix list name that will be displayed here. This name must be 16 characters long.

### Restrictions

None.

### Example

This example shows an IP prefix list named ”list1”:

```
DGS-3620-28SC:admin# show ip prefix_list list1
Command: show ip prefix_list list1

IP Prefix list:  list1
Description:
Total Rule Number:1
     sequence 5 permit 10.0.0.0/8 le 24

DGS-3620-28SC:admin#
```

## 42-5 create ip standard access_list

### Description

This command is used to create an access list used to filter routes.

### Format

**create ip standard access_list <list_name 16>**

### Parameters

**<list_name 16>** - Enter the name of the access list used here. This name can be up to 16 characters long.

### Restrictions

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

### Example

To create an access list named “List1”:

```
DGS-3620-28SC:admin# create ip standard access_list List1
Command:  create ip standard access_list List1

Success.

DGS-3620-28SC:admin#
```

## 42-6 config ip standard access_list

### Description

This command is used to configure an access list to add or delete an entry.

### Format

**config ip standard access_list <list_name 16> [add | delete] <network_address> [deny | permit]**

### Parameters

**<list_name 16>** - Enter the name of the access list used here. This name can be up to 16 characters long.

**add** - Specifies to add a network address in the access list.
**delete** - Specifies to delete a network address from the access list.

**<network_address>** - Specifies the network address that will work as the filter condition for the access list.

**deny** - Specifies that the network matched will be denied.
**permit** - Specifies that the network matched will be permitted.

### Restrictions

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

### Example

This example configures access list “List1” to add one entry:

```
DGS-3620-28SC:admin# config ip standard access_list List1 add 10.10.10.0/24
permit
Command:  config ip standard access_list List1 add 10.10.10.0/24 permit

Success.

DGS-3620-28SC:admin#
```

## 42-7 delete ip standard access_list

### Description

This command is used to delete an access list used from the route filters.

### Format

**delete ip standard access_list [list_name <list_name 16> | all]**

### Parameters

**list_name** - Specifies the name of the access list used.

**<list_name 16>** - Enter the name of the access list used here. This name can be up to 16 characters long.

**all** - Specifies that all the access list will be deleted.

### Restrictions

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

### Example

To delete an access list with the name ”List1”:

```
DGS-3620-28SC:admin# delete ip standard access_list list_name List1
Command: delete ip standard access_list list_name List1

Success.

DGS-3620-28SC:admin#
```

## 42-8 show ip standard access_list

### Description

This command is used to display the information of an access list.

### Format

**show ip standard access_list {<list_name 16>}**

### Parameters

**<list_name 16>** - (Optional) Enter the name of the access list used here. This name can be up to 16 characters long.

If no parameter is specified, all access lists on the Switch will be displayed.

### Restrictions

None.

### Example

To display the information of an access list named “List1”:

```
DGS-3620-28SC:admin#show ip standard access_list List1
Command: show ip standard access_list List1

IP standard Access_list:   List1
Total entries number   :   1
      filter : permit 10.1.1.1/8

DGS-3620-28SC:admin#
```

## 42-9 clear ip prefix_list counter

### Description

This command is used to clear prefix list hit counters. The hit count is a value indicating the number of matches to a specific prefix list entry.

### Format

**clear ip prefix_list counter [<list_name 16> {<network_address>} | all]**

### Parameters

**<list_name 16>** - Enter the name of the prefix list from which the hit count is to be cleared. This name can be up to 16 characters long.

**<network_address>** - (Optional) Enter the IPv4 network address used here that will be used to clear the hit count.

**all** - Specifies that all the prefix list counters will be cleared.

### Restrictions

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

### Example

To clear prefix list counters for the prefix list named “first_list” that matches the 192.168.10.0/24 prefix:

```
DGS-3620-28SC:admin# clear ip prefix_list counter list_name 192.168.10.0/24
Command: clear ip prefix_list counter list_name 192.168.10.0/24

Success.

DGS-3620-28SC:admin#
```

## 42-10 create route_map

### Description

This command is used to create a route map or add/delete sequences to a route map. A route map can have multiple rule entries, each with a different sequence number. When creating a route map, a sequence ID of 10 will be added to the route map. If the sequence number is not specified, it will be automatically given. The automatically given sequence number will be a multiple of 10.

### Format

**create route_map <map_name 16>**

### Parameters

**<map_name 16>** - Enter the route map name used here. This name can be up to 16 characters long.

### Restrictions

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

### Example

To create a route map named "map1" and add one sequence ID of 5 to the route map:

```
DGS-3620-28SC:admin# create route_map map1
Command: create route_map map1

Success.

DGS-3620-28SC:admin#
```

## 42-11 config route_map

### Description

This command is used to configure the route map. A route map can have multiple rule entries, each with a different sequence number. When creating a route map, a sequence ID of 10 will be added to the route map. If the sequence number is not specified, it will be automatically given. The automatically given sequence number will be a multiple of 10. If neither permit nor deny is specified, permit is implied.

## Format

**config route_map <map_name 16> [[add | delete] sequence <value 1-65535> {[deny | permit]} | sequence <value 1-65535> [match [add | delete] [as_path <list_name 16> | community_list <list_name 16> {exact} | ip [next_hop | address] {prefix_list} <list_name 16> | metric <uint 0-4294967294>] | set [add | delete] [next_hop [<ipaddr> | peer_address] | metric <uint 0-4294967294> | local_preference <uint 0-4294967295> | weight <value 0-65535> | as_path <aspath_list> | community {community_set <community_set 80> | internet | no_export | no_advertise | local_as} {additive} | origin [egp | igp | incomplete] | dampening <min 1-45> <value 1-20000> <value 1-20000> <min 1-255> <min 1-45>]]]**

## Parameters

| |
|---|
| **<map_name 16>** - Enter the route map name used here. This name can be up to 16 characters long. |
| **add** - Specifies to add a sequence entry.<br>**delete** - Specifies to remove a sequence entry. |
| **sequence** - Specifies the sequence number for the route map rule.<br>**<value 1-65535>** - Enter the sequence number used here. This value must be between 1 and 65535. |
| **deny** - (Optional) Specifies to deny the route if the rule is matched.<br>**permit** - (Optional) Specifies to permit the route if the rule is matched. |
| **sequence** - Specifies the sequence number for the route map rule.<br>**<value 1-65535>** - Enter the sequence number used here. This value must be between 1 and 65535. |
| **match** - Specifies to check if the sequence entry matches.<br>**add** - Specifies the entry or the set to add.<br>**delete** - Specifies the entry or the set to delete. |
| **as_path** - Specifies to match the AS path of the route against the AS path list. The AS path list specified here needs to be a sub-list of the AS path list associated with the route.<br>**<list_name 16>** - Enter the AS path name used here. This name can be up to 16 characters long. |
| **community_list** - Specifies to match the community of the route against the community string.<br>**<list_name 16>** - Enter the community list name used here. This name can be up to 16 characters long. |
| **exact** - (Optional) Specifies that all of the communities and only those communities specified must be present. |
| **ip** - Specifies to match the route according to the access list.<br>**next_hop** - Specifies to match the next hop of the route according to the access list.<br>**address** - Specifies to match the route according to the access list.<br>**prefix_list** - (Optional) Specifies to match the route according to the prefix list.<br>**<list_name 16>** - Enter the prefix list name used here. This name can be up to 16 characters long. |
| **metric** - Specifies to match the metric of the route.<br>**<uint 0-4294967294>** - Enter the metric value used here. This value must be between 0 and 4294967294. |
| **set** - Specifies to define the conditions for redistributing routes from one routing protocol into another.<br>**add** - Specifies the set to add.<br>**delete** - Specifies the set to delete. |
| **next_hop** - Specifies the next hop attribute.<br>**<ipaddr>** - Specifies the IP address to set.<br>**peer_address** - This will take effect for both the ingress and egress directions. When set to next_hop to peer address, for ingress direction, the next hop will be set to the neighbor peer address. For egress direction, the next hop associated with the route in the packet will be the neighbor peer address. |
| **metric** - Specifies to set the metric.<br>**<uint 0-4294967294>** - Enter the metric value used here. This value must be between 0 and |

4294967294.

**local_preference** - Specifies to set the local preference for the matched route.
**<uint 0-4294967295>** - Enter the local preference value used here. This value must be between 0 and 4294967295.

**weight** - Set the weight for the matched routes. It will overwrite the weight specified by the neighbor weight command for the routes received from the neighbor. If weight is neither specified by the neighbor weight command nor set by the route map, then routes learned through another BGP peer have a default weight of 0. This will only take effect for ingress direction.
**<value 0-65535>** - Enter the weight value used here. This value must be between 0 and 65535. The default value is 32768.

**as_path** - Specifies an AS path list which is used to prepend the AS list.
**<aspath_list>** - Enter the AS path list value used here.

**community** - Specifies a community to be used or to be appended to the original communities of the route.
**community_set** - Specifies a community set used.
**<community_set 80>** - Enter the community set value used here. This value can be up to 80 characters long.
**internet** - Specifies that routes with this community will be sent to all peers either internal or external.
**no_export** - Specifies that routes with this community will be sent to peers in the same AS or in other sub autonomous systems within a confederation, but will not be sent to an external BGP (eBGP) peer.
**no_advertise** - Specifies that routes with this community will not be advertised to any peer either internal or external.
**local_as** - Specifies that routes with this community will be sent to peers in the same AS, but will not be sent to peers in other sub-AS's in the same confederation and to the external peers.

**additive** - (Optional) Specifies that the community string will be appended to the original community string. If not specified, the specified community string will replace the original community string.

**origin** - Specifies to set the origin for the route.
**egp** - Specifies that the origin for the route will be set to EGP.
**igp** - Specifies that the origin for the route will be set to IGP.
**incomplete** - Specifies that the origin for the route will be set to 'incomplete'.

**dampening** - Specifies the dampening timer and parameter used.
**<min 1-45>** - Enter the dampening time used here. This value must be between 1 and 45 minutes.
**<value 1-20000>** - Enter the dampening parameter value here. This value must be beteen 1 and 20000.
**<value 1-20000>** - Enter the dampening parameter value here. This value must be beteen 1 and 20000.
**<min 1-255>** - Enter the dampening time used here. This value must be between 1 and 255 minutes.
**<min 1-45>** - Enter the dampening time used here. This value must be between 1 and 45 minutes.

## Restrictions

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

## Example

To configure a route map named “map1” and add one sequence ID of 20 to the route map:

```
DGS-3620-28SC:admin# config route_map map1 add sequence 20
Command: config route_map map1 add sequence 20

Success.

DGS-3620-28SC:admin#
```

To configure the route map match access list “ac_list1” and set the metric to 50:

```
DGS-3620-28SC:admin# config route_map map1 sequence 10 set add metric 50
Command: config route_map map1 sequence 10 set add metric 50

Success.

DGS-3620-28SC:admin# config route_map map1 sequence 10 set add dampening 15 750
2000 60 15
Command: config route_map map1 sequence 10 set add dampening 15 750 2000 60 15

Success.

DGS-3620-28SC:admin#
```

## 42-12 delete route_map

### Description

This command is used to delete a route map configuration.

### Format

**delete route_map [map_name <map_name 16> {all_seqence} | all]**

### Parameters

**map_name** - Specifies the route map name used.
**<map_name 16>** - Enter the route map name used here. This name can be up to 16 characters long.

**all_seqence** - (Optional) Specifies that all sequence entries will be removed from the route map.

**all** - Specifies to delete all route maps.

### Restrictions

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

### Example

To delete the route map named “map1”:

```
DGS-3620-28SC:admin# delete route_map map_name map1
Command: delete route_map map_name map1

Success.

DGS-3620-28SC:admin#
```

## 42-13 show route_map

### Description

This command is used to display the route map configuration.

### Format

**show route_map {<map_name 16>}**

### Parameters

**<map_name 16>** - Enter the route map name used here. This name can be up to 16 characters long.

### Restrictions

None.

### Example

To show the route map named “map1”:

```
DGS-3620-28SC:admin# show route_map map1
Command: show route_map map1

  route_map : map1
--------------------------
     sequence : 10   (Permit)
     Match clauses:
     access_list :  ac_list1
     Set clauses:
     metric :  50

DGS-3620-28SC:admin#
```

# Chapter 43 IP Routing Commands

| |
|---|
| **create iproute** [default \| <network_address>] [null0 \| <ipaddr> {<metric 1-65535>} {[primary \| backup \| weight <value 1-4>]} \| ip_tunnel <tunnel_name 12>] |
| **delete iproute** [default \| <network_address>] [null0 \| <ipaddr> \| ip_tunnel <tunnel_name 12>] |
| **show iproute** {[<network_address> \| <ipaddr>]} {[static \| rip \| ospf \| bgp \| hardware]} |
| **create ipv6route** [default \| <ipv6networkaddr>] [[<ipif_name 12> <ipv6addr> \| <ipv6addr>] {<metric 1-65535>} {[primary \| backup]} \| ip_tunnel <tunnel_name 12>] |
| **delete ipv6route** [[default \| <ipv6networkaddr>] [<ipif_name 12> <ipv6addr> \| <ipv6addr> \| ip_tunnel <tunnel_name 12>] \| all] |
| **show ipv6route** {[<ipv6networkaddr> \| <ipv6addr>]} {[static \| ripng \| ospfv3 \| hardware]} |
| **enable ecmp ospf** |
| **disable ecmp ospf** |
| **config ecmp algorithm** {ip_destination \| [ip_source\| crc_low \| crc_high] \| tcp_udp_port} (1) |
| **show ecmp algorithm** |

## 43-1 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 and not set this route to be a multipath route.

### Format

**create iproute [default | <network_address>] [null0 | <ipaddr> {<metric 1-65535>} {[primary | backup | weight <value 1-4>]} | ip_tunnel <tunnel_name 12>]**

### Parameters

| |
|---|
| **default** - Specifies to create a default IP route entry. |
| **<network_address> -** The IP address and netmask of the IP interface that is the destination of the route. Specifies the address and mask information using the traditional format (for example, 10.1.2.3/255.0.0.0 or in CIDR format, 10.1.2.3/8). |
| **null0** - Specifies the null interface as the next hop. |
| **<ipaddr>** - Specifies the IP address for the next hop router.<br>**<metric 1-65535>** - (Optional) The default setting is 1.That is, the default hop cost is 1.<br>**primary** - (Optional) Specifies the route as the primary route to the destination.<br>**backup** - (Optional) Specifies the route as the backup route to the destination. If the route is not specified as the primary route or the backup route, then it will be auto-assigned by the system. The first created is the primary, the second created is the backup.<br>**weight** - (Optional) Specifies the weight value of the IP route.<br>**<value 1-4>** - Enter the weight value used here. This value must be between 1 and 4. |
| **ip_tunnel** - Specifies the IP tunnel used. **(EI Mode Only Parameter)**<br>**<tunnel_name 12>** - Enter the IP tunnel name used here. This name can be up to 12 characters long. |

### Restrictions

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

### Example

To add a default route with a nexthop of 10.48.74.21:

```
DGS-3620-28SC:admin#create iproute default 10.48.74.121
Command: create iproute default 10.48.74.121

Success.

DGS-3620-28SC:admin#
```

## 43-2 delete iproute

### Description

This command is used to delete an IP route entry from the switch’s IP routing table.

### Format

**delete iproute [default | <network_address>] [null0 | <ipaddr> | ip_tunnel <tunnel_name 12>]**

### Parameters

**default** - Specifies to delete a default IP route entry.

**<network_address>** - The IP address and netmask of the IP interface that is the destination of the route. Specifies the address and mask information using the traditional format (for example, 10.1.2.3/255.0.0.0 or in CIDR format, 10.1.2.3/8).

**null0** - Specifies the null interface as the next hop.

**<ipaddr>** - Specifies the IP address for the next hop router.

**ip_tunnel** - Specifies the IP tunnel used. **(EI Mode Only Parameter)**
  **<tunnel_name 12>** - Enter the IP tunnel name used here. This name can be up to 12 characters long.

### Restrictions

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

### Example

To delete a default route from the routing table:

```
DGS-3620-28SC:admin#delete iproute default 10.48.74.121
Command: delete iproute default 10.48.74.121

Success.

DGS-3620-28SC:admin#
```

## 43-3 show iproute

### Description

This command is used to display the switch’s current IP routing table.

### Format

**show iproute {[<network_address> | <ipaddr>]} {[static | rip | ospf | bgp | hardware]}**

### Parameters

**<network_address>** - (Optional) Specifies the destination network address of the route want to be displayed.

**<ipaddr>** - (Optional) Specifies the destination IP address of the route want to be displayed. The longest prefix matched route will be displayed.

**static** - (Optional) Specifies to display only static routes. One static route may be active or inactive.

**rip** - (Optional) Specifies to display only RIP routes.

**ospf** - (Optional) Specifies to display only OSPF routes.

**bgp** - (Optional) Specifies to display only BGP routes. **(EI Mode Only Parameter)**

**hardware** - (Optional) Specifies 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-3620-28SC:admin#show iproute
Command: show iproute

Routing Table

IP Address/Netmask  Gateway          Interface     Cost      Protocol
------------------  ---------------  ------------  --------  --------
10.0.0.0/8          0.0.0.0          System        1         Local

Total Entries : 1

DGS-3620-28SC:admin#
```

## 43-4 create ipv6route

### Description

This command is used to create an IPv6 static route in the switch’s IP routing table. If the next hop is a global address, it is not necessary to indicate the interface name. If the next hop is a link local address, then the interface name must be specified.

### Format

**create ipv6route [default | <ipv6networkaddr>] [[<ipif_name 12> <ipv6addr> | <ipv6addr>] {<metric 1-65535>} {[primary | backup]} | ip_tunnel <tunnel_name 12>]**

### Parameters

**default** - Specifies the default route.

**<ipv6networkaddr>** - Specifies the destination network for the route.

**<ipif_name 12> <ipv6addr>** - Specifies the interface for the route.

**<ipv6addr>** - Specifies the next hop address for this route.

**<metric 1-65535>** - (Optional) The default setting is 1.

**primary** - (Optional) Specifies the route as the primary route to the destination.

**backup** - (Optional) Specifies the route as the backup route to the destination. If the route is not specified as the primary route or the backup route, then it will be auto-assigned by the system. The first created is the primary, the second created is the backup.

**ip_tunnel** - Specifies the IPv6 tunnel name used. **(EI Mode Only Parameter)**
**<tunnel_name 12>** - Enter the IPv6 tunnel name used here. This name can be up to 12 characters long.

### Restrictions

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

### Example

To create an IPv6 default route:

```
DGS-3620-28SC:admin#create ipv6route default System FEC0::5
Command: create ipv6route default System FEC0::5

Success.

DGS-3620-28SC:admin#
```

## 43-5 delete ipv6route

### Description

This command is used to delete an IPv6 static route from the switch's IP routing table. If the next hop is a global address, it is not necessary 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> | ip_tunnel <tunnel_name 12>] | all]**

### Parameters

**default** - Specifies the default route.

**<ipv6networkaddr>** - Specifies the IPv6 network address.

**<ipif_name 12> <ipv6addr>** - Specifies the IP interface name.

**<ipv6addr>** - Specifies the next hop address for the IPv6 route

| |
|---|
| **ip_tunnel** - Specifies the IPv6 tunnel name used. **(EI Mode Only Parameter)**<br>**<tunnel_name 12>** - Enter the IPv6 tunnel name used here. This name can be up to 12 characters long. |
| **all** - All created static routes will be deleted. |

### Restrictions

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

### Example

To delete an IPv6 static route:

```
DGS-3620-28SC:admin#delete ipv6route default System FEC0::5
Command: delete ipv6route default System FEC0::5

Success.

DGS-3620-28SC:admin#
```

## 43-6 show ipv6route

### Description

This command is used to display the switch's current IPv6 routing table.

### Format

**show ipv6route {[<ipv6networkaddr> | <ipv6addr>]} {[static | ripng | ospfv3 | hardware]}**

### Parameters

| |
|---|
| **<ipv6networkaddr>** - (Optional) Specifies the IPv6 destination network address of the route.<br>**<ipv6addr>** - (Optional) Specifies the IPv6 address. |
| **static** - (Optional) Specifies the static route entries. |
| **ripng** - (Optional) Specifies the RIPng route entries. **(EI Mode Only Parameter)** |
| **ospfv3** - (Optional) Specifies the OSPFv3 route entries. **(EI Mode Only Parameter)** |
| **hardware** - (Optional) Specifies the route entries which have been written into hardware table. |

### Restrictions

None.

### Example

To display an IPv6 route:

```
DGS-3620-28SC:admin#show ipv6route
Command: show ipv6route

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

```

```
Total Entries: 1

DGS-3620-28SC:admin#
```

## 43-7 enable ecmp ospf

### Description

This command is used to activate the OSPF ECMP function.

### Format

**enable ecmp ospf**

### Parameters

None.

### Restrictions

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

### Example

To enable the OSPF ECMP function:

```
DGS-3620-28SC:admin# enable ecmp ospf
Command: enable ecmp ospf

Success.

DGS-3620-28SC:admin#
```

## 43-8 disable ecmp ospf

### Description

This command is used to disable the OSPF ECMP function.

### Format

**disable ecmp ospf**

### Parameters

None.

### Restrictions

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

### Example

To disable the OSPF ECMP function:

```
DGS-3620-28SC:admin# disable ecmp ospf
Command: disable ecmp ospf

Success.

DGS-3620-28SC:admin#
```

## 43-9 config ecmp algorithm

### Description

This command is used to configure the ECMP route load-balancing algorithm.

### Format

**config ecmp algorithm {ip_destination | [ip_source| crc_low | crc_high] | tcp_udp_port} (1)**

### Parameters

**ip_destination** - (Optional) Specifies that the ECMP algorithm will include the destination IP. It is set by default.

**ip_source** - (Optional) Specifies that the ECMP algorithm will include the lower 5 bits of the source IP. This attribution is mutually exclusive with crc_low and crc_high. If it is set, crc_low and crc_high will be excluded. It is not set by default.

**crc_low** - (Optional) Specifies that the ECMP algorithm will include the lower 5 bits of the CRC. This attribution is mutually exclusive with crc_high and ip_source. If it is set, crc_high and ip_source will be excluded. It is set by default.

**crc_high** - (Optional) Specifies that the ECMP algorithm will include the upper 5 bits of the CRC. This attribution is mutually exclusive with ip_source and crc_low. If it is set, crc_low and ip_source will be excluded. It is not set by default.

**tcp_udp_port** - (Optional) Specifies that the ECMP algorithm will include the TCP or UDP port. It is not set by default.

### Restrictions

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

### Example

To set the ECMP hash algorithm:

```
DGS-3620-28SC:admin# config ecmp algorithm ip_destination ip_source
Command: config ecmp algorithm ip_destination ip_source

Success.

DGS-3620-28SC:admin#
```

## 43-10 show ecmp algorithm

### Description

This command is used to display the ECMP related settings.

### Format

**show ecmp algorithm**

### Parameters

None.

### Restrictions

None.

### Example

To show current ECMP related settings:

```
DGS-3620-28SC:admin#show ecmp algorithm
Command: show ecmp algorithm

ECMP for OSPF : Enabled
ECMP Load Balance Algorithm :
  Destination IP : used.
  Source IP : not used.
  CRC_Low  : used.
  CRC_High : not used.
  TCP_UDP_Port : not used.


DGS-3620-28SC:admin#
```

# Chapter 44 IP Tunnel Commands

| |
|---|
| **create ip_tunnel** <tunnel_name 12> |
| **delete ip_tunnel** <tunnel_name 12> |
| **config ip_tunnel manual** <tunnel_name 12> {ipv6address <ipv6networkaddr> \| source <ipaddr> \| destination <ipaddr>}(1) |
| **config ip_tunnel 6to4** <tunnel_name 12> {ipv6address <ipv6networkaddr> \| source <ipaddr>}(1) |
| **config ip_tunnel isatap** <tunnel_name 12> {ipv6address <ipv6networkaddr> \| source <ipaddr>}(1) |
| **show ip_tunnel** {<tunnel_name 12>} |
| **enable ip_tunnel** {<tunnel_name 12>} |
| **disable ip_tunnel** {<tunnel_name 12>} |
| **config ip_tunnel gre** <tunnel_name 12> {ipaddress <network_address> \| ipv6address <ipv6networkaddr> \| source [<ipaddr> \| <ipv6addr>] \| destination [<ipaddr> \| <ipv6addr>]}(1) |

## 44-1 create ip_tunnel

### Description

This command is used to create an IP tunnel interface.

### Format

**create ip_tunnel <tunnel_name 12>**

### Parameters

| |
|---|
| **<tunnel_name 12>** - Enter the IP tunnel interface name used here. This name can be up to 12 characters long. |

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

To create an IP tunnel interface (with the tunnel name “tn2”):

```
DGS-3620-28SC:admin# create ip_tunnel tn2
Command: create ip_tunnel tn2

Success.

DGS-3620-28SC:admin#
```

## 44-2 delete ip_tunnel

### Description

This command is used to delete an IP tunnel interface.

### Format

**delete ip_tunnel <tunnel_name 12>**

### Parameters

**<tunnel_name 12>** - Enter the IP tunnel interface name used here. This name can be up to 12 characters long.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

To delete an IP tunnel interface (with the tunnel name "tn2"):

```
DGS-3620-28SC:admin# delete ip_tunnel tn2
Command: delete ip_tunnel tunnel tn2

Success.

DGS-3620-28SC:admin#
```

## 44-3 config ip_tunnel manual

### Description

This command is used to configure an IPv6 manual tunnel. If this tunnel has previously been configured in another mode, the tunnel's information will still exist in the database. However, whether the tunnel's former information is invalid or not, will depend on the current mode.

IPv6 Manual tunnels are simple point-to-point tunnels that can be used within a site or between sites.

### Format

**config ip_tunnel manual <tunnel_name 12> {ipv6address <ipv6networkaddr> | source <ipaddr> | destination <ipaddr>}(1)**

### Parameters

**<tunnel_name 12>** - Enter the IP tunnel interface name used here. This name can be up to 12 characters long.

**ipv6address** - (Optional) Specifies the IPv6 address assigned to the IPv6 tunnel interface. IPv6 processing becomes enabled on the IPv6 tunnel interface when an IPv6 address is

configured. The IPv6 address is not connected with the tunnel source or the destination IPv4 address.
**<ipv6networkaddr>** - Enter the IPv6 address used here.

**source** - (Optional) Specifies the source IPv4 address of the IPv6 tunnel interface. It is used as the source address for packets in the IPv6 tunnel.
**<ipaddr>** - Enter the IPv4 source address used here.

**destination** - (Optional) Specifies the destination IPv4 address of the IPv6 tunnel interface. It is used as the destination address for packets in the IPv6 tunnel. It is not required for 6to4 and ISATAP tunnels.
**<ipaddr>** - Enter the IPv4 destination address used here.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

To configure an IPv6 manual tunnel (Tunnel name is “tn2”, Tunnel source IPv4 address is 1.0.0.1, Tunnel destination IPv4 address is 1.0.0.2, Tunnel IPv6 address is 2001::1/64):

```
DGS-3620-28SC:admin# config ip_tunnel manual tn2 source 1.0.0.1 destination
1.0.0.2
Command: config ip_tunnel manual tn2 source 1.0.0.1 destination 1.0.0.2

Success.

DGS-3620-28SC:admin# config ip_tunnel manual tn2 ipv6address 2001::1/64
Command: config ip_tunnel manual tn2 ipv6address 2001::1/64

Success.

DGS-3620-28SC:admin#
```

## 44-4 config ip_tunnel 6to4

### Description

This command is used to configure an existing IPv6 tunnel as an IPv6 6to4 tunnel on the switch. If this tunnel has previously been configured in another mode, the tunnel’s information will still exist in the database. However, whether the tunnel’s former information is invalid or not will depend on the current mode. A maximum of one IPv6 6to4 tunnel can exist on the system.

IPv6 6to4 tunnels are point-to-multipoint tunnels that can be used to connect isolated IPv6 sites. Each IPv6 site has at least one connection to a shared IPv4 network and this IPv4 network could be the global Internet or a corporate backbone. The key requirement is that each site has a globally unique IPv4 address, which is used to construct a 48-bit globally unique 6to4 IPv6 prefix (starting with the prefix 2002::/16).

### Format

**config ip_tunnel 6to4 <tunnel_name 12> {ipv6address <ipv6networkaddr> | source <ipaddr>}(1)**

### Parameters

**<tunnel_name 12>** - Enter the IP tunnel interface name used here. This name can be up to 12 characters long.

**ipv6address** - (Optional) Specifies the IPv6 address assigned to this IPv6 tunnel interface. IPv6 processing will be enabled on this IPv6 tunnel interface as soon as its IPv6 address is configured. The 32 bits following the initial 2002::/16 prefix correspond to an IPv4 address assigned to the tunnel source.
**<ipv6networkaddr>** - Enter the IPv6 address used here.

**source** - (Optional) Specifies the IPv4 source address for a packet sent to the remote end of the 6to4 tunnel. The IPv4 destination address for the packet is derived from the IPv6 destination address of the remote destination, which is in the format of a 6to4 address. The address is derived by extracting the 4-octets immediately following the IPv6 destination address's 2002::/16 prefix. For example, a 6to4 address, 2002:c0a8:0001::/48 will be extracted to 192.168.0.1. Any IPv6 address that begins with the 2002::/16 prefix is known as a 6to4 address
**<ipaddr>** - Enter the IPv4 source address used here.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

To configure an IPv6 6to4 tunnel (Tunnel name is “tn2”, Tunnel source IPv4 address is 10.0.0.1, Tunnel IPv6 address is 2002:a00:1::1/64):

```
DGS-3620-28SC:admin# config ip_tunnel 6to4 tn2 source 10.0.0.1
Command: config ip_tunnel 6to4 tn2 source 10.0.0.1

Success.

DGS-3620-28SC:admin# config ip_tunnel 6to4 tn2 ipv6address 2002:a00:1::1/64
Command: config ip_tunnel 6to4 tn2 ipv6address 2002:a00:1::1/64

Success.

DGS-3620-28SC:admin#
```

## 44-5 config ip_tunnel isatap

### Description

This command is used to configure an existing IPv6 tunnel as an IPv6 ISATAP tunnel on the switch. If this tunnel has previously been configured in another mode, the tunnel’s information will still exist in the database. However, whether the tunnel’s former information is valid or not will depend on the current mode. IPv6 ISATAP tunnels are point-to-multipoint tunnels that can be used to connect systems within a site. An IPv6 ISATAP address is a well-defined unicast address that includes a 64-bit unicast IPv6 prefix (it can be either link-local or global prefixes), a 32-bit value 0000:5EFE/0200:5EFE and a 32-bit tunnel source IPv4 address.

### Format

**config ip_tunnel isatap <tunnel_name 12> {ipv6address <ipv6networkaddr> | source <ipaddr>}(1)**

### Parameters

**<tunnel_name 12>** - Enter the IP tunnel interface name used here. This name can be up to 12 characters long.

**ipv6address** - (Optional) Specifies the IPv6 address assigned to this IPv6 tunnel interface. IPv6 processing will be enabled on the IPv6 tunnel interface when an IPv6 address is configured. The last 32 bits of the IPv6 ISATAP address correspond to an IPv4 address assigned to the tunnel source.
**<ipv6networkaddr>** - Enter the IPv6 address used here.

**source** - (Optional) Specifies the source IPv4 address of this IPv6 tunnel interface. It is used as the source address for packets in the IPv6 tunnel. The tunnel destination IPv4 address is extracted from the last 32 bits of the remote tunnel endpoint's IPv6 ISATAP address.
**<ipaddr>** - Enter the source IPv4 address used here.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

To configure an IPv6 ISATAP tunnel (Tunnel name is "tn2", Tunnel source IPv4 address is 10.0.0.1, Tunnel IPv6 address is 2001::5efe:a00:1/64):

```
DGS-3620-28SC:admin# config ip_tunnel isatap tn2 source 10.0.0.1
Command: config ip_tunnel isatap tn2 source 10.0.0.1

Success.

DGS-3620-28SC:admin# config ip_tunnel isatap tn2 ipv6address
2001::5efe:a00:1/64
Command: config ip_tunnel isatap tn2 ipv6address 2001::5efe:a00:1/64

Success.

DGS-3620-28SC:admin#
```

## 44-6 show ip_tunnel

### Description

This command is used to show one or all IP tunnel interfaces' information.

### Format

**show ip_tunnel {<tunnel_name 12>}**

### Parameters

**<tunnel_name 12>** - (Optional) Enter the IP tunnel interface name used here. This name can be up to 12 characters long.

### Restrictions

None. (EI Mode Only Command)

### Example

To show an IP tunnel interface's information (Tunnel name is "tn2"):

```
DGS-3620-28SC:admin# show ip_tunnel tn2
Command: show ip_tunnel tn2

Tunnel Interface         : tn2
Interface Admin State    : Enabled
Tunnel Mode              : Manual
IPv6 Address             : 2000::1/64
Tunnel Source            : 1.0.0.1
Tunnel Destination       : 1.0.0.2

DGS-3620-28SC:admin#
```

## 44-7 enable ip_tunnel

### Description

This command is used to enable a single specified IP tunnel or all IP tunnels on the Switch.

### Format

**enable ip_tunnel {<tunnel_name 12>}**

### Parameters

**<tunnel_name 12>** - (Optional) Enter the IP tunnel interface name used here. This name can be up to 12 characters long.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

To enable an IP tunnel interface (Tunnel name is "tn2"):

```
DGS-3620-28SC:admin# enable ip_tunnel tn2
Command: enable ip_tunnel tn2

Success.

DGS-3620-28SC:admin#
```

## 44-8 disable ip_tunnel

### Description

This command is used to disable a single specified IP tunnel or all IP tunnels on the Switch.

### Format

**disable ip_tunnel {<tunnel_name 12>}**

### Parameters

**<tunnel_name 12>** - (Optional) Enter the IP tunnel interface name used here. This name can be up to 12 characters long.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

To disable an IP tunnel interface (Tunnel name is “tn2”):

```
DGS-3620-28SC:admin# disable ip_tunnel tn2
Command: disable ip_tunnel tn2

Success.

DGS-3620-28SC:admin#
```

## 44-9 config ip_tunnel gre

### Description

This command is used to configure an existing tunnel as a GRE tunnel (IPv6/IPv4-in-IPv4 or IPv6/IPv4-in-IPv6) on the switch. If this tunnel has been configured in another mode before, the tunnel’s information will still exist in the database. However, whether the tunnel’s former information is valid or not, depends on the current mode.

GRE tunnel are simple point-to-point tunnels that can be used within a site or between sites.

When a user wants to configure a GRE IPv6/IPv4-in-IPv4 tunnel, both the source and destination address must be IPv4 addresses because the delivery protocol is the IPv4 protocol. If the source and destination address type are not consistent, then the GRE tunnel will not work.

When a user wants to configure a GRE IPv6/IPv4-in-IPv6 tunnel, both the source and destination address must be IPv6 addresses because the delivery protocol is the IPv6 protocol. If the source and destination address type are not consistent then the GRE tunnel will not work.

## Format

**config ip_tunnel gre <tunnel_name 12> {ipaddress <network_address> | ipv6address <ipv6networkaddr> | source [<ipaddr> | <ipv6addr>] | destination [<ipaddr> | <ipv6addr>]}(1)**

## Parameters

| |
|---|
| **<tunnel_name 12>** - Enter the IP tunnel interface name used here. This name can be up to 12 characters long. |
| **ipaddress** - (Optional) Specifies the IPv4 address assigned to the GRE tunnel interface. IPv4 processing will be enabled on the IPv4 tunnel interface when an IPv4 address is configured. This IPv4 address is not connected with the tunnel source or destination IPv4 address.<br>**<network_address>** - Enter the IPv4 network address used here. |
| **ipv6address** - (Optional) Specifies the IPv6 address assigned to the GRE tunnel interface. IPv6 processing will be enabled on the IPv6 tunnel interface when an IPv6 address is configured. This IPv6 address is not connected with the tunnel source or destination IPv4 address.<br>**<ipv6networkaddr>** - Enter the IPv6 network address used here. |
| **source** - (Optional) Specifies the source IPv4 or IPv6 address of the GRE tunnel interface. It is used as the source address for packets in the tunnel. The address type that will be used depends on the Delivery Protocol. The address type used at both the source and destination must be consistent, otherwise, the GRE tunnel will not work.<br>**<ipaddr>** - Enter the IPv4 source address used here.<br>**<ipv6addr>** - Enter the IPv6 source address used here. |
| **destination** - (Optional) Specifies the destination IPv4 or IPv6 address of the GRE tunnel interface. It is used as the destination address for packets in the tunnel. The address type that will be used depends on the Delivery Protocol. The address type used at both the source and destination must be consistent, otherwise, the GRE tunnel will not work.<br>**<ipaddr>** - Enter the IPv4 destination address used here.<br>**<ipv6addr>** - Enter the IPv6 destination address used here. |

## Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

## Example

To configure a GRE tunnel (tunnel with: the name “tn1”, the delivery protocol as IPv4, tunnel source the IPv4 address 1.0.0.1, the tunnel destination IPv4 address i1.0.0.2, the GRE tunnel interface’s IPv6 address 2001::1/64, and the GRE tunnel interface’s IPv4 address 2.0.0.1/8):

```
DGS-3620-28SC:admin# config ip_tunnel gre tn1 source 1.0.0.1 destination
1.0.0.2
Command: config ip_tunnel gre tn1 source 1.0.0.1 destination 1.0.0.2

Success.

DGS-3620-28SC:admin# config ip_tunnel gre tn1 ipaddress 2.0.0.1/8 ipv6address
2001::1/64
Command: config ip_tunnel gre tn1 ipaddress 2.0.0.1/8 ipv6address 2001::1/64

Success.

DGS-3620-28SC:admin#
```

To display the configuration of a GRE tunnel interface named “tn1”:

```
DGS-3620-28SC:admin# show ip_tunnel tn1
Command: show ip_tunnel tn1

Tunnel Interface         : tn1
Interface Admin State    : Enabled
Tunnel Mode              : GRE
Ipv4 Address             : 2.0.0.1/8
IPv6 Address             : 2001::1/64
Tunnel Source            : 1.0.0.1
Tunnel Destination       : 1.0.0.2

DGS-3620-28SC:admin#
```

To configure a GRE tunnel (tunnel with: the name “tn2”, the delivery protocol IPv6, tunnel source the IPv6 address 2000::1, the tunnel destination IPv6 address 2000::2, the GRE tunnel interface’s IPv6 address 3001::1/64, the GRE tunnel interface’s IPv4 address 3.0.0.1/8):

```
DGS-3620-28SC:admin# config ip_tunnel gre tn2 source 2000::1 destination
2000::2
Command: config ip_tunnel gre tn2 source 2000::1 destination 2000::2

Success.

DGS-3620-28SC:admin# config ip_tunnel gre tn2 ipaddress 3.0.0.1/8
Command: config ip_tunnel gre tn2 ipaddress 3.0.0.1/8

Success.

DGS-3620-28SC:admin# config ip_tunnel gre tn2 ipv6address 3001::1/64
Command: config ip_tunnel gre tn2 ipv6address 3001::1/64

Success.

DGS-3620-28SC:admin#
```

To display the configuration of a GRE tunnel interface named “tn2”:

```
DGS-3620-28SC:admin# show ip_tunnel tn2
Command: show ip_tunnel tn2

Tunnel Interface         : tn2
Interface Admin State    : Enabled
Tunnel Mode              : GRE
Ipv4 Address             : 3.0.0.1/8
IPv6 Address             : 3001::1/64
Tunnel Source            : 2000::1
Tunnel Destination       : 2000::2

DGS-3620-28SC:admin#
```

# Chapter 45 IPv6 NDP Commands

| |
|---|
| **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] {hardware} |
| **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) |
| **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) |
| **show ipv6 nd** {ipif <ipif_name 12>} |

## 45-1 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>** - Specify the interface’s name. |
| **<ipv6addr>** - Specify the IPv6 address of the neighbor. |
| **<macaddr>** - Specify the MAC address of the neighbor. |

### Restrictions

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

### Example

To add a static entry into the NDP table:

```
DGS-3620-28SC: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-3620-28SC:admin#
```

## 45-2 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>** - Specify the IPv6 interface name.

**all** - Specify all IPv6 interfaces.

**<ipv6addr>** - Specify the IPv6 address of the neighbor.

**static** - Specify to delete the IPv6 static entries.

**dynamic** - Specify to delete the IPv6 dynamic entries.

**all** - Specify all IPv6 entries, including static and dynamic, to be deleted.

### Restrictions

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

### Example

To delete the neighbor cache.entry for IPv6 address 3ffc::1 on the IP interface “System”:

```
DGS-3620-28SC:admin#delete ipv6 neighbor_cache ipif System 3ffc::1
Command: delete ipv6 neighbor_cache ipif System 3FFC::1

Success.

DGS-3620-28SC:admin#
```

## 45-3 show ipv6 neighbor_cache ipif

### Description

This command is used to display the neighbor cache entry for the specified interface. Users can display a specific entry, all static entries, all dynamic entries, or all entries.

### Format

**show ipv6 neighbor_cache ipif [<ipif_name 12> | all] [ipv6address <ipv6addr> | static | dynamic | all ] {hardware}**

### Parameters

**<ipif_name 12>** - Specify the IPv6 interface name.

**all** - Specify all the IPv6 interface names.

**ipv6address** - Specify the IPv6 address of the neighbor.

**<ipv6addr>** - Specify the IPv6 address

**static** - Specify to display the IPv6 static neighbor cache entries.

**dynamic** - Specify to display the IPv6 dynamic entries.

**all** - Specify to display all IPv6 addresses, static and dynamic.

**hardware** - (Optional) Specify to display all the neighbor cache entries which were written into the hardware table.

### Restrictions

None.

### Example

To display all neighbor cache entries for the IP interface “System”:

```
DGS-3620-28SC:admin#show ipv6 neighbor_cache ipif System all
Command: show ipv6 neighbor_cache ipif System all

FE80::215:72FF:FE36:104                State: Reachable
MAC Address : 00-15-72-36-01-04        Port : 1:21
Interface   : System                   VID  : 1

Total Entries: 1

DGS-3620-28SC:admin#
```

## 45-4 config ipv6 nd ns ipif

### Description

This command is used to configure the NS retransmit time of a specified interface.

### Format

**config ipv6 nd ns ipif <ipif_name 12> retrans_time <millisecond 0-4294967295>**

### Parameters

**<ipif_name 12>** - Specify the name of the interface. The maximum length is 12 characters.

**retrans_time** - Specify the neighbor solicitation’s retransmit timer in milliseconds. It has the same value as ra retrans_time in the config ipv6 nd ra command. If one is configured, the other will change too.

**<millisecond 0-4294967295>** - Specify the neighbor solicitation’s retransmit timer in milliseconds. It has the same value as ra retrans_time in the config ipv6 nd ra command. If one is configured, the other will change too. Specify a time between 0 and 4294967295 milliseconds.

### Restrictions

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

### Example

To configure the NS retransmit time of a specified interface:

```
DGS-3620-28SC:admin#config ipv6 nd ns ipif System retrans_time 400
Command: config ipv6 nd ns ipif System retrans_time 400

Success.

DGS-3620-28SC:admin#
```

## 45-5 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** - Specifies the amount of time that a node can consider a neighboring node reachable after receiving a reachability confirmation in millisecond.
- **<millisecond 0-3600000>** - Specify the time between 0 and 3600000 milliseconds.

**retrans_time** - Specifies the amount of time between retransmissions of router advertisement message in millisecond, and the router advertisement packet will take it to host.
- **<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 Administrator, Operator and Power-User level users can issue this command.

### Example

To configure the RA state as enabled and the life_time of the "tiberius" interface to be 1000 seconds:

```
DGS-3620-28SC:admin#config ipv6 nd ra ipif tiberius state enable life_time 1000
Command: config ipv6 nd ra ipif tiberius state enable life_time 1000

Success.

DGS-3620-28SC:admin#
```

## 45-6 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 seconds 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 seconds. 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 seconds. 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-3620-28SC: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-3620-28SC:admin#
```

## 45-7 show ipv6 nd

### Description

This command is used to display IPv6 Neighbor Discover related configuration.

### Format

**show ipv6 nd {ipif <ipif_name 12>}**

### Parameters

**ipif** - (Optional) Specify the interface name.
**<ipif_name 12>** - Specify the interface name. The maximum length is 12 characters.

**Note:** If no IP interface is specified, the IPv6 ND related configuration of all interfaces will be displayed.

### Restrictions

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

### Example

To display IPv6 Neighbor Discover related configuration:

```
DGS-3620-28SC:admin#show ipv6 nd ipif System
Command: show ipv6 nd ipif System



Interface Name            : System
Hop Limit                 : 64
```

```
NS Retransmit Time         : 400 (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         : 400 (ms)
RA Managed Flag            : Disabled
RA Other Configure Flag    : Disabled
Prefix                               Preferred  Valid      OnLink   Autonomous
1000:A111:B111:C111::/64             604800     2592000    Enabled  Enabled

DGS-3620-28SC:admin#
```

# Chapter 46 IP-MAC-Port Binding (IMPB) Commands

**create address_binding ip_mac ipaddress** <ipaddr> mac_address <macaddr> {ports[<portlist>| all ]}

**create address_binding ip_mac ipv6address** <ipv6addr> mac_address <macaddr> {ports [<portlist> | all]}

**config address_binding ip_mac ports** [<portlist> | all] {arp_inspection [strict | loose | disable] | ip_inspection [enable | disable] | protocol [ipv4 | ipv6 | all] | allow_zeroip [enable | disable] | forward_dhcppkt [enable | disable] | stop_learning_threshold <int 0-500>}(1)

**config address_binding ip_mac ipaddress** <ipaddr> 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>]

**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> mac_address <macaddr> | ipv6address <ipv6addr> mac_address <macaddr>]

**enable address_binding trap_log**

**disable address_binding trap_log**

**enable address_binding dhcp_snoop** {[ipv6 | all]}

**disable address_binding dhcp_snoop** {[ipv6 | all]}

**clear address_binding dhcp_snoop binding_entry ports** [<portlist> | all] {[ipv6 | all]}

**show address_binding dhcp_snoop** {max_entry {ports <portlist>}}

**show address_binding dhcp_snoop binding_entry** {port <port>}

**config address_binding dhcp_snoop max_entry ports** [<portlist> | all] limit [<value 1-50> | no_limit] {ipv6}

**config address_binding recover_learning ports** [<portlist> | all]

**enable address_binding nd_snoop**

**disable address_binding nd_snoop**

**config address_binding nd_snoop ports** [<portlist> | all] max_entry [<value 1-50> | no_limit]

**show address_binding nd_snoop** {ports <portlist>}

**show address_binding nd_snoop binding_entry** {port <port>}

**clear address_binding nd_snoop binding_entry ports** [<portlist> | all]

## 46-1 create address_binding ip_mac ipaddress

### Description

This command is used to create an IP-MAC-Port binding entry.

### Format

**create address_binding ip_mac ipaddress <ipaddr> mac_address <macaddr> {ports[<portlist>| all ]}**

### Parameters

**<ipaddr>** - Specify the IP address.

**mac_address** - Specify the MAC address.
  **<macaddr>** - Enter the MAC address here.

**ports** - (Optional) Configure the portlist or all ports.
  **<portlist>** - Specify a range of ports to be configured.
  **all** - Specify to apply to all the ports.

### Restrictions

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

### Example

To create address binding on the switch:

```
DGS-3620-28SC: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-3620-28SC:admin#
```

## 46-2 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>** - Specify the IPv6 address.

**mac_address** - Specify the MAC address.
  **<macaddr>** - Enter the MAC address here.

**ports** - (Optional) Configure the portlist or all ports.
  **<portlist>** - Specify a range of ports to be configured.
  **all** - Specify to apply to all the ports.

### Restrictions

Only Administrator, Operator and Power-User level 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-3620-28SC: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-3620-28SC:admin#
```

## 46-3 config address_binding ip_mac ports

### Description

This command is used to configure the per port state of IP-MAC-Port binding in the switch. If a port has been configured as group member of an aggregated link, then it can not enable its IP-MAC-Port binding function. When the binding check state is enabled, for IP packet and ARP packet received by this port, the switch will check whether the the IP address and MAC address match the binding entries. The packets will be dropped if they do not match. For this function, the switch can operate in ARP Inspection and IP Inspection.

**ARP Inspection:** All ARP packets will be checked while ARP Inspection is enabled. The legal ARP packets will be forwarded, while the illegal ARP packets will be dropped.

**IP Inspection:** All IP packets will be checked while IP Inspection is enabled. The legal IP packets will be forwarded, while the illegal IP packets will be dropped. When IP Inspection is enabled, and ARP Inspection is disabled, all non-IP packets (L2 packets, ARP…) will be forwarded by default.

### Format

**config address_binding ip_mac ports [<portlist> | all] {arp_inspection [strict | loose | disable] | ip_inspection [enable | disable] | protocol [ipv4 | ipv6 | all] | allow_zeroip [enable | disable] | forward_dhcppkt [enable | disable] | stop_learning_threshold <int 0-500>}(1)**

### Parameters

**<portlist>** - Specify a range of ports to configure.
**all** - Specify to configure all ports.

**arp_inspection** - (Optional) Specifies that when the ARP inspection function is enabled, the legal ARP packets wil be forwarded, while the illegal packets will be dropped.
- **strict** - Specifies that in this mode, all packets are dropped by default until a legal ARP or IP packet is detected.
- **loose** - Specifies that in this mode, all packets are forwarded by default until an illegal ARP or broadcast IP packet is detected.
- **disable** - Disable the ARP inspection function. The default value is disable.

**ip_inspection** - (Optional) Specifies the IP inspection function state.
- **enable** - Specifies to enable the IP inspection function. The legal IP packets will be forwarded, while the illegal IP packets will be dropped.
- **disable** - Specifies to disable the IP inspection function. The default value is disable.

**protocol** - (Optional) Specifies the IP protocoal of the packets that will be checked.
- **ipv4** - Specifies that only IPv4 packets will be checked.
- **ipv6** - Specifies that only IPv6 packets will be checked.
- **all** - Specifies that both IPv4 and IPv6 packets will be checked.

**allow_zeroip** - (Optional) Specify whether to allow ARP packets with SIP address 0.0.0.0.
- **enable** - If 0.0.0.0 is not configured in the binding list, when it is set to enabled, the ARP packet with this source IP address 0.0.0.0 will be allowed.
- **disable** - When set to disable, this option does not affect the IP-MAC-port binding IP

Inspection.

**forward_dhcppkt** - (Optional) By default, the DHCP packets with broadcast DA will be flooded.
**enable** - This setting is effective when DHCP snooping is enabled because the DHCP packet which has been trapped to CPU needs to be forwarded by the software. This setting controls the forwarding behaviour under this situation.
**disable** - When set to disable, the broadcast DHCP packets received by the specified port will not be forwarded.

**stop_learning_threshold** - (Optional) Enter the stop learning threshold value here.
**<int 0-500>** - The stop learning threshold value must be between 0 and 500.

### Restrictions

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

### Example

To configure port 1 to be enabled for address binding:

```
DGS-3620-28SC:admin# config address_binding ip_mac ports 1 arp_inspection
strict ip_inspection enable protocol ipv4
Command: config address_binding ip_mac ports 1 arp_inspection strict
ip_inspection enable protocol ipv4


Success.


DGS-3620-28SC:admin#
```

## 46-4 config address_binding ip_mac ipaddress

### Description

This command is used to update an address binding entry.

### Format

**config address_binding ip_mac ipaddress <ipaddr> mac_address <macaddr> {ports [<portlist>| all ]}**

### Parameters

**<ipaddr>** - Specify the IP address.

**mac_address** - Specify the MAC address.
**<macaddr>** - Enter the MAC address here.

**ports** - (Optional) Configure the portlist to apply, if ports are not configured, then it will apply to all ports.
**<portlist>** - Specify the list of ports to apply.
**all** - Specify to apply to all the ports.

### Restrictions

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

### Example

To configure an address binding entry:

```
DGS-3620-28SC: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-3620-28SC:admin#
```

## 46-5 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

| |
|---|
| **ipv6address** - Specifies the IPv6 address used.<br>**<ipv6addr>** - Enter the IPv6 address used here. |
| **mac_address** - Specify the MAC address.<br>**<macaddr>** - Enter the MAC address here. |
| **ports** - (Optional) Configure the portlist to apply, if ports are not configured, then it will apply to all ports.<br>**<portlist>** - Specify the list of ports to apply.<br>**all** - Specify to apply to all the ports. |

### Restrictions

Only Administrator, Operator and Power-User level 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-3620-28SC: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-3620-28SC:admin#
```

## 46-6 delete address_binding blocked

### Description

This command is used to delete a blocked entry. It specifies the address database that the system has automatically learned and blocked.

### Format

**delete address_binding blocked [all | vlan_name <vlan_name> mac_address <macaddr>]**

### Parameters

**all** - Specifies that all the blocked MAC addresses will be used.

**vlan_name** - Specifies the name of the VLAN that the blocked MAC address belongs to.
  **<vlan_name>** - Enter the VLAN name used here.

**mac_address** - Specifies the MAC address of the blocked MAC address.
  **<macaddr>** - Enter the MAC address used here.

### Restrictions

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

### Example

To delete the blocked MAC address 00-00-00-00-00-11, which belongs to the VLAN named “v31”:

```
DGS-3620-28SC: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-3620-28SC:admin#
```

## 46-7 delete address_binding ip_mac

### Description

This command is used to delete an IMPB entry.

### Format

**delete address_binding ip_mac [all | ipaddress <ipaddr> mac_address <macaddr>] | ipv6address <ipv6addr> mac_address <macaddr>**

### Parameters

**all** - Specifies that all the MAC addresses will be used.

**vlan_name** - Specifies the name of the VLAN that the MAC address belongs to.
  **<vlan_name>** - Enter the VLAN name used here.

**mac_address** - Specifies the MAC address of the IMPB entry.
  **<macaddr> -** Enter the MAC address of the IMPB entry here.

**ipv6address** - Specifies the IPv6 address of the IMPB entry.
    **<ipv6addr>** - Enter the IPv6 address of the IMPB entry here.

**mac_address** - Specifies the MAC address of the IMPB entry.
    **<macaddr>** - Enter the MAC address of the IMPB entry here.

### Restrictions

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

### Example

To delete an IMPB entry that binds the IP address 10.1.1.1.1 to the MAC address 00-00-00-00-00-11:

```
DGS-3620-28SC: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-3620-28SC:admin#
```

To delete 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-3620-28SC:admin# delete address_binding ip_mac ipv6address
fe80::240:5ff:fe00:28 mac_address 00-00-00-00-00-11
Command: delete address_binding ip_mac ipv6address fe80::240:5ff:fe00:28
mac_address 00-00-00-00-00-11

Success.

DGS-3620-28SC:admin#
```

## 46-8 show address_binding

### Description

This command is used to display address binding information.

### Format

**show address_binding {ports {<portlist>}}**

### Parameters

**ports** – (Optional) Specify to display the state of IP MAC port binding for all ports.
    **<portlist>** - Enter the list of ports for the display here.

### Restrictions

None.

### Example

To display address binding information:

```
DGS-3620-28SC:admin#show address_binding
Command: show address_binding

Trap/Log          : Disabled
DHCP Snoop(IPv4)  : Disabled
DHCP Snoop(IPv6)  : Disabled
ND Snoop          : Disabled


DGS-3620-28SC:admin#
```

To display address binding information for all ports:

```
DGS-3620-28SC:admin#show address_binding ports
Command: show address_binding ports

ARP: ARP Inspection   IP: IP Inspection

Port   ARP       IP       Protocol Zero IP   DHCP Packet  Stop Learning
                                                       Threshold/Mode
----- -------- --------  ----- ---------  -----------  --------------
1      Loose     Disabled  IPv4  Allow      Forward      100/Stop
2      Strict    Enabled   IPv6  Not Allow  Not Forward  200/Normal
3      Disabled  Enabled   All   Not Allow  Not Forward  200/Normal
4      Strict    Disabled  All   Not Allow  Not Forward  200/Normal
5      Disabled  Disabled  All   Not Allow  Not Forward  200/Normal
6      Strict    Disabled  All   Not Allow  Not Forward  200/Normal
7      Disabled  Disabled  All   Not Allow  Not Forward  200/Normal
8      Strict    Disabled  All   Not Allow  Not Forward  200/Normal
9      Disabled  Disabled  All   Not Allow  Not Forward  200/Normal
10     Strict    Disabled  All   Not Allow  Not Forward  No Limit/Normal
11     Disabled  Disabled  All   Not Allow  Not Forward  200/Normal
12     Strict    Disabled  All   Not Allow  Not Forward  200/Normal

DGS-3620-28SC:admin#
```

## 46-9 show address_binding blocked

### Description

This command is used to display address binding information for blocked entries.

### Format

**show address_binding blocked [all | vlan_name <vlan_name> mac_address <macaddr>]**

### Parameters

**blocked** - (Optional) Specify the address database that system auto learned and blocked.

**all** - Specify to display all.
**vlan_name** - Specify the VLAN name (the blocked MAC belongs to).
**<vlan_name>** - Enter the VLAN name here.
**mac_address** - Specify the MAC address.
**<macaddr>** - Enter the MAC address here.

### Restrictions

None.

### Example

To show the IMPB entries that are currently blocked:

```
DGS-3620-28SC:admin#show address_binding blocked all
Command: show address_binding blocked all

 VID  VLAN Name                        MAC Address       Port
 ---- -------------------------------- ----------------- ----
 1     default                         00-01-02-03-29-38  7
 1     default                         00-0C-6E-5C-67-F4  7
 1     default                         00-0C-F8-20-90-01  7
 1     default                         00-0E-35-C7-FA-3F  7
 1     default                         00-0E-A6-8F-72-EA  7
 1     default                         00-0E-A6-C3-34-BE  7
 1     default                         00-11-2F-6D-F3-AC  7
 1     default                         00-50-8D-36-89-48  7
 1     default                         00-50-BA-00-05-9E  7
 1     default                         00-50-BA-10-D8-F6  7
 1     default                         00-50-BA-38-7D-E0  7
 1     default                         00-50-BA-51-31-62  7
 1     default                         00-50-BA-DA-01-58  7
 1     default                         00-A0-C9-01-01-23  7
 1     default                         00-E0-18-D4-63-1C  7

Total Entries : 15

DGS-3620-28SC:admin#
```

## 46-10 show address_binding ip_mac

### Description

This command is used to display the user created database of address binding information.

### Format

**show address_binding ip_mac [all | ipaddress <ipaddr> mac_address <macaddr>] | ipv6address <ipv6addr> mac_address <macaddr>**

## Parameters

**ip_mac** - (Optional) Specify the database that a user creates for address binding.

**all** - Specify to display all.
**ipaddress** - Specify the IP address.
    **<ipaddr>** - Enter the IP address here.
**mac_address** - Specify the MAC address.
    **<macaddr>** - Enter the MAC address here.

**ipv6address** - Specify the IPv6 address.
    **<ipv6addr>** - Enter the IPv6 address here.
**mac_address** - Specify the MAC address.
    **<macaddr>** - Enter the MAC address here.

## Restrictions

None.

## Example

To display all the IP-MAC address binding information:

```
DGS-3620-28SC: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                                00-11-22-33-44-55 S  I  1
 10.1.1.2                                00-22-33-44-55-66 S  A  2
 2001::1                                 00-33-44-55-66-77 S  I  3
 2011::1                                 00-44-55-66-77-88 S  I  4

Total Entries : 4

DGS-3620-28SC:admin#
```

To display the IMPB entry by IP address and MAC address:

```
DGS-3620-28SC:admin# show address_binding ip_mac ipaddress 10.1.1.1 mac_address
00-00-00-00-00-11
Command: show address_binding ip_mac ipaddress 10.1.1.1 mac_address 00-00-00-
00-00-11

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 1,3,5,7,8

Total Entries : 1

DGS-3620-28SC:admin#
```

## 46-11 enable address_binding trap_log

### Description

This command is used to send trap and log messages when an address binding module detects illegal IP and MAC addresses.

### Format

**enable address_binding trap_log**

### Parameters

None.

### Restrictions

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

### Example

To enable the address binding trap and log:

```
DGS-3620-28SC:admin#enable address_binding trap_log
Command: enable address_binding trap_log

Success.

DGS-3620-28SC:admin#
```

## 46-12 disable address_binding trap_log

### Description

This command is used to disable address binding trap logs.

### Format

**disable address_binding trap_log**

### Parameters

None.

### Restrictions

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

### Example

To disable the address binding trap and log:

```
DGS-3620-28SC:admin#disable address_binding trap_log
Command: disable address_binding trap_log

Success.

DGS-3620-28SC:admin#
```

## 46-13 enable address_binding dhcp_snoop

### Description

This command is used to enable the address binding DHCP snooping mode. By default, DHCP snooping is disabled. If a user enables DHCP snooping, all address binding disabled ports will function as server ports (the switch will learn IP addresses through server ports (by DHCP OFFER and DHCP ACK packets)). Note that the DHCP discover packet can not be passed through the user ports if the 'forward_dhcppkt' function is disabled on this port.

The auto-learned IP-MAC-Port binding entry will be mapped to a specific source port based on the MAC address learning function. This entry will be created as an binding entry for this specific port. Each entry is associated with a lease time. When the lease time expires, the expired entry will be removed from this 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.

Consider the case in which a binding entry learned by DHCP snooping conflicts with the statically configured entry. This means that the binding relation is in conflict. For example, if IP A is binded with MAC X by static configuration, suppose that the binding entry learned by DHCP snooping is IP A binded by MAC Y, then there is a conflict. When the DHCP snooping learned entry is binded with the static configured entry, then the DHCP snooping learned entry will not be created.

Consider the other conflict case, when the DHCP snooping learned a binding entry, and the same IP-MAC-Port binding pair has been statically configured. If the learned information is consistent with the statically configured entry, then the auto-learned entry will not be created. If the entry is statically configured in ARP table, then the auto learned entry will not be created. If the entry is statically configured on one port and the entry is auto-learned on another port, then the auto-learned entry will not be created either.

### Format

**enable address_binding dhcp_snoop {[ipv6 | all]}**

### Parameters

| |
|---|
| **ipv6** – (Optional) Specifies that the address used is an IPv6 address. |
| **all** – (Optional) Specifies that all IP addresses will be used. |

### Restrictions

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

### Example

To enable the address binding DHCP snooping mode:

```
DGS-3620-28SC:admin#enable address_binding dhcp_snoop
Command: enable address_binding dhcp_snoop

Success.

DGS-3620-28SC:admin#
```

## 46-14 disable address_binding dhcp_snoop

### Description

This command is used to disable address binding DHCP snooping. When DHCP snooping is disabled, all of the auto-learned binding entries will be removed.

### Format

**disable address_binding dhcp_snoop {[ipv6 | all]}**

### Parameters

**ipv6** – (Optional) Specifies that the address used is an IPv6 address.

**all** – Specifies that all IP addresses will be used.

### Restrictions

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

### Example

To disable the address binding DHCP snooping mode:

```
DGS-3620-28SC:admin#disable address_binding dhcp_snoop
Command: disable address_binding dhcp_snoop

Success.

DGS-3620-28SC:admin#
```

## 46-15 clear address_binding dhcp_snoop binding_entry ports

### Description

This command is used to clear the address binding entries learned for the specified ports.

### Format

**clear address_binding dhcp_snoop binding_entry ports [<portlist> | all] {[ipv6 | all]}**

### Parameters

**<portlist>** - Specify the list of ports to clear the DHCP-snoop learned entry.

**all** - Specify to clear the address binding entries learned for all ports.

**ipv6** – (Optional) Specifies that the address used is an IPv6 address.

**all** – Specifies that all IPv6 addresses will be used.

### Restrictions

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

### Example

To clear the address binding entries for ports 1 to 3:

```
DGS-3620-28SC:admin# clear address_binding dhcp_snoop binding_entry ports 1-3
Command: clear address_binding dhcp_snoop binding_entry ports 1-3

Success.

DGS-3620-28SC:admin#
```

## 46-16 show address_binding dhcp_snoop

### Description

This command is used to display DHCP snooping information.

### Format

**show address_binding dhcp_snoop {max_entry {ports <portlist>}}**

### Parameters

**max_entry** - (Optional) Specify to display the maximum number of entries.

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

### Restrictions

None.

### Example

To display address binding DHCP snooping:

```
DGS-3620-28SC:admin#show address_binding dhcp_snoop
Command: show address_binding dhcp_snoop

DHCP Snoop(IPv4) : Disabled
DHCP Snoop(IPv6) : Disabled

DGS-3620-28SC:admin#
```

To display the address binding DHCP snooping maximum entries on port 1 to 10:

```
DGS-3620-28SC:admin#show address_binding dhcp_snoop max_entry ports 1-10
```

```
Command: show address_binding dhcp_snoop max_entry ports 1-10

Port  Max Entry  Max IPv6 Entry
----  ---------  --------------
1     No Limit   No Limit
2     10         No Limit
3     20         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

DGS-3620-28SC:admin#
```

## 46-17 show address_binding dhcp_snoop binding_entry

### Description

This command is used to display DHCP snooping information of a specific binding entry.

### Format

**show address_binding dhcp_snoop binding_entry {port <port>}**

### Parameters

**port** - (Optional) Specify a port on which to display the binding entry.
**<port>** - Enter the port number here.

### Restrictions

None.

### Example

To display the DHCP snooping binding entries:

```
DGS-3620-28SC: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  LT(sec)    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
 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 : 4

DGS-3620-28SC:admin#
```

**Note:** “Inactive” indicates that the entry is currently inactive due to port link down.

## 46-18 config address_binding dhcp_snoop max_entry ports

### Description

This command is used to specifiy the maximum number of entries which can be learned by the specified ports. By default, the per port maximum entry is no limit.

### Format

**config address_binding dhcp_snoop max_entry ports [<portlist> | all] limit [<value 1-50> | no_limit] {ipv6}**

### Parameters

**<portlist>** - Specify the list of ports to configure maximum number of entries.
**all** - Specify all the ports to configure maximum number of entries.

**limit** - Specify the maximum number of entries which can be learned by the specified ports.
  **<value 1-50>** - Specify a maximum limit between 1 and 50.
  **no_limit** - Specify an unlimited number of entries.

**ipv6** – (Optional) Specifies that the configuration is for IPv6 DHCP Snooping.

### Restrictions

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

### Example

To set the maximum number of entries that ports 1 to 3 can learn to 10:

```
DGS-3620-28SC: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-3620-28SC:admin#
```

## 46-19 config address_binding recover_learning ports

### Description

This command is used to recover port learning.

### Format

**config address_binding recover_learning ports [<portlist> | all]**

### Parameters

**<portlist>** - Specify the list of ports to recover learning.
**all** - Specify to recover learning for all ports.

### Restrictions

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

### Example

To configure ports 1 to 3 to recover learning:

```
DGS-3620-28SC:admin#config address_binding recover_learning ports 1-3
Command: config address_binding recover_learning ports 1-3

Success.

DGS-3620-28SC:admin#
```

## 46-20 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 Administrator, Operator and Power-User level users can issue this command.

### Example

To enable the ND snooping function on the Switch:

```
DGS-3620-28SC:admin# enable address_binding nd_snoop
Command: enable address_binding nd_snoop

Success.

DGS-3620-28SC:admin#
```

## 46-21 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 Administrator, Operator and Power-User level users can issue this command.

### Example

To disable the DHCPv6 snooping function on the Switch:

```
DGS-3620-28SC:admin# disable address_binding nd_snoop
Command: disable address_binding nd_snoop

Success.

DGS-3620-28SC:admin#
```

## 46-22 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.

### Format

**config address_binding nd_snoop ports [<portlist> | all] max_entry [<value 1-50> | no_limit]**

### Parameters

**ports** - Specifies the list of ports used for this configuration.
**<portlist>** - Enter the list of ports used for this configuration here.
**all** - Specifies that all the ports will be usd for this configuration.

**max_entry** - Specifies the maximum number of entries.
**<value 1-50>** - Enter the maximum number of entries used here. This value must be between 1 and 50.
**no_limit** - Specifies that the maximum number of learned entries is unlimited.

### Restrictions

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

### Example

To specify that a maximum of 10 entries can be learned by ND snooping on ports 1–3:

```
DGS-3620-28SC: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-3620-28SC:admin#
```

## 46-23 show address_binding nd_snoop

### Description

This command is used to display the status of ND snooping on the Switch.

### Format

**show address_binding nd_snoop {ports <portlist>}**

### Parameters

**ports** – (Optional) Specifies the list of ports used for this display.
**<portlist>** - Enter the list of ports used for this display here.

### Restrictions

None.

### Example

To show the ND snooping state:

```
DGS-3620-28SC:admin# show address_binding nd_snoop
Command: show address_binding nd_snoop

ND Snoop     : Enabled

DGS-3620-28SC:admin#
```

To show the ND snooping maximum entry information for ports 1-5:

```
DGS-3620-28SC:admin#show address_binding nd_snoop ports 1:1-1:5
Command: show address_binding nd_snoop ports 1:1-1:5

Port  Max Entry
----  ---------
1:1   No Limit
1:2   No Limit
1:3   No Limit
1:4   No Limit
1:5   No Limit

DGS-3620-28SC:admin#
```

## 46-24 show address_binding nd_snoop binding_entry

### Description

This command is used to show the ND snooping binding entries on the Switch.

### Format

**show address_binding nd_snoop binding_entry {port <port>}**

### Parameters

**port** - (Optional) Specifies a port used for this display.
  **<port>** - Enter the port number used for this display here.

### Restrictions

None.

### Example

To display the ND snooping binding entry:

```
DGS-3620-28SC: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-3620-28SC:admin#
```

## 46-25 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

**ports** - Specify the list of ports that you would like to clear the ND snoop learned entry.
**<portlist>** - Enter the list of port used here.
**all** - Clear all ND snooping learned entries.

### Restrictions

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

### Example

To clear ND snooping entry on ports 1-3:

```
DGS-3620-28SC:admin# clear address_binding nd_snoop binding_entry ports 1-3
Command: clear address_binding nd_snoop binding_entry ports 1-3

Success.

DGS-3620-28SC:admin#
```

# Chapter 47 Japanese Web-based Access Control (JWAC) Commands

| |
|---|
| **enable jwac** |
| **disable jwac** |
| **enable jwac redirect** |
| **disable jwac redirect** |
| **enable jwac forcible_logout** |
| **disable jwac forcible_logout** |
| **enable jwac udp_filtering** |
| **disable jwac udp_filtering** |
| **enable jwac quarantine_server_monitor** |
| **disable jwac quarantine_server_monitor** |
| **config jwac quarantine_server_error_timeout** <sec 5-300> |
| **config jwac [quarantine_server_url** <string 128> \| clear_quarantine_server_url] |
| **config jwac redirect** {destination [quarantine_server \| jwac_login_page] \| delay_time <sec 0-10>}(1) |
| **config jwac virtual_ip** <ipaddr> {url [<string 128> \| clear]} |
| **config jwac update_server** [add \| delete] ipaddress <network_address> {[tcp_port <port_number 1-65535> \| udp_port <port_number 1-65535>]} |
| **config jwac switch_http_port** <tcp_port_number 1-65535> {[http \| https]} |
| **config jwac ports** [<portlist> \| all] {state [enable \| disable] \| max_authenticating_host <value 0-100> \| aging_time [infinite \| <min 1-1440>] \| idle_time [infinite \| <min 1-1440>] \| block_time [<sec 0-300>]}(1) |
| **config jwac radius_protocol** [local \| eap_md5 \| pap \| chap \| ms_chap \| ms_chapv2] |
| **create jwac user** <username 15> {vlan <vlanid 1-4094>} |
| **config jwac user** <username 15> {vlan <vlanid 1-4094>} |
| **delete jwac** [user <username 15> \| all_users] |
| **show jwac user** |
| **show jwac** |
| **show jwac auth_state ports** {<portlist>} |
| **show jwac update_server** |
| **show jwac ports** {<portlist>} |
| **clear jwac auth_state** [ports [all \| <portlist>] {authenticated \| authenticating \| blocked} \| mac_addr <macaddr>] |
| **config jwac authenticate_page** [japanese \| english] |
| **show jwac authenticate_page** |
| **config jwac authentication_page element** [japanese \| english] [default \| page_title <desc 128> \| login_window_title <desc 32> \| user_name_title <desc 16> \| password_title <desc 16> \| logout_window_title <desc 32> \| notification_line <value 1-5> <desc 128>] |
| **config jwac authorization attributes** {radius [enable \| disable] \| local [enable \| disable]}(1) |

## 47-1 enable jwac

### Description

This command is used to enable the Japanese Web-based access control (JWAC) function. JWAC and WAC are mutually exclusive functions. That is, they can not be enabled at the same time.

Using the JWAC function, PC users need to pass two stages of authentication. The first stage is to do the authentication with the quarantine server and the second stage is the authentication with the switch. For the second stage, the authentication is similar to WAC, except that there is no port VLAN membership change by JWAC after a host passes authentication. The RADIUS server will share the server configuration defined by the 802.1X command set.

### Format

**enable jwac**

### Parameters

None.

### Restrictions

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

### Example

To enable JWAC:

```
DGS-3620-28SC:admin#enable jwac
Command: enable jwac

Success.

DGS-3620-28SC:admin#
```

## 47-2 disable jwac

### Description

This command is used to disable JWAC.

### Format

**disable jwac**

### Parameters

None.

### Restrictions

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

### Example

To disable JWAC:

```
DGS-3620-28SC:admin#disable jwac
Command: disable jwac

Success.

DGS-3620-28SC:admin#
```

## 47-3 enable jwac redirect

### Description

This command is used to enable JWAC redirect. When **redirect quarantine_server** is enabled, the unauthenticated host will be redirected to a quarantine server when it tries to access a random URL. When **redirect jwac_login_page** is enabled, the unauthenticated host will be redirected to the **jwac_login_page** on the Switch to finish authentication.

### Format

**enable jwac redirect**

### Parameters

None.

### Restrictions

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

### Example

To enable JWAC redirect:

```
DGS-3620-28SC:admin#enable jwac redirect
Command: enable jwac redirect

Success.

DGS-3620-28SC:admin#
```

## 47-4 disable jwac redirect

### Description

This command is used to disable JWAC redirect. When redirect is disabled, only access to **quarantine_server** and the **jwac_login_page** from an unauthenticated host is allowed, all other Web access will be denied.

### Format

**disable jwac redirect**

### Parameters

None.

### Restrictions

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

### Example

To disable JWAC redirect:

```
DGS-3620-28SC:admin#disable jwac redirect
Command: disable jwac redirect

Success.

DGS-3620-28SC:admin#
```

## 47-5 enable jwac forcible_logout

### Description

This command is used to enable JWAC forcible logout. When enabled, a Ping packet from an authenticated host to the JWAC Switch with TTL=1 will be regarded as a logout request, and the host will be moved back to unauthenticated state.

### Format

**enable jwac forcible_logout**

### Parameters

None.

### Restrictions

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

### Example

To enable JWAC forcible logout:

```
DGS-3620-28SC:admin#enable jwac forcible_logout
Command: enable jwac forcible_logout

Success.

DGS-3620-28SC:admin#
```

## 47-6 disable jwac forcible_logout

### Description

This command is used to disable JWAC forcible logout.

### Format

**disable jwac forcible_logout**

### Parameters

None.

### Restrictions

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

### Example

To disable JWAC forcible logout:

```
DGS-3620-28SC:admin#disable jwac forcible_logout
Command: disable jwac forcible_logout

Success.

DGS-3620-28SC:admin#
```

## 47-7 enable jwac udp_filtering

### Description

This command is used to enable the JWAC UDP filtering function. When UDP filtering is enabled, all UDP and ICMP packets except DHCP and DNS packets from unauthenticated hosts will be dropped.

### Format

**enable jwac udp_filtering**

### Parameters

None.

### Restrictions

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

### Example

To enable JWAC UDP filtering:

```
DGS-3620-28SC:admin#enable jwac udp_filtering
Command: enable jwac udp_filtering

Success.

DGS-3620-28SC:admin#
```

## 47-8 disable jwac udp_filtering

### Description

This command is used to disable JWAC UDP filtering.

### Format

**disable jwac udp_filtering**

### Parameters

None.

### Restrictions

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

### Example

To disable JWAC UDP filtering:

```
DGS-3620-28SC:admin#disable jwac udp_filtering
Command: disable jwac udp_filtering

Success.

DGS-3620-28SC:admin#
```

## 47-9 enable jwac quarantine_server_monitor

### Description

This command is used to enable the JWAC quarantine server monitor. When enabled, the JWAC switch will monitor the quarantine server to ensure the server is okay. If the switch detects no quarantine server, it will redirect all unauthenticated HTTP accesses to the JWAC Login Page forcibly if the redirect is enabled and the redirect destination is configured to be quarantine server.

### Format

**enable jwac quarantine_server_monitor**

### Parameters

None.

### Restrictions

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

### Example

To enable JWAC quarantine server monitoring:

```
DGS-3620-28SC:admin#enable jwac quarantine_server_monitor
Command: enable jwac quarantine_server_monitor

Success.

DGS-3620-28SC:admin#
```

## 47-10 disable jwac quarantine_server_monitor

### Description

This command is used to disable JWAC quarantine server monitoring.

### Format

**disable jwac quarantine_server_monitor**

### Parameters

None.

### Restrictions

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

### Example

To disable JWAC quarantine server monitoring:

```
DGS-3620-28SC:admin#disable jwac quarantine_server_monitor
Command: disable jwac quarantine_server_monitor

Success.

DGS-3620-28SC:admin#
```

## 47-11 config jwac quarantine_server_error_timeout

### Description

This command is used to set the quarantine server error timeout. When the quarantine server monitor is enabled, the JWAC switch will periodically check if the quarantine works okay. If the switch does not receive any response from quarantine server during the configured error timeout, the switch then regards it as not working properly.

### Format

**config jwac quarantine_server_error_timeout <sec 5-300>**

### Parameters

**<sec 5-300>** - Specify the error timeout interval.

### Restrictions

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

### Example

To set the quarantine server error timeout:

```
DGS-3620-28SC:admin#config jwac quarantine_server_error_timeout 60
Command: config jwac quarantine_server_error_timeout 60

Success.

DGS-3620-28SC:admin#
```

## 47-12 config jwac

### Description

This command is used to configure the quarantine server URL. If the redirection is enabled and the redirection destination is a quarantine server, when a HTTP request from an unauthenticated host which is not headed to a quarantine server reaches the Switch, the Switch will handle this HTTP packet and send back a message to the host to make it access the quarantine server with the configured URL. When the PC connected to the specified URL, the quarantine server will request the PC user to input the user name and password to authenticate.

**Note:** If the quarantine server is linked to the JWAC enabled port on the switch, it must be added to the static FDB correctly before it can work properly.

### Format

**config jwac [quarantine_server_url <string 128> | clear_quarantine_server_url]**

### Parameters

**quarantine_server_url** - Specify the entire URL of the authentication page on the quarantine server.
  **<string 128>** - Specify the entire URL of the authentication page on the quarantine server. The quarantine server URL can be up to 128 characters long.

**clear_quarantine_server_url** - Specify to clear the current quarantine server URL.

### Restrictions

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

### Example

To configure the quarantine server URL:

```
DGS-3620-28SC:admin#config jwac quarantine_server_url
http://10.90.90.88/authpage.html
Command: config jwac quarantine_server_url http://10.90.90.88/authpage.html

Success.

DGS-3620-28SC:admin#
```

## 47-13 config jwac redirect

### Description

This command is used to configure redirect destination and delay time before an unauthenticated host is redirected to the quarantine server or the JWAC login web page. The unit of delay time is seconds. 0 means no delaying the redirect.

### Format

**config jwac redirect {destination [quarantine_server | jwac_login_page] | delay_time <sec 0-10>}(1)**

### Parameters

**destination** - Specify the destination which the unauthenticated host will be redirected to.
  **quarantine_server** - Specify the unauthenticated host will be redirected to the quarantine_server.
  **jwac_login_page** - Specify the unauthenticated host will be redirected to the jwac_login_page.

**delay_time** - Specify the time interval after which the unauthenticated host will be redirected.
  **<sec 0-10>** - Specify the time interval after which the unauthenticated host will be redirected. The delay time must be between 0 and 10 seconds.

### Restrictions

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

### Example

To configure JWAC redirect destination to JWAC login web page and a delay time of 5 seconds:

```
DGS-3620-28SC:admin#config jwac redirect destination jwac_login_page delay_time
5
Command: config jwac redirect_ destination jwac_login_page delay_time 5

Success.

DGS-3620-28SC:admin#
```

## 47-14 config jwac virtual_ip

### Description

This command is used to configure JWAC virtual IP addresses used to accept authentication requests from an unauthenticated host. The virtual IP of JWAC is used to accept authentication request from unauthenticated host. Only requests sent to this IP will get correct responses. This IP does not respond to ARP requests or ICMP packets.

### Format

**config jwac virtual_ip <ipaddr> {url [<string 128> | clear]}**

### Parameters

**<ipaddr>** - Specify the IP address of the virtual IP.

**url** - (Optional) Specify the URL of the virtual IP.
  **<string 128>** - Specify the URL of the virtual IP.
  **clear** - Clear the URL of the virtual IP.

### Restrictions

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

### Example

To configure a JWAC virtual IP address of 1.1.1.1 to accept authentication requests from an unauthenticated host:

```
DGS-3620-28SC:admin#config jwac virtual_ip 1.1.1.1
Command: config jwac virtual_ip 1.1.1.1

Success.

DGS-3620-28SC:admin#
```

## 47-15 config jwac update_server

### Description

This command is used to add or delete a server network address to which the traffic from an unauthenticated client host will not be blocked by the JWAC Switch. Any servers running ActiveX need to be able to have access to accomplish authentication. Before the client passes authentication, it should be added to the Switch with its IP address. For example, the client may need to access update.microsoft.com or some sites of the Anti-Virus software companies to check whether the OS or Anti-Virus software of the client are the latest; and so IP addresses of update.microsoft.com and of Anti-Virus software companies need to be added in the Switch.

### Format

**config jwac update_server [add | delete] ipaddress <network_address> {[tcp_port <port_number 1-65535> | udp_port <port_number 1-65535>]}**

### Parameters

| |
|---|
| **add** - Specify to add a network address to which the traffic will not be blocked. Up to 100 network addresses can be added. |
| **delete** - Specify to delete a network address to which the traffic will not be blocked. |
| **ipaddress** - Specify the network address to add or delete.<br>**<network_address>** - Enter the network address here. |
| **tcp_port** - (Optional) Specify a TCP port number between 1 and 65535.<br>**<port_number 1-65535>** - Specify a TCP port value between 1 and 65535. |
| **udp_port** - (Optional) Specify a UDP port number between 1 and 65535.<br>**<port_number 1-65535>** - Specify a UDP port value between 1 and 65535. |

### Restrictions

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

### Example

To configure servers the PC may need to connect to in order to complete JWAC authentication:

```
DGS-3620-28SC:admin#config jwac update_server add ipaddress 10.90.90.109/24
Command: config jwac update_server add ipaddress 10.90.90.109/24

 Update Server 10.90.90.0/24 is added.

Success.

DGS-3620-28SC:admin#
```

## 47-16 config jwac switch_http_port

### Description

This command is used to configure the TCP port which the JWAC switch listens to. This port number is used in the second stage of the authentication. PC users will connect to the page on the switch to input the user name and password. If not specified, the default port number is 80. If no protocol is specified, the protocol is HTTP.

### Format

**config jwac switch_http_port <tcp_port_number 1-65535> {[http | https]}**

### Parameters

| |
|---|
| **<tcp_port_number 1-65535>** - Specify a TCP port which the JWAC switch listens to and uses to finish the authenticating process. |
| **http** - (Optional) Specify the JWAC run HTTP protocol on this TCP port. |
| **https** - (Optional) Specify the JWAC run HTTPS protocol on this TCP port. |

### Restrictions

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

### Example

To configure the TCP port which the JWAC switch listens to:

```
DGS-3620-28SC:admin#config jwac switch_http_port 8888 http
Command: config jwac switch_http_port 8888 http

Success.

DGS-3620-28SC:admin#
```

## 47-17 config jwac ports

### Description

This command is used to configure port state of JWAC.

### Format

**config jwac ports [<portlist> | all] {state [enable | disable] | max_authenticating_host <value 0-100> | aging_time [infinite | <min 1-1440>] | idle_time [infinite | <min 1-1440>] | block_time [<sec 0-300>]}(1)**

### Parameters

| |
|---|
| **<portlist>** - Specify a port range for setting the JWAC state.<br>**all** - Specify to configure all switch ports' JWAC state. |
| **state** - Specify the port state of JWAC.<br>**enable** - Specify to enable the JWAC port state.<br>**disable** - Specify to disable the JWAC port state. |
| **max_authenticating_host** - Specify the maximum number of hosts that can process authentication on each port at the same time. The default value is 100.<br>**<value 0-100>** - Specify the maximum number of authenticating hosts, between 0 and 100. |
| **aging_time** - Specify a time period during which an authenticated host will keep in authenticated state.<br>**infinite** - Specify to indicate the authenticated host on the port will never ageout.<br>**<min 1-1440>** - Specify an aging time between 1 and 1440 minutes. The default value is 1440 minutes. |
| **idle_time** - If there is no traffic during idle time, the host will be moved back to unauthenticated state.<br>**infinite** - Specify to indicate the idle state of the authenticated host on the port will never be checked. The default value is infinite.<br>**<min 1-1440>** - Specify an idle time between 1 and 1440 minutes. |

**block_time** - If a host fails to pass the authentication, it will be blocked for a period specified by the blocking time.The default value is 60 seconds.
**<sec 0-300>** - Specify a blocking time value between 0 and 300.

### Restrictions

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

### Example

To configure the JWAC port state:

```
DGS-3620-28SC:admin#config jwac ports 1-9 state enable
Command: config jwac ports 1-9 state enable

Success.

DGS-3620-28SC:admin#
```

## 47-18 config jwac radius_protocol

### Description

This command is used to specify the RADIUS protocol used by JWAC to complete RADIUS authentication.

### Format

**config jwac radius_protocol [local | eap_md5 | pap | chap | ms_chap | ms_chapv2]**

### Parameters

**local** - Specify the JWAC switch uses the local user DB to complete the authentication.

**eap_md5** - Specify the JWAC switch uses EAP MD5 to communicate with the RADIUS server.

**pap** - Specify the JWAC switch uses PAP to communicate with the RADIUS server.

**chap** - Specify the JWAC switch uses CHAP to communicate with the RADIUS server.

**ms_chap** - Specify the JWAC switch uses MS-CHAP to communicate with the RADIUS server.

**ms_chapv2** - Specify the JWAC switch uses MS-CHAPv2 to communicate with the RADIUS server.

### Restrictions

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

### Example

To configure the RADIUS protocol used by JWAC:

```
DGS-3620-28SC:admin# config jwac radius_protocol ms_chapv2
Command: config jwac radius_protocol ms_chapv2

Success.
```

```
DGS-3620-28SC:admin#
```

## 47-19 create jwac user

### Description

This command creates JWAC users in the local database. When “local” is chosen while configuring the JWAC RADIUS protocol, the local database will be used.

### Format

**create jwac user <username 15> {vlan <vlanid 1-4094>}**

### Parameters

**<username 15> -** Specify the user name to be created.

**vlan** - (Optional) Specify the target VLAN ID for the authenticated host which uses this user account to pass authentication.

**<vlanid 1-4094> -** Specify the target VLAN ID for the authenticated host which uses this user account to pass authentication. The VLAN ID value must be between 1 and 4094.

### Restrictions

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

### Example

To create a JWAC user in the local DB:

```
DGS-3620-28SC:admin# create jwac user 112233
Command: create jwac user 112233

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

DGS-3620-28SC:admin#
```

## 47-20 config jwac user

### Description

This command configures a JWAC user.

### Format

**config jwac user <username 15> {vlan <vlanid 1-4094>}**

### Parameters

**<username 15> -** Specify the user name to be configured.

**vlan** - (Optional) Specify the target VLAN ID for the authenticated host which uses this user account to pass authentication.

**<vlanid 1-4094>** - Specify the target VLAN ID for the authenticated host which uses this user account to pass authentication. The VLAN ID value must be between 1 and 4094.

### Restrictions

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

### Example

To configure a JWAC user:

```
DGS-3620-28SC:admin#config jwac user 112233
Command: config jwac user 112233

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

DGS-3620-28SC:admin#
```

## 47-21 delete jwac

### Description

This command is used to delete JWAC users from the local database.

### Format

**delete jwac [user <username 15> | all_users]**

### Parameters

**user** - Specify the user name to be deleted.

**<username 15>** - Specify the user name to be deleted. The user name can be up to 15 characters long.

**all_users** - Specify all user accounts in the local database will be deleted.

### Restrictions

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

### Example

To delete a JWAC user from the local database:

```
DGS-3620-28SC:admin#delete jwac user 112233
Command: delete jwac user 112233

Success.

DGS-3620-28SC:admin#
```

## 47-22 show jwac user

### Description

This command is used to display JWAC users in the local database.

### Format

**show jwac user**

### Parameters

None.

### Restrictions

None.

### Example

To display the current JWAC local users:

```
DGS-3620-28SC:admin#show jwac user
Command: show jwac user

Current Accounts:

Username            Password         VID
----------------    ---------------  ---------
123                 w                1
rer                                  -

Total Entries:2

DGS-3620-28SC:admin#
```

## 47-23 show jwac

### Description

This command is used to display the JWAC configuration settings.

### Format

**show jwac**

### Parameters

None.

### Restrictions

None.

### Example

To display the current JWAC configuration:

```
DGS-3620-28SC:admin#show jwac
Command: show jwac

State                   : Disabled
  Enabled Ports           :
  Virtual IP/URL          : 0.0.0.0/-
  Switch HTTP Port        : 80 (HTTP)
  UDP Filtering           : Enabled
  Forcible Logout         : Enabled
  Redirect State          : Enabled
  Redirect Delay Time     : 1 Seconds
  Redirect Destination    : Quarantine Server
  Quarantine Server       :
  Q-Server Monitor        : Disabled
  Q-Server Error Timeout  : 5 Seconds
  RADIUS Auth-Protocol    : PAP
  RADIUS Authorization    : Enabled
  Local Authorization     : Enabled

DGS-3620-28SC:admin#
```

## 47-24 show jwac auth_state ports

### Description

This command is used to display information for JWAC client hosts.

### Format

**show jwac auth_state ports {<portlist>}**

### Parameters

**<portlist>** - (Optional) Specify a port range to show the JWAC authentication entries.

✎ **Note:** If no port is specified, the JWAC authentication state will be displayed for all ports.

### Restrictions

None.

### Example

To display JWAC authentication entries for ports 1 to 2:

```
DGS-3620-28SC:admin#show jwac auth_state ports 1-2
Command: show jwac auth_state ports 1-2

Pri:Priority. State – A:Authenticated. B:Bloacked. -:Authenticating
Time – Aging Time/Idle Time for authenticated entries.

Port  MAC Address      State VID Pri  Time          IP           User Name
----- -----------------   -- ---- -- -------- ------------------- -------------
-
1     00-00-00-00-00-42   -  -   -  4         -                  -
1     00-00-12-34-56-02   -  -   -  21        -                  -
2     00-00-DF-12-E5-6A   -  -   -  24        -                  -
2     00-03-38-10-28-01   -  -   -  13        -                  -

Total Authenticating Hosts  : 4
Total Authenticated Hosts   : 0
Total Blocked Hosts         : 0

DGS-3620-28SC:admin#
```

## 47-25 show jwac update_server

### Description

This command is used to display the JWAC update server.

### Format

**show jwac update_server**

### Parameters

None.

### Restrictions

None.

### Example

To display the JWAC update server:

```
DGS-3620-28SC:admin#show jwac update_server
Command: show jwac update_server

Index  IP                 TCP/UDP  Port  State
-----  ------------------  ------  ----  -------
1      172.18.0.0/21       TCP     1     Active
2      172.18.0.0/21       TCP     2     Active
```

```
3       172.18.0.0/21       TCP     3     Active

DGS-3620-28SC:admin#
```

## 47-26 show jwac ports

### Description

This command is used to display the port configuration of JWAC.

### Format

**show jwac ports {<portlist>}**

### Parameters

**<portlist>** - (Optional) Specify a port range to show the configuration of JWAC.

### Restrictions

None.

### Example

To display JWAC ports 1 to 4:

```
DGS-3620-28SC:admin#show jwac ports 1-4
Command: show jwac ports 1-4

 Port   State     Aging Time  Idle Time  Block Time  Max
                     (min)      (min)      (sec)     Hosts
 -----  --------  ----------  ---------  ----------  -----
 1      Disabled  1440        Infinite   60          100
 2      Disabled  1440        Infinite   60          100
 3      Disabled  1440        Infinite   60          100
 4      Disabled  1440        Infinite   60          100

DGS-3620-28SC:admin#
```

## 47-27 clear jwac auth_state

### Description

This command is used to clear authentication entries.

### Format

**clear jwac auth_state [ports [all | <portlist>] {authenticated | authenticating | blocked} | mac_addr <macaddr>]**

### Parameters

**ports** - Specify the port range to delete hosts on.
  **all** - Specify to delete all ports.
  **<portlist>** - Specify range of ports to delete.

**authenticated** - (Optional) Specify the state of host to delete.

**authenticating** - (Optional) Specify the state of host to delete.

**blocked** - (Optional) Specify the state of host to delete.

**mac_addr** - Delete a specified host with this MAC address.
  **<macaddr>** - Enter the MAC address here.

### Restrictions

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

### Example

To delete authentication entries:

```
DGS-3620-28SC:admin#clear jwac auth_state ports all blocked
Command: clear jwac auth_state ports all blocked

Success.

DGS-3620-28SC:admin#
```

## 47-28 config jwac authenticate_page

### Description

This command is used by administrators to decide which authenticate page to use.

### Format

**config jwac authenticate_page [japanese | english]**

### Parameters

**japanese** - Specify to change to the Japanese page.

**english** - Specify to change to the English page. This is the default page.

### Restrictions

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

### Example

To customize the authenticate page:

```
DGS-3620-28SC:admin#config jwac authenticate_page japanese
Command: config jwac authenticate_page japanese

Success.

```

```
DGS-3620-28SC:admin#
```

## 47-29 show jwac authenticate_page

### Description

This command is used to display the element mapping of the customized authenticate page.

### Format

**show jwac authenticate_page**

### Parameters

None.

### Restrictions

None.

### Example

To display the element mapping of the customized authenticate page:

```
DGS-3620-28SC:admin#show jwac authenticate_page
Command: show jwac authenticate_page

 Current Page : English Version
English Page Element
-----------------------------------------------------------
Page Title              :
Login Window Title      : Authentication Login
User Name Title        : User Name
Password Title         : Password
Logout Window Title    : Logout from the network
Notification           :


Japanese Page Element
-----------------------------------------------------------
Page Title              :
Login Window Title      : 社内 LAN 認証ログイン
User Name Title         : ユーザ ID
Password Title          : パスワード
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

## 47-30 config jwac authentication_page element

### Description

This command is used by administrators to customize the JWAC authenticate page.

## Format

**config jwac authentication_page element [japanese | english] [default | page_title <desc 128> | login_window_title <desc 32> | user_name_title <desc 16> | password_title <desc 16> | logout_window_title <desc 32> | notification_line <value 1-5> <desc 128>]**

## Parameters

**japanese** - Specify to change to the Japanese page.
**english** - Specify to change to the English page.

**default** - Specify to reset the page element to default.

**page_title** - Specify the title of the authenticate page.
  **<desc 128>** - Specify the title of the authenticate page. The page title description can be up to 128 characters long.

**login_window_title** - Specify the login window title of the authenticate page.
  **<desc 32>** - Specify the login window title of the authenticate page. The login window title description can be up to 32 characters long.

**user_name_title** - Specify the user name title of the authenticate page.
  **<desc 16>** - Specify the user name title of the authenticate page. The user name title description can be up to 16 characters long.

**password_title** - Specify the password title of the authenticate page.
  **<desc 16>** - Specify the password title of the authenticate page. The password title description can be up to 16 characters long.

**logout_window_title** - Specify the logout windown title mapping of the authenticate page.
  **<desc 32>** - Specify the logout windown title mapping of the authenticate page. The logout window title description can be up to 32 characters long.

**notification_line** - Specify this parameter to set the notification information by line in authentication Web pages.
  **<value 1-5>** - Specify a notification line value between 1 and 5.
  **<desc 128>** - Specify a notification line description up to 128 characters long.

## Restrictions

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

## Example

To customize the authenticate page:

```
DGS-3620-28SC:admin# config jwac authentication_page element japanese
page_title  ディーリンクジャパン株式会社
Command: config jwac authentication_page element japanese page_title  ディーリン
クジャパン株式会社

Success.

DGS-3620-28SC:admin# config jwac authentication_page element japanese
login_window_title JWAC 认证
Command: config jwac authentication_page element japanese login_window_title
JWAC 认证

Success.

DGS-3620-28SC:admin# config jwac authentication_page element japanese
```

```
user_name_title ユーザ名
Command: config jwac authentication_page element japanese user_name_title ユーザ
名

Success.

DGS-3620-28SC:admin# config jwac authentication_page element japanese
password_title パスワード
Command: config jwac authentication_page element japanese password_title パスワー
ド

Success.

DGS-3620-28SC:admin# config jwac authentication_page element japanese
logout_window_title ログアウト
Command: config jwac authentication_page element japanese logout_window_title ロ
グアウト

Success.

DGS-3620-28SC:admin#
```

## 47-31 config jwac authorization attributes

### Description

This command is used to enable or disable acceptation of authorized configuration. When the authorization is enabled for JWAC'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 JWAC's local, the authorized data assigned by the local database will be accepted.

### Format

**config jwac authorization attributes {radius [enable | disable] | local [enable | disable]}(1)**

### Parameters

**radius** - If 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 RADUIS server to be accepted.
**disable** - Specify to disable authorized data assigned by the RADUIS 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 Administrator, Operator and Power-User level users can issue this command.

### Example

To disable the configuration authorized from the local database:

```
DGS-3620-28SC:admin#config jwac authorization attributes local disable
Command: config jwac authorization attributes local disable

Success.

DGS-3620-28SC:admin#
```

# Chapter 48 Jumbo Frame Commands

**enable jumbo_frame**

**disable jumbo_frame**

**config jumbo_frame ports** [<portlist> | all] state [enable | disable]

**show jumbo_frame** {<portlist>}

## 48-1 enable jumbo_frame

### Description

This command is used to enable support of Jumbo Frames.

### Format

**enable jumbo_frame**

### Parameters

None.

### Restrictions

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

### Example

To enable Jumbo Frames:

```
DGS-3620-28SC:admin#enable jumbo_frame
Command: enable jumbo_frame

DGS-3620-28SC:admin#
```

## 48-2 disable jumbo_frame

### Description

This command is used to disable support of Jumbo Frames.

### Format

**disable jumbo_frame**

### Parameters

None.

### Restrictions

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

### Example

To disable Jumbo Frames:

```
DGS-3620-28SC:admin#disable jumbo_frame
Command: disable jumbo_frame

Success.

DGS-3620-28SC:admin#
```

## 48-3 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>** - Enter the list of ports used for this configuration here.
**all** - Specifies that all the ports will be used for this configuration.

**state** - Specifies the jumbo frame state to be applied to a range of ports specified.
**enable** - Specifies that the jumbo frame state will be enabled.
**disable** - Specifies that the jumbo frame state will be disabled.

### Restrictions

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

### Example

To enable jumbo frames on ports 1:1-1:5:

```
DGS-3620-28SC:admin# config jumbo_frame ports 1:1-1:5 state enable
Command: config jumbo_frame ports 1:1-1:5 state enable

Success.

DGS-3620-28SC:admin#
```

## 48-4 show jumbo_frame

### Description

This command is used to display Jumbo Frames.

### Format

**show jumbo_frame {<portlist>}**

### Parameters

**<portlist>** - (Optional) Enter the list of ports to be displayed here.

### Restrictions

None.

### Example

To display Jumbo Frames for port 1 to 5:

```
DGS-3620-28SC:admin#show jumbo_frame 1-5
Command: show jumbo_frame 1-5

 Jumbo Frame Global State : Disabled

 Maximum Jumbo Frame Size : 1536 Bytes

 Port       Jumbo Frame State
 -------    --------------------
 1          Enabled
 2          Enabled
 3          Enabled
 4          Enabled
 5          Enabled

DGS-3620-28SC:admin#
```

# Chapter 49 LACP Configuration Commands

| |
|---|
| **config lacp_port** <portlist> mode [active \| passive] |
| **show lacp_port** {<portlist>} |

## 49-1 config lacp_port

### Description

This command is used to configure per-port LACP mode.

### Format

**config lacp_port <portlist> mode [active | passive]**

### Parameters

| |
|---|
| **<portlist>** - Specify a range of ports to be configured. |
| **mode** – Specify the port mode.<br>**active** - Specify the mode as active.<br>**passive** - Specify the mode as passive. |

### Restrictions

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

### Example

To configure port LACP mode for ports 1 to 3:

```
DGS-3620-28SC:admin#config lacp_port 1-3 mode active
Command: config lacp_port 1-3 mode active

Success.

DGS-3620-28SC:admin#
```

## 49-2 show lacp_port

### Description

This command is used to display per-port LACP mode.

### Format

**show lacp_port {<portlist>}**

## Parameters

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

**Note:** If no parameter is specified, the system will display current LACP mode for all ports.

## Restrictions

None.

## Example

To display the current LACP mode for ports 1 to 3 on the switch:

```
DGS-3620-28SC:admin#show lacp_port 1-3
Command: show lacp_port 1-3

Port    Activity
------  --------
1       Active
2       Active
3       Active

DGS-3620-28SC:admin#
```

# Chapter 50 Layer 2 Protocol Tunneling (L2PT) Command List

**config l2protocol_tunnel ports** [<portlist> | all] type [uni tunneled_protocol [{stp | gvrp | protocol_mac [01-00-0C-CC-CC-CC | 01-00-0C-CC-CC-CD]}(1) | all] {threshold <value 0-65535>} | nni | none]

**show l2protocol_tunnel** {[uni | nni]}

**enable l2protocol_tunnel**

**disable l2protocol_tunnel**

## 50-1 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

**ports** -Specify the ports on which the Layer 2 protocol tunneling will be configured.
  **<portlist>** - Enter a list of ports to be configured here.
  **all** - Specify to use this configuration on all the ports.

**type** - Specify the type of the ports.
**uni** - Specify the port is UNI port
**tunneled_protocol** - Specify tunneled protocols on this UNI port. If specified all, all tunnel-able Layer 2 protocols will be tunneled on this port.
  **stp** - (Optional) Specify to use the STP protocol.
  **gvrp** - (Optional) Specify to use the GVRP protocol.
  **protocol_mac** - (Optional) Specify which protocol MAC address to use.
    **01-00-0C-CC-CC-CC** - Specify to use this protocol MAC address.
    **01-00-0C-CC-CC-CD** - Specify to use this protocol MAC address.
**all** - Specify to use all the MAC addresses.

**threshold** - (Optional) Specify the drop threshold for packets-per-second accepted on this UNI port. The port drops the PDU if the protocol’s threshold is exceeded. The range of the threshold value is 0 to 65535 (packet/second). The value 0 means on limit. By default, the value is 0.

**<value 0-65535>** - Enter the threshold packets-per-seconds value here. This value must be between 0 and 65535.

**nni** - Specify the port is NNI port

**none** - Disables tunnel on it. By default, a port is none port.

### Restrictions

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

### Example

To configure the STP tunneling on ports 1-4:

```
DGS-3620-28SC: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-3620-28SC:admin#
```

## 50-2 show l2protocol_tunnel

### Description

This command is used to show Layer 2 protocol tunneling information.

### Format

**show l2protocol_tunnel {[uni | nni]}**

### Parameters

**uni** - (Optional) Specify show UNI detail information, include tunneled and dropped PDU statistic.

**nni** - (Optional) Specify show NNI detail information, include de-capsulated Layer 2 PDU statistic.

### Restrictions

None.

### Example

To show Layer 2 protocol tunneling information summary:

```
DGS-3620-28SC:admin# show l2protocol_tunnel
Command: show l2protocol_tunnel

Global State: Enabled
UNI Ports: 1-2
NNI Ports: 3-4

DGS-3620-28SC:admin#
```

To show Layer 2 protocol tunneling detail information on UNI ports:

```
DGS-3620-28SC:admin# show l2protocol_tunnel uni
Command: show l2protocol_tunnel uni

 UNI   Tunneled           Threshold
 Port  Protocol           (packet/sec)
 ----  -----------------  ------------
 1:1   STP                10
       GVRP               10
       01-00-0C-CC-CC-CC  10
 1:2   STP                20
       GVRP               20
       01-00-0C-CC-CC-CC  20
 1:3   STP                0
 1:4   STP                0

DGS-3620-28SC:admin#
```

To show Layer 2 protocol tunneling detail information on NNI ports:

```
DGS-3620-28SC:admin# show l2protocol_tunnel nni
Command: show l2protocol_tunnel nni

NNI     Protocol
Port
----   --------------------
1       STP
        GVRP
        01-00-0C-CC-CC-CC
        01-00-0C-CC-CC-CD
2       STP
        GVRP
        01-00-0C-CC-CC-CC
        01-00-0C-CC-CC-CD

DGS-3620-28SC:admin#
```

## 50-3 enable l2protocol_tunnel

### Description

Used to enable the Layer 2 protocol tunneling function.

### Format

**enable l2protocol_tunnel**

### Parameters

None.

### Restrictions

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

### Example

To enable the Layer 2 protocol tunneling function:

```
DGS-3620-28SC:admin# enable l2protocol_tunnel
Command: enable l2protocol_tunnel

Success.

DGS-3620-28SC:admin#
```

## 50-4 disable l2protocol_tunnel

### Description

Used to disable the Layer 2 protocol tunneling function.

### Format

**disable l2protocol_tunnel**

### Parameters

None.

### Restrictions

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

### Example

To disable the Layer 2 protocol tunneling function:

```
DGS-3620-28SC:admin# disable l2protocol_tunnel
Command: disable l2protocol_tunnel

Success.

DGS-3620-28SC:admin#
```

# Chapter 51 Limited Multicast IP Address Commands

| |
|---|
| **create mcast_filter_profile** {[ipv4 \| ipv6]} profile_id <value 1-60> profile_name <name 32> |
| **config mcast_filter_profile** [profile_id <value 1-60> \| profile_name <name 32>] {profile_name <name 32> \| [add \| delete] <mcast_address_list>}(1) |
| **config mcast_filter_profile ipv6** [profile_id <value 1-60> \| profile_name <name 32>] {profile_name <name 32> \| [add \| delete] <mcastv6_address_list>}(1) |
| **delete mcast_filter_profile** {[ipv4 \| ipv6]} [profile_id [<value 1-60> \| all] \| profile_name <name 32>] |
| **show mcast_filter_profile** {[ipv4 \| ipv6]} {[profile_id <value 1-60> \| profile_name <name 32>]} |
| **config limited_multicast_addr** [ports <portlist> \| vlanid <vlanid_list>] {[ipv4 \| ipv6]} {[add \| delete] [profile_id <value 1-60> \| profile_name <name 32>] \| access [permit \| deny]}(1) |
| **show limited_multicast_addr** [ ports <portlist> \| vlanid <vlanid_list>] {[ipv4 \| ipv6]} |
| **config max_mcast_group** [ports <portlist> \| vlanid <vlanid_list>] {[ipv4 \| ipv6]} {max_group [<value 1-1024> \| infinite] \| action [drop \| replace]} (1) |
| **show max_mcast_group** [ports <portlist> \| vlanid <vlanid_list>] {[ipv4 \| ipv6]} |

## 51-1 create mcast_filter_profile

### Description

This command is used to create a multicast address profile. If the IPv4 or IPv6 option is not specified, IPv4 is implied.

### Format

**create mcast_filter_profile {[ipv4 | ipv6]} profile_id <value 1-60> profile_name <name 32>**

### Parameters

| |
|---|
| **ipv4** – (Optional) Specifies to add an IPv4 multicast profile. |
| **ipv6** – (Optional) Specifies to add an IPv6 multicast profile. |
| **profile_id** – Specifies the ID of the profile.<br>**<value 1-60>** - The profile ID range must be from 1 to 60 |
| **profile_name** - Provides a meaningful description for the profile.<br>**<name 32>** - The profile name can be up to 32 characters long. |

### Restrictions

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

### Example

To create a multicast address profile named MOD:

```
DGS-3620-28SC:admin#create mcast_filter_profile profile_id 2 profile_name MOD
Command: create mcast_filter_profile profile_id 2 profile_name MOD


Success.
```

```
DGS-3620-28SC:admin#
```

## 51-2 config mcast_filter_profile

### Description

This command is used to modify the profile name, add or delete a range of previously defined multicast IP addresses to or from the profile.

### Format

**config mcast_filter_profile [profile_id <value 1-60> | profile_name <name 32>] {profile_name <name 32> | [add | delete] <mcast_address_list>}(1)**

### Parameters

| |
|---|
| **profile_id** - Specify the ID of the profile.<br>**<value 1-60>** - The profile ID must be between 1 and 60. |
| **profile_name** - Specify the name of the profile.<br>**<name 32>** - The profile name can be up to 32 characters long. |
| **profile_name** –Specify a new name of the profile.<br>**<name 32>** - The profile name can be up to 32 characters long.<br>**add** - Specify to add a range of multicast IP addresses.<br>**delete** - Specify to delete a range of multicast IP addresses.<br>**<mcast_address_list>** - List of the multicast addresses to be added to or deleted from the profile. Either specifiy a single multicast IP address or a range of multicast addresses using a hyphen. |

### Restrictions

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

### Example

To add a range of multicast addresses to a profile:

```
DGS-3620-28SC:admin#config mcast_filter_profile profile_id 2 add 225.1.1.1 –
225.1.1.100
Command: config mcast_filter_profile profile_id 2 add 225.1.1.1 – 225.1.1.100

Success.

DGS-3620-28SC:admin#
```

## 51-3 config mcast_filter_profile ipv6

### Description

This command is used to add or delete a range of previously defined IPv6 multicast IP addresses to or from the profile.

### Format

**config mcast_filter_profile ipv6 [profile_id <value 1-60> | profile_name <name 32>] {profile_name <name 32> | [add | delete] <mcastv6_address_list>}(1)**

### Parameters

**profile_id** - Specify the ID of the profile.
**<value 1-60>** - The profile ID must be between 1 and 60.

**profile_name** - Specify the name of the profile.
**<name 32>** - The profile name can be up to 32 characters long.

**profile_name** –Specify a new name of the profile.
**<name 32>** - The profile name can be up to 32 characters long.
**add** - Specify to add a range of multicast IP addresses.
**delete** - Specify to delete a range of multicast IP addresses.
**<mcastv6_address_list>** - List of the IPv6 multicast addresses to be added to or deleted from the profile. Either specifiy a single IPv6 multicast IP address or a range of IPv6 multicast addresses using a hyphen.

### Restrictions

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

### Example

To add the IPv6 multicast address range FF0E::100:0:0:20 – FF0E::100:0:0:22 to profile ID 3:

```
DGS-3620-28SC:admin#config mcast_filter_profile ipv6 profile_id 3 add
FF0E::100:0:0:20 - FF0E::100:0:0:22
Command: config mcast_filter_profile ipv6 profile_id 3 add FF0E::100:0:0:20 -
FF0E::100:0:0:22


Success.


DGS-3620-28SC:admin#
```

## 51-4 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 1-60> | 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. The range is from 1 to 60.
**<value 1-60>** - The profile ID must be between 1 and 60.

**all** - All multicast address profiles will be deleted.

**profile_name** - Specify a profile based on the profile name.
**<name 32>** - The profile name can be up to 32 characters long.

### Restrictions

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

### Example

To delete a multicast profile with a profile ID of 3:

```
DGS-3620-28SC:admin#delete mcast_filter_profile profile_id 3
Command: delete mcast_filter_profile profile_id 3

Success.

DGS-3620-28SC:admin#
```

To delete a multicast profile with a profile named MOD:

```
DGS-3620-28SC:admin#delete mcast_filter_profile profile_name MOD
Command: delete mcast_filter_profile profile_name MOD

Success.

DGS-3620-28SC:admin#
```

## 51-5 show mcast_filter_profile

### Description

This command is used to display 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 1-60> | profile_name <name 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. If both profile_id and profile_name are not specified, all profiles will be displayed.
**<value 1-60>** - The profile ID must be between 1 and 60.

**profile_name** - (Optional) Specify to display a profile based on the profile name. If both profile_id and profile_name are not specified, all profiles will be displayed.
**<name 32>** - The profile name can be up the 32 characters long.

### Restrictions

None.

### Example

To display all the defined multicast address profiles:

```
DGS-3620-28SC: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-3620-28SC:admin#
```

## 51-6 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 or VLAN, it limits the multicast group operated by the IGMP/MLD snooping function and layer 3 function. If the IPv4 or IPv6 option is not specified, IPv4 is implied.

### Format

**config limited_multicast_addr [ports <portlist> | vlanid <vlanid_list>] {[ipv4 | ipv6]} {[add | delete] [profile_id <value 1-60> | profile_name <name 32>] | access [permit | deny]}(1)**

### Parameters

**ports** - Specify a range of ports to configure the multicast address filtering function.
**<portlist>** - Specify a range of ports to be configured.

**vlanid** - Specify the VLAN ID of the VLAN that the multicast address filtering function will be configured on.
**<vlanid_list>** - Enter the VLAN ID of the VLAN that the multicast address filtering functions will be configured on here.

**ipv4** - (Optional) Specify the IPv4 multicast profile.

**ipv6** - (Optional) Specify the IPv6 multicast profile.

**add** - (Optional) Add a multicast address profile to a port or VLAN.

**delete** - (Optional) Delete a multicast address profile from a port or VLAN.

**profile_id** - (Optional) Specify a profile ID to be added to or deleted from the port or VLAN.
**<value 1-60>** - The profile ID must be between 1 and 60.

**profile_name** - (Optional) Specify a profile name to be added to or deleted from the port or VLAN.
**<name 32>** - The profile name can be up to 32 characters long.

**access** - (Optional) Specify whether the access is permit or deny.
**permit** - Specify that the packets that match the addresses defined in the profiles will be permitted.
**deny** - Specify that the packets that match the addresses defined in the profiles will be denied.

### Restrictions

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

### Example

To add multicast address profile 2 to ports 1 and 3:

```
DGS-3620-28SC:admin#config limited_multicast_addr ports 1,3 add profile_id 2
Command: config limited_multicast_addr ports 1,3 add profile_id 2

Success.

DGS-3620-28SC:admin#
```

## 51-7 show limited_multicast_addr

### Description

This command is used to display a multicast address range by ports or by VLANs. When the function is configured on a port or VLAN, it limits the multicast group operated by the IGMP/MLD snooping function and layer 3 function. 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 a range of ports to show the limited multicast address configuration.<br>**<portlist>** - Specify a range of ports to be displayed. |
| **vlanid** - Specify the VLAN ID of VLANs that require information displaying about the multicast address filtering function.<br>**<vlanid_list>** - Enter the VLAN ID of the VLAN here. |
| **ipv4** - (Optional) Specify to display the IPv4 multicast profile associated with the port or VLAN. |
| **ipv6** - (Optional) Specify to display the IPv6 multicast profile associated with the port or VLAN. |

### Restrictions

None.

### Example

To display the limited multicast address range on VLAN 1:

```
DGS-3620-28SC:admin#show limited_multicast_addr vlanid 1
Command: show limited_multicast_addr vlanid 1

VLAN    : 1
Access  : Deny

Profile ID      Name                 Multicast Addresses
-----------    -----------          -----------------------------
1              customer             224.19.62.34 - 224.19.162.200
```

```

DGS-3620-28SC:admin#
```

To display the limited multicast address range on ports 1 and 3:

```
DGS-3620-28SC: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
-----------    -----------          -----------------------------
1              customer             224.19.62.34 – 224.19.162.200


Port    : 3
Access  : Deny

Profile ID      Name                 Multicast Addresses
-----------    ----------------     -----------------------------
1              customer             224.19.62.34 – 224.19.162.200


DGS-3620-28SC:admin#
```

## 51-8 config max_mcast_group

### Description

This command is used to configure the maximum number of multicast groups a port or VLAN 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 oldest group if the action is specified as replace.

### Format

**config max_mcast_group [ports <portlist> | vlanid <vlanid_list>] {[ipv4 | ipv6]} {max_group [<value 1-1024> | infinite] | action [drop | replace]} (1)**

### Parameters

| |
|---|
| **ports** - Specify a range of ports to configure the maximum multicast group.<br>**<portlist>** - Specify a range of ports to be configured. |
| **vlanid** - Specify the VLAN ID to configure the maximum multicast group.<br>**<vlanid_list>** - Enter the VLAN ID of the VLAN 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 the multicast groups.<br>**<value 1-1024>** - The range is from 1 to 1024 or infinite.<br>**infinite** - Infinite is the default setting. |
| **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 oldest group in the register table.

### Restrictions

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

### Example

To configure the maximum number of multicast groups that ports 1 and 3 can join to 100:

```
DGS-3620-28SC:admin# config max_mcast_group ports 1, 3 max_group 100
Command: config max_mcast_group ports 1, 3 max_group 100

Success.

DGS-3620-28SC:admin#
```

## 51-9 show max_mcast_group

### Description

This command is used to display the maximum number of multicast groups that a port or VLAN 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 a range of ports to display the maximum number of multicast groups.
**<portlist>** - Specify a range of ports to be displayed.

**vlanid** - Specify the VLAN ID for displaying the maximum number of multicast groups.
**<vlanid_list>** - Enter the VLAN ID of the VLAN 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 for ports 1-2:

```
DGS-3620-28SC:admin# show max_mcast_group ports 1-2
Command: show max_mcast_group ports 1-2

Port     Max Multicast Group Number  Action
-----    --------------------------- ---------
1        Infinite                     Drop
2        Infinite                     Drop

Total Entries : 2
DGS-3620-28SC:admin#
```

# Chapter 52 Link Aggregation Commands

| |
|---|
| **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 1-32> {master_port <port> \| ports <portlist> \| state [enable \| disable]} (1) |
| **config link_aggregation algorithm** [mac_source \| mac_destination \| mac_source_dest \| ip_source \| ip_destination \| ip_source_dest \| l4_src_port \| l4_dest_port \| l4_src_dest_port] |
| **show link_aggregation** {group_id <value 1-32> \| algorithm} |

## 52-1 create link_aggregation group_id

### Description

This command is used to create a link aggregation group.

### Format

**create link_aggregation group_id <value 1-32> {type [lacp | static]}**

### Parameters

| |
|---|
| **<value 1-32>** - Specify the group ID. The group number identifies each of the groups. The switch allows up to 32 link aggregation groups to be created. |
| **type** - (Optional) Specify the group type belongs to static or LACP. If type is not specified, the default is the static type.<br>**lacp** - Specify the group type as LACP.<br>**static** - Specify the group type as static. |

### Restrictions

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

### Example

To create a link aggregation group:

```
DGS-3620-28SC:admin#create link_aggregation group_id 1 type lacp
Command: create link_aggregation group_id 1 type lacp

Success

DGS-3620-28SC:admin#
```

## 52-2 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>** - Specify the group ID.

### Restrictions

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

### Example

To delete a link aggregation group:

```
DGS-3620-28SC:admin#delete link_aggregation group_id 3
Command: delete link_aggregation group_id 3

Success.

DGS-3620-28SC:admin#
```

## 52-3 config link_aggregation group_id

### Description

This command allows you to configure a link aggregation group that was created with the **create link_aggregation** command above.

### Format

**config link_aggregation group_id <value 1-32> {master_port <port> | ports <portlist> | state [enable | disable]} (1)**

### Parameters

**<value 1-32>** - Specify the group ID. The group number identifies each of the groups. The switch allows up to 32 link aggregation groups to be configured.

**master_port** - 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>** - Specify the master port ID.

**ports** - Specify a range of ports that will belong to the link aggregation group. The port list should include the master port.
**<portlist>** - Specify a range of ports to be configured.

**state** - Enable or disable the specified link aggregation group. If LACP group state is enabled and

the group type is LACP, the ports' state machine will start.
**enable** - Enable the specified link aggregation group.
**disable** - Disable the specified link aggregation group.

### Restrictions

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

### Example

To configure a link aggregation group, group-id 1, master port 7, member ports 5-7:

```
DGS-3620-28SC:admin#config link_aggregation group_id 1 master_port 7 ports 5-7
Command: config link_aggregation group_id 1 master_port 7 ports 5-7

Success.

DGS-3620-28SC:admin#
```

## 52-4 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.

If the load sharing algorithm is based on IP information and the packet is a non-IP packet, it will be based on the source MAC.

If the load sharing algorithm is based on L4 information and the packet is not a TCP/UDP packet:

1) If the packet is a non-IP packet, it will be based on the source MAC.
2) If the packet is an IP packet, it will use the default value of "0" for the TCP/UDP port. It means that if it is not a TCP/UDP IP packet, it will deal with it the same as way as the TCP/UDP packets, but just the TCP/UDP value is 0.

### Format

**config link_aggregation algorithm [mac_source | mac_destination | mac_source_dest | ip_source | ip_destination | ip_source_dest | l4_src_port | l4_dest_port | l4_src_dest_port]**

### 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** - Indicate that the switch should examine the IP source address.

**ip_destination** - Indicate that the switch should examine the IP destination address.

**ip_source_dest** - Indicate that the switch should examine the IP source and destination address.

**l4_src_port** - Indicate that the switch should examine the Layer 4 source port.

**l4_dest_port** - Indicate that the switch should examine the Layer 4 destination port.

**l4_src_dest_port** - Indicate that the switch should examine the Layer 4 source and destination port.

### Restrictions

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

### Example

To configure the link aggregation algorithm to mac-source-dest:

```
DGS-3620-28SC:admin#config link_aggregation algorithm mac_source_dest
Command: config link_aggregation algorithm mac_source_dest

Success.

DGS-3620-28SC:admin#
```

## 52-5 show link_aggregation

### Description

This command is used to display the current link aggregation configuration of 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>** - The switch supports up to 32 link aggregation groups.

**algorithm** - (Optional) Specify the display of link aggregation by the algorithm in use by that group.

**Note:** If no parameter is specified, the system will display all the link aggregation information.

### Restrictions

None.

### Example

To display the current link aggregation configuration when link aggregation is enabled:

```
DGS-3620-28SC: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

Total Entries: 1

DGS-3620-28SC:admin#
```

To display the current link aggregation configuration when link aggregation is disabled:

```
DGS-3620-28SC: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 :

Total Entries: 1

DGS-3620-28SC:admin#
```

# Chapter 53 LLDP Commands

**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>]

**show lldp**

**config lldp forward_message** [enable | disable]

**config lldp notification_interval** <sec 5-3600>

**config lldp ports** [<portlist> | all] [notification [enable | disable] | admin_status [tx_only | rx_only | tx_and_rx | disable] | mgt_addr [ipv4 <ipaddr> | ipv6 <ipv6addr>] [enable | disable] | basic_tlvs [{all} | {port_description | system_name | system_description | system_capabilities}] [enable | disable] | dot1_tlv_pvid [enable | disable] | dot1_tlv_protocol_vid [vlan [all | <vlan_name 32>] | vlanid <vidlist>] [enable | disable] | dot1_tlv_vlan_name [vlan [all | <vlan_name 32>] | vlanid <vidlist>] [enable | disable] | dot1_tlv_protocol_identity [all | {eapol | lacp | gvrp | stp}] [enable | disable] | dot3_tlvs [{all} | {mac_phy_configuration_status | link_aggregation | power_via_mdi | maximum_frame_size}] [enable | disable]]

**show lldp ports** {<portlist>}

**config lldp_med fast_start repeat_count** <value 1-10>

**config lldp_med log state** [enable | disable]

**config lldp_med notification topo_change ports** [<portlist> | all] state [enable | disable]

**config lldp_med ports** [<portlist> | all] med_transmit_capabilities [all | {capabilities | network_policy | power_pse | inventory}(1)] state [enable | disable]

**show lldp_med ports** {<portlist>}

**show lldp_med**

**show lldp_med local_ports** {<portlist>}

**show lldp_med remote_ports** {<portlist>}

**show lldp local_ports** {<portlist>} {mode [brief | normal | detailed]}

**show lldp mgt_addr** {[ipv4 <ipaddr> | ipv6 <ipv6addr>]}

**show lldp remote_ports** {<portlist>} {mode [brief | normal | detailed]}

**show lldp statistics**

**show lldp statistics ports** {<portlist>}

## 53-1 enable lldp

### Description

This command is used to enable LLDP. This is a global control for 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 Administrator, Operator and Power-User level users can issue this command.

### Example

To enable LLDP:

```
DGS-3620-28SC:admin#enable lldp
Command: enable lldp

Success.

DGS-3620-28SC:admin#
```

## 53-2 disable lldp

### Description

This command is used to disable LLDP. The switch will stop the sending and receiving of LLDP advertisement packets.

### Format

**disable lldp**

### Parameters

None.

### Restrictions

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

### Example

To disable LLDP:

```
DGS-3620-28SC:admin#disable lldp
Command: disable lldp

Success.

DGS-3620-28SC:admin#
```

## 53-3 config lldp

### Description

This command is used to configure LLDP timer values. The message TX interval controls how often active ports retransmit advertisements to their neighbors. The message TX hold multiplier is a multiplier on the msgTxInterval that is used to compute the TTL value of txTTL in an LLDPDU.

The TTL will be carried in the LLDPDU packet. The lifetime will be the minimum of 65535 and (message_tx_interval * message_tx_hold_multiplier). On the partner switch, when the time-to-live for a given advertisement expires, the advertised data is deleted from the neighbor switch's MIB. The TX delay is used to change the minimum time (delay-interval) any LLDP port will delay advertising successive LLDP advertisements due to a change in LLDP MIB content. The TX delay defines the minimum interval between sending of LLDP messages due to the constantly changing MIB content. A re-enabled LLDP port will wait for the reinit delay after the last disable command before reinitializing.

## 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** - Specify the message TX interval between consecutive transmissions of LLDP advertisements on any given port.
**<sec 5-32768>** - The range is from 5 to 32768 seconds. The default setting is 30 seconds.

**message_tx_hold_multiplier** - Specify the message TX hold multiplier.
**<int 2-10>** - Specify the range is from 2 to 10. The default setting is 4.

**tx_delay** - Specify the TX delay time.
**<sec 1-8192>** - Specify the range is from 1 to 8192 seconds. The default setting is 2 seconds.
Note: txDelay should be less than or equal to 0.25 * msgTxInterval.

**reinit_delay** - Specify the reinit delay time.
**<sec 1-10>** - Specify the range is from 1 to 10 seconds. The default setting is 2 seconds.

## Restrictions

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

## Example

To change the packet transmission interval:

```
DGS-3620-28SC:admin#config lldp message_tx_interval 30
Command: config lldp message_tx_interval 30

Success.

DGS-3620-28SC:admin#
```

To change the multiplier value:

```
DGS-3620-28SC:admin#config lldp message_tx_hold_multiplier 3
Command: config lldp message_tx_hold_multiplier 3

Success.

DGS-3620-28SC:admin#
```

To configure the delay-interval interval:

```
DGS-3620-28SC:admin#config lldp tx_delay 8
Command: config lldp tx_delay 8

Success.

DGS-3620-28SC:admin#
```

To change the re-initialization delay interval to five seconds:

```
DGS-3620-28SC:admin#config lldp reinit_delay 5
Command: config lldp reinit_delay 5

Success.

DGS-3620-28SC:admin#
```

## 53-4 show lldp

### Description

This command is used to display LLDP.

### Format

**show lldp**

### Parameters

None.

### Restrictions

None.

### Example

To display LLDP:

```
DGS-3620-28SC:admin#show lldp
Command: show lldp

LLDP System Information
    Chassis ID Subtype        : MAC Address
    Chassis ID                : 00-11-22-33-44-55
    System Name               :
    System Description        : Gigabit Ethernet Switch
    System Capabilities       : Repeater, Bridge

LLDP Configurations
    LLDP Status               : Disabled
    LLDP Forward Status       : Disabled
    Message TX Interval       : 30
    Message TX Hold Multiplier: 4
    ReInit Delay              : 2
    TX Delay                  : 2
    Notification Interval     : 5

DGS-3620-28SC:admin#
```

## 53-5 config lldp forward_message

### Description

This command is used to configure LLDP forwarding messages. When LLDP is disabled and LLDP forward message is enabled, the received LLDPDU packet will be forwarded. The default state is disabled.

### Format

**config lldp forward_message [enable | disable]**

### Parameters

**enable** - Enable LLDP forwarding messages.

**disable** - Disable LLDP forwarding messages.

### Restrictions

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

### Example

To enable LLDP forwarding messages:

```
DGS-3620-28SC:admin#config lldp forward_message enable
Command: config lldp forward_message enable

Success.

DGS-3620-28SC:admin#
```

## 53-6 config lldp notification_interval

### Description

This command is used to configure LLDP timer values. This will globally change the interval between successive LLDP change notifications generated by the switch.

### Format

**config lldp notification_interval <sec 5-3600>**

### Parameters

**<sec 5-3600>** - Specify the notification interval range is from 5 to 3600 seconds. The default setting is 5 seconds.

### Restrictions

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

### Example

To change the notification interval to 10 seconds:

```
DGS-3620-28SC:admin#config lldp notification_interval 10
Command: config lldp notification_interval 10

Success.

DGS-3620-28SC:admin#
```

## 53-7 config lldp ports

### Description

Use this command to configure LLDP options by port. Enable or disable each port for sending change notification to configured SNMP trap receiver(s) if an LLDP data change is detected in an advertisement received on the port from an LLDP neighbor. The definition of change includes new available information, information timeout, information update. And the changed type includes any data update /insert/remove.

The admin status options enable to control which ports participate in LLDP traffic and whether the participating ports allow LLDP traffic in only one direction or in both directions.

The config management address command specifies whether system's IP address needs to be advertised from the specified port. For layer 3 devices, each managed address can be individually specified. The management addresses that are added in the list will be advertised in the LLDP from the specified interface, associated with each management address. The interface for that management address will be also advertised in the if-index form.

An active LLDP port on the switch always includes the mandatory data in its outbound advertisements. And there are four optional data that can be configured for an individual port or group of ports to exclude one or more of these data types from outbound LLDP advertisements. The mandatory data type include four basic types of information (end of LLDPDU TLV, chassis ID TLV, port ID TLV, and Time to Live TLV). The mandatory type cannot be disabled. There are also four data types which can be optionally selected. They are port_description, system_name, system_description, and system_capability.

Configure an individual port or group of ports to exclude one or more of IEEE 802.1 Organizationally port vlan ID TLV data types from outbound LLDP advertisements.

Configure an individual port or group of ports to exclude one or more of IEEE 802.1 Organizationally port and protocol VLAN ID TLV data types from outbound LLDP advertisements.

Configure an individual port or group of ports to exclude one or more of IEEE 802.1 Organizationally VLAN name TLV data types from outbound LLDP advertisements.

Configure an individual port or group of ports to exclude one or more of IEEE 802.1 Organizationally protocol identity TLV data types from outbound LLDP advertisements. 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. 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 are enabled on this port and it is enabled to be advertised, then this protocol identity will be advertised.

## Format

```
config lldp ports [<portlist> | all] [notification [enable | disable] | admin_status [tx_only |
rx_only | tx_and_rx | disable] | mgt_addr [ipv4 <ipaddr> | ipv6 <ipv6addr>] [enable | disable]
| basic_tlvs [{all} | {port_description | system_name | system_description |
system_capabilities}] [enable | disable] | dot1_tlv_pvid [enable | disable] |
dot1_tlv_protocol_vid [vlan [all | <vlan_name 32>] | vlanid <vidlist>] [enable | disable] |
dot1_tlv_vlan_name [vlan [all | <vlan_name 32>] | vlanid <vidlist>] [enable | disable] |
dot1_tlv_protocol_identity [all | {eapol | lacp | gvrp | stp}] [enable | disable] | dot3_tlvs [{all} |
{mac_phy_configuration_status | link_aggregation | power_via_mdi | maximum_frame_size}]
[enable | disable]]
```

## Parameters

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

**all** - Specify to set all the ports on the system.

**notification** - Enable or disable the SNMP trap notification of LLDP data changes detected on advertisements received from neighbor devices. The default notification state is disabled.
**enable** - Enable the SNMP trap notification of LLDP data changes detected on advertisements received from neighbor devices.
**disable** - Disable the SNMP trap notification of LLDP data changes detected on advertisements received from neighbor devices.

**admin_status** - Select the desired administrative per port state. The default per port state is tx_and_rx.
**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_address** - The port types specified for advertising indicated management address instance.
**ipv4** - Specify the IP address of IPv4.
**<ipaddr>** - Specify the IP address of IPv4.
**ipv6** - Specify the IP address of IPv6.
**<ipv6addr>** - Specify the IP address of IPv6.
**enable** - Enable port(s) specified for advertising indicated management address instance.
**disable** - Disable port(s) specified for advertising indicated management address instance.

**basic_tlvs** - Configure an individual port or group of ports to exclude one or more of optional TLV data types from outbound LLDP advertisements.
**all** - (Optional) Configure all four TLV data types listed below.
**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** - Enable configuration of an individual port or group of ports to exclude one or more of optional TLV data types from outbound LLDP advertisements.

**disable** - Disable configuration of an individual port or group of ports to exclude one or more of optional TLV data types from outbound LLDP advertisements.

**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 disabled.

**enable** - Enable port VLAN ID TLV transmission on a given LLDP transmission capable port.

**disable** - Disable port VLAN ID TLV transmission on a given LLDP transmission capable port.

**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 disabled.

**vlan** - (Optional) Specify a VLAN to be transmitted.

**all** - (Optional) Specify that all VLAN names will be transmitted.

**<vlan_name 32>** - (Optional) Specify a VLAN name to be transmitted.

**vlanid** - (Optional) Specify a VLAN ID list to be transmitted.

**<vidlist>** - Specify a VLAN ID list to be transmitted.

**enable** - Enable configuration of an individual port or group of ports to exclude one or more of IEEE 802.1 Organizationally port and protocol VLAN ID TLV data types from outbound LLDP advertisements.

**disable** - Disable configuration of an individual port or group of ports to exclude one or more of IEEE 802.1 Organizationally port and protocol VLAN ID TLV data types from outbound LLDP advertisements.

**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 disabled.

**vlan** - (Optional) Specify a VLAN to be transmitted.

**all** - (Optional) Specify that all VLAN names will be transmitted.

**<vlan_name 32>** - (Optional) Specify a VLAN name to be transmitted.

**vlanid** - (Optional) Specify a VLAN ID list to be transmitted.

**<vidlist>** - Specify a VLAN ID list to be transmitted.

**enable** - Enable configuration of an individual port or group of ports to exclude one or more of IEEE 802.1 Organizationally VLAN name TLV data types from outbound LLDP advertisements.

**disable** - Disable configuration of an individual port or group of ports to exclude one or more of IEEE 802.1 Organizationally VLAN name TLV data types from outbound LLDP advertisements.

**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 which are responsible for maintaining the topology and connectivity of the network. If EAPOL, GVRP, STP (including MSTP), and LACP protocol identity are enabled on this port and enabled to be advertised, then the protocol identity will be advertised. The default state is disabled.

**all** - Advertise all of the protocols lists below.

**eapol** - (Optional) Advertise EAPOL.

**lacp** - (Optional) Advertise LACP.

**gvrp** - (Optional) Advertise GVRP.

**stp** - (Optional) Advertise STP.

**enable** - Enable configuration an individual port or group of ports to exclude one or more of IEEE 802.1 Organizationally protocol identity TLV data types from outbound LLDP advertisements.

**disable** - Disable configuration an individual port or group of ports to exclude one or more of IEEE 802.1 Organizationally protocol identity TLV data types from outbound LLDP advertisements.

**dot3_tlvs** - An individual port or group of ports to exclude one or more of IEEE 802.3 Organizationally Specific TLV data types from outbound LLDP advertisements.

**all** – (Optional) Configure all of the TLV optional data types below.

**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 supports 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 an aggregated link, and the aggregated port ID. The default state is disabled.

**power_via_mdi** - (Optional) This TLV optional data type indicates that LLDP agent should transmit 'Power via MDI TLV'. 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** - Enable the configuration of an individual port or group of ports to exclude one or more of IEEE 802.3 Organizationally Specific TLV data types from outbound LLDP advertisements.

**disable** - Disable the configuration of an individual port or group of ports to exclude one or more of IEEE 802.3 Organizationally Specific TLV data types from outbound LLDP advertisements.

## Restrictions

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

## Example

To change the SNMP notification state of ports 1 to 5 to enable:

```
DGS-3620-28SC:admin#config lldp ports 1-5 notification enable
Command: config lldp ports 1-5 notification enable

Success.

DGS-3620-28SC:admin#
```

To configure the mode of ports 1 to 5 to transmit and receive:

```
DGS-3620-28SC:admin#config lldp ports 1-5 admin_status tx_and_rx
Command: config lldp ports 1-5 admin_status tx_and_rx

Success.

DGS-3620-28SC:admin#
```

To enable ports 1 to 5 to manage address entries:

```
DGS-3620-28SC:admin#config lldp ports 1-5 mgt_addr ipv4 192.168.254.10 enable
Command: config lldp ports 1-5 mgt_addr ipv4 192.168.254.10 enable

```

```
Success.

DGS-3620-28SC:admin#
```

To exclude the system name TLV from the outbound LLDP advertisements for all ports:

```
DGS-3620-28SC:admin#config lldp ports all basic_tlvs system_name enable
Command: config lldp ports all basic_tlvs system_name enable

Success.

DGS-3620-28SC:admin#
```

To exclude the VLAN name TLV from the outbound LLDP advertisements for all ports:

```
DGS-3620-28SC:admin#config lldp ports all dot1_tlv_pvid enable
Command: config lldp ports all dot1_tlv_pvid enable

Success.

DGS-3620-28SC:admin#
```

To exclude the port and protocol VLAN ID TLV from the outbound LLDP advertisements for all ports:

```
DGS-3620-28SC: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-3620-28SC:admin#
```

To exclude the VLAN name TLV from the outbound LLDP advertisements for all ports:

```
DGS-3620-28SC: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-3620-28SC:admin#
```

To exclude the protocol identity TLV from the outbound LLDP advertisements for all ports:

```
DGS-3620-28SC:admin#config lldp ports all dot1_tlv_protocol_identity all enable
Command: config lldp ports all dot1_tlv_protocol_identity all enable

Success.

DGS-3620-28SC:admin#
```

To exclude the MAC/PHY configuration/status TLV from the outbound LLDP advertisements for all ports:

```
DGS-3620-28SC: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-3620-28SC:admin#
```

## 53-8 show lldp ports

### Description

This command is used to display LLDP per port configuration for advertisement options.

### Format

**show lldp ports {<portlist>}**

### Parameters

**<portlist>** - (Optional) Specify the ports to be displayed.

**Note:** When a port list is not specified, information for all ports will be displayed.

### Restrictions

None.

### Example

To display LLDP TLV option port 1:

```
DGS-3620-28SC:admin#show lldp ports 1
Command: show lldp ports 1

Port ID                 : 1
--------------------------------------------------------------
Admin Status            : TX_and_RX
Notification Status     : Disabled
Advertised TLVs Option  :
    Port Description                              Disabled
    System Name                                   Disabled
    System Description                            Disabled
    System Capabilities                           Disabled
    Enabled Management Address
        (None)
    Port VLAN ID                                  Disabled
Enabled Port_and_Protocol_VLAN_ID
    (None)
Enabled VLAN Name
    (None)
Enabled Protocol Identity
        (None)
    MAC/PHY Configuration/Status                   Disabled
    Link Aggregation                               Disabled
    Maximum Frame Size                             Disabled

DGS-3620-28SC:admin#
```

## 53-9 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. The default value is 4.

### Format

**config lldp_med fast_start repeat_count <value 1-10>**

### Parameters

| |
|---|
| **<value 1-10>** - Specify a fast start repeat count value between 1 and 10. The default value is 4. |

### Restrictions

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

### Example

To configure a LLDP-MED fast start repeat count of 5:

```
DGS-3620-28SC:admin#config lldp_med fast_start repeat_count 5
Command: config lldp_med fast_start repeat_count 5

Success.

DGS-3620-28SC:admin#
```

## 53-10 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** - Enable the log state for LLDP-MED events.

**disable** - Disable the log state for LLDP-MED events. The default is disabled.

### Restrictions

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

### Example

To enable the log state of LLDP-MED events:

```
DGS-3620-28SC:admin#config lldp_med log state enable
Command: config lldp_med log state enable

Success.

DGS-3620-28SC:admin#
```

## 53-11 config lldp_med notification topo_change ports

### Description

This command is used to enable or disable each port for sending topology change notification to configured SNMP trap receiver(s) if an endpoint device is removed or moved to another port. The default state is disabled.

### Format

**config lldp_med notification topo_change ports [<portlist> | all] state [enable | disable]**

### Parameters

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

**all** - Specify to set all ports in the system.

**state** - Enable or disable the SNMP trap notification of topology change detected state.
**enable** - Enable the SNMP trap notification of topology change detected.
**disable** - Disable the SNMP trap notification of topology change detected. The default notification state is disabled.

### Restrictions

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

### Example

To enable topology change notification on ports 1 to 2:

```
DGS-3620-28SC:admin#config lldp_med notification topo_change ports 1-2 state
enable
Command: config lldp_med notification topo_change ports 1-2 state enable

Success.

DGS-3620-28SC:admin#
```

## 53-12 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** – (Optional) 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** - (Optional) Specify that the LLDP agent should transmit "LLDP-MED network policy TLV."

**power_pse** - This TLV type indicates that LLDP agent should transmit 'LLDP-MED extended Power via MDI TLV' if local device is PSE device.

**inventory** - (Optional) 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 Administrator and Operator-level users can issue this command.

### Example

To enable transmitting of all capabilities on ports 1 to 2:

```
DGS-3620-28SC:admin#config lldp_med ports 1-2 med_transmit_capabilities all
state enable
Command: config lldp_med ports 1-2 med_transmit_capabilities all state enable

Success.

DGS-3620-28SC:admin#
```

## 53-13 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>** - Specify a range of ports to be displayed. |

**Note:** When a port list is not specified, information for all ports will be displayed.

### Restrictions

None.

### Example

To display LLDP-MED configuration information for port 1:

```
DGS-3620-28SC: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 Inventory TLV                       : Enabled
```

```
DGS-3620-28SC:admin#
```

## 53-14 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-3620-28SC:admin#show lldp_med
Command: show lldp_med

LLDP-MED System Information:
    Device Class              : Network Connectivity Device
    Hardware Revision         : A1
    Firmware Revision         : 1.00.012
    Software Revision         : 1.00.034
    Serial Number             : D1234567890
    Manufacturer Name         : D-Link
    Model Name                : DGS-3620-28SC Gigabit Ethernet S
    Asset ID                  :
    PoE Device Type           : PSE Device
    PoE PSE Power Source      : Primary

LLDP-MED Configuration:
    Fast Start Repeat Count   : 4

LLDP-MED Log State:Disabled

DGS-3620-28SC:admin#
```

## 53-15 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>** - Specify a range of ports to be displayed. |

**Note:** When a port list is not 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-3620-28SC: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-3620-28SC:admin#
```

## 53-16 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) Specify a range of ports to be displayed.

**Note:** When a port list is not specified, information for all ports will be displayed.

## Restrictions

None.

## Example

To display remote entry information:

```
DGS-3620-28SC: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-3620-28SC:admin#
```

## 53-17 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) Specify the ports to be displayed. When a port list is not specified, information for all ports will be displayed.

**mode** - (Optional) Select the mode: brief, normal, or detailed.
**brief** - Specify to display the information in brief mode.
**normal** - Specify to display the information in normal mode. This is the default display mode.
**detailed** - Specify to display the information in detailed mode.

### Restrictions

None.

### Example

To display LLDP local port information for port 1:

```
DGS-3620-28SC:admin#show lldp local_ports  1
Command: show lldp local_ports 1

Port ID : 1
-----------------------------------------------------------------------------
Port ID Subtype                            : MAC Address
Port ID                                    : 00-01-02-03-05-00
Port Description                           : D-Link DGS-3620-28SC R1.00.034
                                             Port 1 on Unit 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-3620-28SC:admin#
```

## 53-18 show lldp mgt_addr

### Description

This command is used to display the LLDP management address.

### Format

**show lldp mgmt_addr {[ipv4 <ipaddr> | ipv6 <ipv6addr>]}**

### Parameters

**ipv4** - (Optional) Specify the IPv4 address of the LLDP managament address entry.
**<ipaddr>** - Specify the IPv4 address of the LLDP managament address entry.

**ipv6** - (Optional) Specify the IPv6 address of the LLDP managament address entry.
**<ipv6addr>** - Specify the IPv6 address of the LLDP managament address entry.

### Restrictions

None.

### Example

To display the LLDP management address:

```
DGS-3620-28SC:admin#show lldp mgt_addr
Command: show lldp mgt_addr

Address 1 :
------------------------------------------------------
    Subtype                               : IPv4
    Address                               : 10.19.72.38
    IF Type                               : Unknown
    OID                                   : 1.3.6.1.4.1.171.10.114.1.1
    Advertising Ports                     :
Total Entries : 1

DGS-3620-28SC:admin#
```

## 53-19 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) Specify the ports to be displayed. When a port list is not specified, information for all ports will be displayed.

**mode** - (Optional) Select the mode: brief, normal, or detailed.
**brief** - Specify to display the information in brief mode.
**normal** - Specify to display the information in normal mode. This is the default display mode.
**detailed** - Specify to display the information in detailed mode.

### Restrictions

None.

### Example

To display LLDP information for remote ports 1 and 2:

```
DGS-3620-28SC:admin#show lldp remote_ports 1-2
Command: show lldp remote_ports 1-2

Remote Entities Count : 0



DGS-3620-28SC:admin#
```

## 53-20 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 LLDP statistics:

```
DGS-3620-28SC:admin#show lldp statistics
Command: show lldp statistics

Last Change Time       : 3648
Number of Table Insert : 0
Number of Table Delete : 0
Number of Table Drop   : 0
Number of Table Ageout : 0

DGS-3620-28SC:admin#
```

## 53-21 show lldp statistics ports

### Description

This command is used to display LLDP statistic information for individual ports.

### Format

**show lldp statistics ports {<portlist>}**

### Parameters

**<portlist>** - (Optional) Specify the ports to be displayed.

**Note:** When a port list is not specified, information for all ports will be displayed.

## Restrictions

None.

## Example

To display LLDP statistic information for port 1:

```
DGS-3620-28SC:admin#show lldp statistics ports 1
Command: show lldp statistics ports 1

Port ID : 1
---------------------------------------------
    LLDPStatsTXPortFramesTotal           : 0
    LLDPStatsRXPortFramesDiscardTotal    : 0
    LLDPStatsRXPortFramesErrors          : 0
    LLDPStatsRXPortFramesTotal           : 0
    LLDPStatsRXPortTLVsDiscardedTotal    : 0
    LLDPStatsRXPortTLVsUnrecognizedTotal : 0
    LLDPStatsRXPortAgeoutsTotal          : 0

DGS-3620-28SC:admin#
```

# Chapter 54 Loopback Detection Commands

| |
|---|
| **config loopdetect** {recover_timer [<value 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 log state** [enable \| disable] |

## 54-1 config loopdetect

### Description

This command is used to set up the loop-back detection function (LBD) for the entire switch.

### Format

**config loopdetect {recover_timer [<value 0> | <sec 60-1000000>] | interval <sec 1-32767> | mode [port-based | vlan-based]}(1)**

### Parameters

| |
|---|
| **recover_timer** - The time interval (in seconds) used by the Auto-Recovery mechanism to decide how long to check if the loop status is gone. The default value is 60.<br>**<value 0>** - Zero is a special value which means to disable the auto-recovery mechanism, hence, the user needs to recover the disabled port back manually.<br>**<sec 60-1000000>** - Enter a value between 60 and 1000000. |
| **interval** - The time interval (in seconds) at which device transmits all the CTP (Configuration Test Protocol) packets to detect the loop-back event. The default setting is 10.<br>**<sec 1-32767>** - Specify the valid range between 1 and 32767. |
| **mode** - Choose the loop-detection operation mode.<br>**port-based** - In the port-based mode, the port will be shut-down (disabled) when detecting a loop.<br>**vlan-based** - In VLAN-based mode, the port cannot forward packets of the VLAN that detects a loop. |

### Restrictions

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

### Example

To set a recover time of 0 and an interval of 20 in VLAN-based mode:

```
DGS-3620-28SC:admin#config loopdetect recover_timer 0 interval 20 mode vlan-
based
Command: config loopdetect recover_timer 0 interval 20 mode vlan-based

Success.

DGS-3620-28SC:admin#
```

## 54-2 config loopdetect ports

### Description

This command is used to set up the loop-back detection function for the ports on the switch.

### Format

**config loopdetect ports [<portlist> | all] state [enable | disable]**

### Parameters

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

**all** - To set all ports in the system, use the all parameter.

**state** – Specify the status.
- **enable** - Enable loop-detect for the ports specified in the port list.
- **disable** - Disable loop-detect for the ports specified in the port list. The default is disabled.

### Restrictions

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

### Example

To set up loop-back detection:

```
DGS-3620-28SC:admin#config loopdetect ports 1-5 state enable
Command: config loopdetect ports 1-5 state enable

Success.

DGS-3620-28SC:admin#
```

## 54-3 enable loopdetect

### Description

This command is used to allow the loop detection function to be globally enabled on the switch. The default value is disabled.

### Format

**enable loopdetect**

### Parameters

None.

### Restrictions

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

### Example

To enable loop detection:

```
DGS-3620-28SC:admin#enable loopdetect
Command: enable loopdetect

Success.

DGS-3620-28SC:admin#
```

## 54-4 disable loopdetect

### Description

This command allows the loop detection function to be globally disabled on the switch. The default value is disabled.

### Format

**disable loopdetect**

### Parameters

None.

### Restrictions

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

### Example

To disable loop detection:

```
DGS-3620-28SC:admin#disable loopdetect
Command: disable loopdetect

Success.

DGS-3620-28SC:admin#
```

## 54-5 show loopdetect

### Description

This command is used to display the switch’s current loop detection configuration.

### Format

**show loopdetect**

### Parameters

None.

### Restrictions

None.

### Example

To display the switch’s current loop detection configuration:

```
DGS-3620-28SC:admin#show loopdetect
Command: show loopdetect

 LBD Global Settings
 ---------------------------
 Status         : Disabled
 Mode           : Port-based
 Interval       : 10 sec
 Recover Time   : 60 sec
 Trap State     : None
 Log State      : Enabled

DGS-3620-28SC:admin#
```

## 54-6 show loopdetect ports

### Description

This command is used to display the switch’s current per-port loop detection configuration and status.

### Format

**show loopdetect ports {<portlist>}**

### Parameters

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

### Restrictions

None.

### Example

To display the loop detection state of ports 1 to 9 in port-based mode:

```
DGS-3620-28SC: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-3620-28SC:admin#
```

To display loop detection state of ports 1 to 9 under VLAN-based mode:

```
DGS-3620-28SC:admin#show loopdetect ports 1-9
Command: show loopdetect  ports 1-9

Port   Loopdetect State    Loop VLAN
------ ------------------ ----------
1      Enabled            None
2      Enabled            None
3      Enabled            None
4      Enabled            None
5      Enabled            2
6      Enabled            None
7      Enabled            2
8      Enabled            None
9      Enabled            None

DGS-3620-28SC:admin#
```

## 54-7 config loopdetect trap

### Description

This command is used to configure the trap mode. A loop detected trap is sent when the loop condition is detected and a loop cleared trap is sent when the loop condition is cleared.

### Format

**config loopdetect trap [none | loop_detected | loop_cleared | both]**

### Parameters

**none** - Trap will not be sent for both cases.

**loop_detected** - Trap is sent when the loop condition is detected

**loop_cleared** - Trap is sent when the loop condition is cleared.

**both** - Trap will be sent for both cases.

### Restrictions

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

### Example

To configure a trap:

```
DGS-3620-28SC:admin#config loopdetect trap both
Command: config loopdetect trap both

Success.

DGS-3620-28SC:admin#
```

## 54-1 config loopdetect log state

### Description

This command is used to configure the log state for LBD. The default value is enabled.

### Format

**config loopdetect log state [enable | disable]**

### Parameters

**state** - Specifies the LBD log feature's state.

- **enable** - Specifies that the LBD log feature will be enabled.
- **disable** - Specifies that the LBD log feature will be disabled.

### Restrictions

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

### Example

To enable the log state for LBD:

```
DGS-3620-28SC:admin# config loopdetect log state enable
Command: config loopdetect log state enable

```

```
Success.

DGS-3620-28SC:admin#
```

# Chapter 55 Loopback Interface Commands

**create loopback ipif** <ipif_name 12> {<network_address>} {state [enable | disable]}

**config loopback ipif** <ipif_name 12> [{ipaddress <network_address> **|** state [enable | disable]}(1)]

**show loopback ipif** {<ipif_name 12>}

**delete loopback ipif** [<ipif_name 12> | all]

## 55-1 create loopback ipif

### Description

This command is used to create a loopback interface on the Switch.

### Format

**create loopback ipif <ipif_name 12> {<network_address>} {state [enable | disable]}**

### Parameters

**<ipif_name 12>** - Enter the IP interface name used for this configuration here. This name can be up to 12 characters long.

**<network_address>** - (Optional) Enter the IPv4 network address of the loopback interface here. It specifies a host address and length of network mask.

**state** - (Optional) Specifies the state of the loopback interface.
**enable** - Specifies that the loopback interface state will be enabled.
**disable** - Specifies that the loopback interface state will be disabled.

### Restrictions

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

### Example

To create one loopback interface named loopback1 with subnet address 20.1.1.1/8 and enable the admin state:

```
DGS-3620-28SC:admin# create loopback ipif loopback1 20.1.1.1/8 state enable
Command: create loopback ipif loopback1 20.1.1.1/8 state enable

Success.

DGS-3620-28SC:admin#
```

## 55-2 config loopback ipif

### Description

This command is used to configure the loopback interface parameters.

### Format

**config loopback ipif <ipif_name 12> [{ipaddress <network_address> | state [enable | disable]}(1)]**

### Parameters

**<ipif_name 12>** - Enter the IP interface name used for this configuration here. This name can be up to 12 characters long.

**ipaddress** – (Optional) Specifies the IPv4 network address of the loopback interface.
**<network_address>** - Enter the IPv4 network address of the loopback interface here. It specifies a host address and length of network mask.

**state** - (Optional) Specifies the state of the loopback interface.
**enable** - Specifies that the loopback interface state will be enabled.
**disable** - Specifies that the loopback interface state will be disabled.

### Restrictions

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

### Example

To configure the loopback interface named loopback1 with subnet address 10.0.0.1/8:

```
DGS-3620-28SC:admin# config loopback ipif loopback1 ipaddress 10.0.0.1/8
Command: config loopback ipif loopback1 ipaddress 10.0.0.1/8

Success.

DGS-3620-28SC:admin#
```

## 55-3 show loopback ipif

### Description

This command is used to display the information of the loopback interface.

### Format

**show loopback ipif {<ipif_name 12>}**

### Parameters

**<ipif_name 12>** - (Optional) Enter the IP interface name used for this configuration here. This name can be up to 12 characters long.

### Restrictions

None.

### Example

To show the information of the loopback interface named loopback1:

```
DGS-3620-28SC:admin# show loopback ipif loopback1
Command: show loopback ipif loopback1

Loopback Interface         : loopback1
Interface Admin State      : Enabled
IPv4 Address               : 10.0.0.1/8 (MANUAL)

Total Entries:1

DGS-3620-28SC:admin#
```

## 55-4 delete loopback ipif

### Description

This command is used to delete a loopback interface.

### Format

**delete loopback ipif [<ipif_name 12> | all]**

### Parameters

**<ipif_name 12>** - Enter the IP interface name used for this configuration here. This name can be up to 12 characters long.

**all** – Specifies that all the IP loopback interfaces will be deleted.

### Restrictions

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

### Example

To delete the loopback interface named loopback1:

```
DGS-3620-28SC:admin# delete loopback ipif loopback1
Command: delete loopback ipif loopback1

Success.

DGS-3620-28SC:admin#
```

# Chapter 56 MAC Notification Commands

| |
|---|
| **enable mac_notification** |
| **disable mac_notification** |
| **config mac_notification** {interval <int 1-2147483647> \| historysize <int 1-500>}(1) |
| **config mac_notification ports** [<portlist> \| all] [enable \| disable] |
| **show mac_notification** |
| **show mac_notification ports** {<portlist>} |

## 56-1 enable mac_notification

### Description

This command is used to enable the trap notification for newly learned and cleared MAC addresses on the Switch.

### Format

**enable mac_notification**

### Parameters

None.

### Restrictions

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

### Example

To enable the MAC notification function:

```
DGS-3620-28SC:admin#enable mac_notification
Command: enable mac_notification

Success.

DGS-3620-28SC:admin#
```

## 56-2 disable mac_notification

### Description

This command is used to disable the trap notification for newly learned and cleared MAC addresses on the Switch.

### Format

**disable mac_notification**

### Parameters

None.

### Restrictions

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

### Example

To disable the MAC notification function:

```
DGS-3620-28SC:admin#disable mac_notification
Command: disable mac_notification

Success.

DGS-3620-28SC:admin#
```

## 56-3 config mac_notification

### Description

This command is used to configure the switch's MAC address table notification global settings.

### Format

**config mac_notification {interval <int 1-2147483647> | historysize <int 1-500>}(1)**

### Parameters

| |
|---|
| **interval** - Specify the time interval in seconds to trigger the notification.<br>**<int 1-2147483647>** - Specify between 1 second and 2147483647 seconds. |
| **historysize** - Specify the entries of new learned MAC to trigger the notification.<br>**<int 1-500>** - Specify up to 500 entries. |

### Restrictions

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

### Example

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

```
DGS-3620-28SC:admin#config mac_notification interval 1 historysize 500
Command: config mac_notification interval 1 historysize 500

Success.

DGS-3620-28SC:admin#
```

## 56-4 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>** - Specifiy a range of ports to be configured. |
| **all** - Specify to set all ports in the system. |
| **enable** - Specify to enable the port’s MAC address table notification. |
| **disable** - Specify to disable the port’s MAC address table notification. |

### Restrictions

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

### Example

To enable MAC address table notification for Port 7:

```
DGS-3620-28SC:admin#config mac_notification ports 7 enable
Command: config mac_notification ports 7 enable

Success.

DGS-3620-28SC:admin#
```

## 56-5 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-3620-28SC:admin#show mac_notification
Command: show mac_notification

Global MAC Notification Settings

State        : Enabled
Interval     : 1
History Size : 500

DGS-3620-28SC:admin#
```

## 56-6 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) Specify a range of ports to be configured.

### Restrictions

None.

### Example

To display the MAC address table notification status settings of all ports:

```
DGS-3620-28SC: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

DGS-3620-28SC:admin#
```

# Chapter 57 MAC-based Access Control Commands

**enable mac_based_access_control**

**disable mac_based_access_control**

**config mac_based_access_control password** <passwd 16>

**config mac_based_access_control method** [local | radius]

**config mac_based_access_control guest_vlan ports** <portlist>

**config mac_based_access_control ports** [<portlist> | all] {state [enable | disable] | aging_time [infinite | <min 1-1440>] | block_time <sec 0-300> | max_users [<value 1-4000> | 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]

**config mac_based_access_control max_users** [<value 1-4000> | no_limit]

**config mac_based_access_control authorization attributes** {radius [enable | disable] | local [enable | disable]}(1)

**delete mac_based_access_control_local** [mac <macaddr> | vlan <vlan_name 32> | vlanid <vlanid 1-4094>]

**show mac_based_access_control auth_state ports** {<portlist>}

**show mac_based_access_control** {ports {<portlist>}}

**show mac_based_access_control_local** {[mac <macaddr> | vlan <vlan_name 32> | vlanid <vlanid 1-4094>]}

**config mac_based_access_control log state** [enable | disable]

**config mac_based_access_control trap state** [enable | disable]

**config mac_based_access_control password_type** [manual_string | client_mac_address]

## 57-1 enable mac_based_access_control

### Description

This command is used to enable the MAC-based access control function.

### Format

**enable mac_based_access_control**

### Parameters

None.

### Restrictions

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

### Example

To enable MAC-based access control:

```
DGS-3620-28SC:admin#enable mac_based_access_control
Command: enable mac_based_access_control

Success.

DGS-3620-28SC:admin#
```

## 57-2 disable mac_based_access_control

### Description

This command is used to disable the MAC-based access control function.

### Format

**disable mac_based_access_control**

### Parameters

None.

### Restrictions

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

### Example

To disable MAC-based access control:

```
DGS-3620-28SC:admin#disable mac_based_access_control
Command: disable mac_based_access_control

Success.

DGS-3620-28SC:admin#
```

## 57-3 config mac_based_access_control password

### Description

This command is used to set the password that will be used for authentication via RADIUS server.

### Format

**config mac_based_access_control password <passwd 16>**

### Parameters

**<passwd 16>** - In RADIUS mode, the switch communicates with the RADIUS server using this password. The maximum length of the key is 16 characters.

### Restrictions

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

### Example

To configure the password “rosebud” that will be used for authentication via RADIUS server:

```
DGS-3620-28SC:admin#config mac_based_access_control password rosebud
Command: config mac_based_access_control password rosebud

Success.

DGS-3620-28SC:admin#
```

## 57-4 config mac_based_access_control method

### Description

This command is used to authenticate via a local database or a RADIUS server.

### Format

**config mac_based_access_control method [local | radius]**

### Parameters

**local** - Specify to authenticate via local database.

**radius** - Specify to authenticate via RADIUS server.

### Restrictions

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

### Example

To configure the MAC-based access control method as local:

```
DGS-3620-28SC:admin#config mac_based_access_control method local
Command: config mac_based_access_control method local

Success.

DGS-3620-28SC:admin#
```

## 57-5 config mac_based_access_control guest_vlan ports

### Description

This command is used to put the specified port in guest VLAN mode. For those ports not contained in the port list, they are in non-guest VLAN mode.For detailed information about the operation of guest VLAN mode, please see the description for configuring the MAC-based access control port command.

### Format

**config mac_based_access_control guest_vlan ports <portlist>**

### Parameters

**<portlist>** - When a port is configured as gurest VLAN member port, this port will move to guest VLAN if it's MAC-based access control state is enable.

### Restrictions

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

### Example

To configure the MAC-based access control guest VLAN membership for port 1 to 8:

```
DGS-3620-28SC:admin# config mac_based_access_control guest_vlan ports 1-8
Command: config mac_based_access_control guest_vlan ports 1-8

Success.

DGS-3620-28SC:admin#
```

## 57-6 config mac_based_access_control ports

### Description

This command is used to configure the MAC-based access control 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.

### Format

**config mac_based_access_control ports [<portlist> | all] {state [enable | disable] | aging_time [infinite | <min 1-1440>] | block_time <sec 0-300> | max_users [<value 1-4000> | no_limit]}(1)**

### Parameters

**<portlist>** - Specify a range of ports to configure the MAC-based access control settings
**all** - Specify to select all the ports.

**state** - Specify whether the MAC-based access control function is enabled or disabled.
- **enable** - Specify to enable the MAC-based access control function.
- **disable** - Specify to disable the MAC-based access control function.

**aging_time** - Specify a time period during which an authenticated host will be kept in the authenticated state. When the aging time is timed-out, the host will be moved back to unauthenticated state.
- **infinite** - Specify an unlimited aging time.
- **<min 1-1440>** - Specify the age-out time, in minutes, between 1 and 1440.

**block_time** - Specify the blocking time, in seconds, between 0 and 300.
- **<second 0-300>** - Specify the blocking time. The blocking time value must be between 0 and 300 seconds.

**max_users** - Specify the number of maximum users. The default value is 128 users.
- **<value 1-4000>** - Specify the maximum number of users between 1 and 4000.
- **no_limit** - Specify an unlimited number of users.

### Restrictions

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

### Example

To configure the port state for ports 1 to 8:

```
DGS-3620-28SC:admin# config mac_based_access_control ports 1-8 state enable
Command: config mac_based_access_control ports 1-8 state enable

Success.

DGS-3620-28SC:admin#
```

## 57-7 create mac_based_access_control

### Description

This command is used to create 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 the name of the guest VLAN.<br>**<vlan_name 32>** - Specify the name of the guest VLAN. The guest VLAN name can be up to 32 characters long. |
| **guest_vlanid** - Specify the VLAN ID of the guest VLAN.<br>**<vlanid 1-4094>** - Specify the VLAN ID of the guest VLAN. The guest VLAN ID must be between 1 and 4094. |

### Restrictions

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

### Example

To create a MAC-based access control guest VLAN:

```
DGS-3620-28SC:admin#create mac_based_access_control guest_vlan default
Command: create mac_based_access_control guest_vlan default

Success.

DGS-3620-28SC:admin#
```

## 57-8 delete mac_based_access_control

### Description

This command is used to delete MAC-based access control guest VLANs.

### Format

**delete mac_based_access_control [guest_vlan <vlan_name 32> | guest_vlanid < vlanid 1-4094>]**

### Parameters

| |
|---|
| **guest_vlan** - Specify the name of the guest VLAN.<br>**<vlan_name 32>** - Specify the name of the guest VLAN. The guest VLAN name can be up to 32 characters long. |
| **guest_vlanid** - Specify the VLAN ID of the guest VLAN.<br>**<vlanid 1-4094>** - Specify the VLAN ID of the guest VLAN. The guest VLAN ID must be between 1 and 4094. |

### Restrictions

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

### Example

To delete a MAC-based access control guest VLAN:

```
DGS-3620-28SC:admin#delete mac_based_access_control guest_vlan default
Command: delete mac_based_access_control guest_vlan default
```

```
Success.

DGS-3620-28SC:admin#
```

## 57-9 clear mac_based_access_control auth_state

### Description

This command is used to clear the authentication state of a user (or port). The port (or the user) will return to 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 clear the authentication state.<br>**all** - Specify all ports.<br>**<portlist>** - Specify a range of ports. |
| **mac_addr** - Specify to clear a specified host authentication state.<br>**<macaddr>** - Enter the MAC address here. |

### Restrictions

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

### Example

To clear the authentication state of all ports:

```
DGS-3620-28SC:admin#clear mac_based_access_control auth_state ports all
Command: clear mac_based_access_control auth_state ports all

Success.

DGS-3620-28SC:admin#
```

## 57-10 create mac_based_access_control_local mac

### Description

This command is used to create a database entry.

### Format

**create mac_based_access_control_local mac <macaddr> {[vlan <vlan_name 32> | vlanid <vlanid 1-4094>]}**

### Parameters

**<macaddr>** - Specify the MAC address that access accepts by local mode.

**vlan** - (Optional) If the MAC address is authorized, the port will be assigned to this VLAN.
**<vlan_name 32>** - Specify a VLAN name up to 32 characters long.

**vlanid** - (Optional) If the MAC address is authorized, the port will be assigned to this VLAN ID.
**<vlanid 1-4094>** - Specify a VLAN ID between 1 and 4094.

### Restrictions

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

### Example

To create a local database entry:

```
DGS-3620-28SC: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-3620-28SC:admin#
```

## 57-11 config mac_based_access_control_local mac

### Description

This command is used to modify a database entry.

### Format

**config mac_based_access_control_local mac <macaddr> [vlan <vlan_name 32> | vlanid <vlanid 1-4094> | clear_vlan]**

### Parameters

**<macaddr>** - Specify the MAC address that access is accepted by local mode.

**vlan** - If the MAC address is authorized, the port will be assigned to this VLAN.
**<vlan_name 32>** - Specify a VLAN name up to 32 characters long.

**vlanid** - If the MAC address is authorized, the port will be assigned to this VLAN ID.
**<vlanid 1-4094>** - Specify a VLAN ID between 1 and 4094.

**clear_vlan** - Specify to clear the specified VLAN.

### Restrictions

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

### Example

To configure a local database entry:

```
DGS-3620-28SC: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-3620-28SC:admin#
```

## 57-12 config mac_based_access_control max_users

### Description

This command is used to configure the MAC-based access control maximum number of authorized users.

### Format

**config mac_based_access_control max_users [<value 1-4000> | no_limit]**

### Parameters

| | |
|---|---|
| **<value 1-4000>** - Specify the maximum number of authorized users. | |
| **no_limit** - Specify an unlimited number of authorized users. | |

### Restrictions

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

### Example

To configure the MAC-based access control maximum number of authorized users:

```
DGS-3620-28SC:admin#config mac_based_access_control max_users 2
Command: config mac_based_access_control max_users 2

Success.

DGS-3620-28SC:admin#
```

## 57-13 config mac_based_access_control authorization attributes

### Description

This command is used to enable or disable the acceptance of an authorized configuration. When authorization is enabled for MAC-based access controls with RADIUS authentication, the authorized attributes (for example VLAN, 802.1p default priority, and ACL) assigned by the 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** - Specify to enable or disable the authorized attributes assigned by the RADIUS server that will be accepted.
- **enable** - If specified to enable, the authorized attributes (for example VLAN, 802.1p default priority, and ACL) assigned by the RADIUS server will be accepted if the global authorization status is enabled. The default state is enabled.
- **disable** - If specified to disable, the authorized attributes (for example VLAN, 802.1p default priority, and ACL) assigned by the RADIUS server will not be accepted even if the global authorization status is enabled.

**local** - Specify to enable to disable the authorized attributes assigned by the local database.
- **enable** - 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.
- **disable** - If specified to disable, the authorized attributes assigned by the local database will not be accepted even if the global authorization status is enabled.

### Restrictions

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

### Example

To disable the configuration authorized from the local database:

```
DGS-3620-28SC:admin#config mac_based_access_control authorization attributes
local disable
Command: config mac_based_access_control authorization attributes local disable

Success.

DGS-3620-28SC:admin#
```

## 57-14 delete mac_based_access_control_local

### Description

This command is used to delete a database entry

### Format

**delete mac_based_access_control_local [mac <macaddr> | vlan <vlan_name 32> | vlanid <vlanid 1-4094>]**

### Parameters

**mac** - Delete database by this MAC address.
- **<macaddr>** - Enter the MAC address here.

**vlan** - Delete database by this VLAN name.
- **<vlan_name 32>** - Specify a VLAN name up to 32 characters long.

**vlanid** - Delete database by this VLAN ID.
- **<vlanid 1-4094>** - Specify a VLAN ID value must be between 1 and 4094.

### Restrictions

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

### Example

To delete a MAC-based access control local by MAC address:

```
DGS-3620-28SC: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-3620-28SC:admin#
```

To delete a MAC-based access control local by VLAN name:

```
DGS-3620-28SC:admin#delete mac_based_access_control_local vlan default
Command: delete mac_based_access_control_local vlan default

Success.

DGS-3620-28SC:admin#
```

## 57-15 show mac_based_access_control auth_state ports

### Description

This command is used to display MAC-based access control authentication MAC information.

### Format

**show mac_based_access_control auth_state ports {<portlist>}**

### Parameters

**<portlist>** - (Optional) Specify the ports to display.

### Restrictions

None.

### Example

To display MAC-based access control authentication MAC information:

```
DGS-3620-28SC:admin# show mac_based_access_control auth_state ports
Command: show mac_based_access_control auth_state ports

(P): Port-based    Prio: Priority

Port    MAC Address       Original  State        VID  Prio Aging Time/
                           RX VID                           Block Time
------ -------------------- ---- -------------- ---- ---- -----------
1      00-00-00-00-00-01    1    Authenticated  -    6    1439
1      00-00-12-00-03-00    1    Blocked        -    -    286
3      00-00-00-00-00-02(P) 1    Authenticated  -    6    1440

Total Authenticating Hosts  : 0
Total Authenticated Hosts   : 2
Total Blocked Hosts         : 1

DGS-3620-28SC:admin#
```

## 57-16 show mac_based_access_control

### Description

This command is used to display MAC-based access control information.

### Format

**show mac_based_access_control {ports {<portlist>}}**

### Parameters

**ports** - (Optional) Specify to display the MAC-based access control port state.
**<portlist>** - Specify a range of ports to be displayed.

### Restrictions

None.

### Example

To display MAC-based access control information:

```
DGS-3620-28SC:admin#show mac_based_access_control
Command: show mac_based_access_control

MAC-based Access Control
------------------------------------
State                  : Disabled
Method                 : Local
Password Type          : Manual String
Password               : default
Max User               : No Limit
```

```
Guest VLAN              :
Guest VLAN Member Ports:
RADIUS Authorization    : Enabled
Local Authorization     : Enabled
Trap State              : Enabled
Log State               : Enabled

DGS-3620-28SC:admin#
```

To display MAC-based access control information for ports 1 to 4:

```
DGS-3620-28SC:admin#show mac_based_access_control ports 1-4
Command: show mac_based_access_control ports 1-4


Port    State     Aging Time   Block Time  Max User
                    (min)        (sec)
-----  --------   ----------   ---------   --------
1      Disabled   1440         300         1024
2      Disabled   1440         300         1024
3      Disabled   1440         300         1024
4      Disabled   1440         300         1024

DGS-3620-28SC:admin#
```

## 57-17 show mac_based_access_control_local

### Description

This command is used to display MAC-based access control local data.

### Format

**show mac_based_access_control_local {[mac <macaddr> | vlan <vlan_name 32> | vlanid <vlanid 1-4094>]}**

### Parameters

**mac** - (Optional) Display MAC-based access control local databases by this MAC address.
**<macaddr>** - Enter the MAC address here.

**vlan** - (Optional) Specify the VLAN.
**<vlan_name 32>** - Specify the VLAN name up to 32 characters long.

**vlanid** - (Optional) Specify the VLAN ID.
**<vlanid 1-4094>** - Specify the VLAN ID value between 1 and 4094.

### Restrictions

None.

### Example

To display MAC-based access control local data:

```
DGS-3620-28SC:admin#show mac_based_access_control_local
Command: show mac_based_access_control_local

MAC Address             VID
-----------------       ------
00-00-00-00-00-01       1

Total Entries:1

DGS-3620-28SC:admin#
```

To display MAC-based access control local data by MAC address:

```
DGS-3620-28SC:admin#show mac_based_access_control_local mac 00-00-00-00-00-01
Command: show mac_based_access_control_local mac 00-00-00-00-00-01

MAC Address         VID
-----------------   ------
00-00-00-00-00-01   1

Total Entries:1

DGS-3620-28SC:admin#
```

To display MAC-based access control local data by VLAN:

```
DGS-3620-28SC: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

Total Entries: 1

DGS-3620-28SC:admin#
```

## 57-18 config mac_based_access_control log state

### Description

This command is used to enable or disable the generating of MAC-based Access Control logs.

### Format

**config mac_based_access_control log state [enable | disable]**

### Parameters

| |
|---|
| **state** - Specifies the log state for MAC-based Access Control.<br>**enable** - Specifies that the log for MAC-based Access Control will be enabled.<br>**disable** - Specifies that the log for MAC-based Access Control will be disabled. |

### Restrictions

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

### Example

To disable the log state for MAC-based Access Control:

```
DGS-3620-28SC:admin# config mac_based_access_control log state disable
Command: config mac_based_access_control log state disable

Success.

DGS-3620-28SC:admin#
```

## 57-19 config mac_based_access_control trap state

### Description

This command is used to enable or disable the sending of MAC-based Access Control traps.

### Format

**config mac_based_access_control trap state [enable | disable]**

### Parameters

**state** - Specifies the trap state for MAC-based Access Control.
**enable** - Specifies that the trap state for MAC-based Access Control will be enabled.
**disable** - Specifies that the trap state for MAC-based Access Control will be disabled.

### Restrictions

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

### Example

To enable the trap state for MAC-based Access Control:

```
DGS-3620-28SC:admin# config mac_based_access_control trap state enable
Command: config mac_based_access_control trap state enable

Success.

DGS-3620-28SC:admin#
```

## 57-20 config mac_based_access_control password_type

### Description

This command is used to configure the type of RADIUS authentication password for MAC-based Access Control.

## Format

**config mac_based_access_control password_type [manual_string | client_mac_address]**

## Parameters

**manual_string** - Specifies to use the same string as password for all clients do RADIUS authentication, the string can be configured by using the command “config mac_based_access_control password”.

**client_mac_address** - Specifies to use the client’s MAC address as the password for RADIUS authentication. The MAC address format can be configured by using the command “config authentication mac_format”.

## 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-3620-28SC:admin# config mac_based_access_control password_type
client_mac_address
Command: config mac_based_access_control password_type client_mac_address


Success.


DGS-3620-28SC:admin#
```

To configure the MAC-based Access Control using “manual_string” as authentication password:

```
DGS-3620-28SC:admin# config mac_based_access_control password_type
manual_string
Command: config mac_based_access_control password_type manual_string


Success.


DGS-3620-28SC:admin#
```

# Chapter 58 MD5 Configuration Command List

**config md5 key** <key_id 1-255> <password 16>

**create md5 key** <key_id 1-255> <password 16>

**delete md5 key** <key_id 1-255>

**show md5** {key <key_id 1-255>}

## 58-1 config md5 key

### Description

This command is used to configure an MD5 key and password. The MD5 configuration allows for the entry of a 16 character Message Digest - version 5 (MD5) key which can be used to authenticate every packet exchanged between OSPF routers. It is used as a security mechanism to limit the exchange of network topology information to the OSPF routing domain.

### Format

**config md5 key <key_id 1-255> <password 16>**

### Parameters

**key** - Specifies that the MD5 Key will be configured.

**<key_id 1-255>** - Enter the MD5 Key used here. This key must be between 1 and 255.

**<password 16>** - Enter an alphanumeric string of between 1 and 16, case-sensitive characters, used to generate the Message Digest which is in turn is used to authenticate OSPF packets within the OSPF routing domain.

### Restrictions

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

### Example

To configure an MD5 key and password:

```
DGS-3620-28SC:admin# config md5 key 1 dlink
Command: config md5 key 1 dlink

Success.

DGS-3620-28SC:admin#
```

## 58-2 create md5 key

### Description

This command is used to create an MD5 key table.

### Format

**create md5 key <key_id 1-255> <password 16>**

### Parameters

**key** - Specifies that the MD5 Key will be created.
**<key_id 1-255>** - Enter the MD5 Key used here. This key must be between 1 and 255.
**<password 16>** - Enter an alphanumeric string of between 1 and 16, case-sensitive characters, used to generate the Message Digest which is in turn is used to authenticate OSPF packets within the OSPF routing domain.

### Restrictions

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

### Example

To create an MD5 key table:

```
DGS-3620-28SC:admin# create md5 key 1 dlink
Command: create md5 key 1 dlink

Success.

DGS-3620-28SC:admin#
```

## 58-3 delete md5 key

### Description

This command is used to delete an MD5 key table.

### Format

**delete md5 key <key_id 1-255>**

### Parameters

**key** - Specifies that the MD5 Key will be removed.
**<key_id 1-255>** - Enter the MD5 Key used here. This key must be between 1 and 255.

### Restrictions

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

### Example

To delete an MD5 key table:

```
DGS-3620-28SC:admin# delete md5 key 1
Command: delete md5 key 1

Success.

DGS-3620-28SC:admin#
```

## 58-4 show md5

### Description

This command is used to display the MD5 key table.

### Format

**show md5 {key <key_id 1-255>}**

### Parameters

| |
|---|
| **key** - (Optional) Specifies that the MD5 Key will be displayed.<br>**<key_id 1-255>** - Enter the MD5 Key used here. This key must be between 1 and 255. |
| If no parameter is specified, the system will display the MD5 key table. |

### Restrictions

None.

### Example

To display the MD5 key table:

```
DGS-3620-28SC:admin#show md5
Command: show md5

MD5 Key Table Configurations

Key-ID  Key
------  ----------
1       dlink

Total Entries: 1

DGS-3620-28SC:admin#
```

# Chapter 59 Mirror Commands

**create mirror group_id** <value 1-4>

**config mirror port** <port> {[add | delete] source ports <portlist> [rx | tx | both]}

**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>

**enable mirror**

**disable mirror**

**show mirror** {group_id <value 1-4>}

## 59-1 create mirror group_id

### Description

This command used to create a mirror group. If the mirror group has existed, do nothing and return success.

### Format

**create mirror group_id <value 1-4>**

### Parameters

**<value 1-4>** - Enter the mirror group ID used here. This value must be between 1 and 4.

### Restrictions

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

### Example

Create mirror group 3:

```
DGS-3620-28SC:admin# create mirror group_id 3
Command: create mirror group_id 3

Success.

DGS-3620-28SC:admin#
```

## 59-2 config mirror port

### Description

This command is used to allow a range of ports to have all of their traffic also sent to a designated port − where a network sniffer or other device can monitor the network traffic. In addition, you can specify that only traffic received by, sent by or both is mirrored to the target port.

### Format

**config mirror port <port> {[add |delete] source ports <portlist> [rx | tx | both]}**

### Parameters

**<port>** - Specify the port that will receive the packets duplicated at the mirror port.

**add** - (Optional) Specify the mirror entry to be added.

**delete** - (Optional) Specify the mirror entry to be deleted.

**source ports** - (Optional) Specify the ports that will be mirrored. All packets entering and leaving the source port can be duplicated in the mirror port.
**<portlist>** - Specify a range of ports to be configured.

**rx** - (Optional) Allow the mirroring of only packets received (flowing into) the port or ports in the port list.

**tx** - (Optional) Allow the mirroring of only packets sent (flowing out of) the port or ports in the port list.

**both** - (Optional) Mirror all the packets received or sent by the port or ports in the port list.

### Restrictions

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

### Example

To add mirroring target port 6 and the source ports 1 to 5 rx and tx packets:

```
DGS-3620-28SC:admin#config mirror port 6 add source ports 1-5 both
Command: config mirror port 6 add source ports 1-5 both

Success.

DGS-3620-28SC:admin#
```

## 59-3 config mirror group_id

### Description

This command 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]}**

### Parameters

**<value 1-4>** - Enter the mirror group ID used here. This value must be between 1 and 4.

**target_port** - (Optional) Specifies the port that will receive the packets duplicated at the mirror port.
**<port>** - Enter the target port number used here.

**add** - (Optional) Specifies the mirror source ports to be add.

**delete** - (Optional) Specifies the mirror source ports to be delete

**source** - (Optional) Specifies the source ports used.

**ports** - (Optional) Specifies the list of ports used as source ports.
**<portlist>** - Enter the list of ports to be used as the source ports here.

**rx** - (Optional) Specifies that only the received packets on the mirror group source ports will be mirrored to the mirror group target port.
**tx** - (Optional) Specifies that only the sent packets on the mirror group source ports will be mirrored to the mirror group target port.
**both** - (Optional) Specifies that both the received and sent packets on the mirror group source ports will be mirrored to the mirror group target port.

**state** - (Optional) Specifies the mirror group state to enable or disable the mirror group function.
**enable** - Specifies that the mirror group state will be enabled.
**disable** - Specifies that the mirror group state will be disabled.

### Restrictions

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

### Example

Configure mirror group 2 with state enable and add source ports 1:4-1:9:

```
DGS-3620-28SC:admin# config mirror group_id 2 state enable add source ports
1:4-1:9 both
Command: config mirror group_id 2 state enable add source ports 1:4-1:9 both

Success.

DGS-3620-28SC:admin#
```

## 59-4 delete mirror group_id

### Description

This command is used to delete a mirror group on the Switch.

### Format

**delete mirror group_id <value 1-4>**

### Parameters

**<value 1-4>** - Enter the mirror group ID used here. This value must be between 1 and 4.

### Restrictions

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

### Example

To delete mirror group 3:

```
DGS-3620-28SC:admin# delete mirror group_id 3
Command: delete mirror group_id 3

Success.

DGS-3620-28SC:admin#
```

## 59-5 enable mirror

### Description

This command, combined with the disable mirror command below, allows you to enable or disable mirror function without having to modify the mirror session configuration.

**Note:** If the target port hasn’t been set, enable mirror will not take effect.

### Format

**enable mirror**

### Parameters

None.

### Restrictions

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

### Example

To enable mirroring configurations:

```
DGS-3620-28SC:admin#enable mirror
Command: enable mirror

Success.

DGS-3620-28SC:admin#
```

## 59-6 disable mirror

### Description

This command, combined with the enable mirror command above, allows you to enable or disable mirror function without having to modify the mirror session configuration.

### Format

**disable mirror**

### Parameters

None.

### Restrictions

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

### Example

To disable mirroring configurations:

```
DGS-3620-28SC:admin#disable mirror
Command: disable mirror

Success.

DGS-3620-28SC:admin#
```

## 59-7 show mirror

### Description

This command is used to display the current port mirroring configuration on the switch.

### Format

**show mirror {group_id <value 1-4>}**

### Parameters

**group_id** – (Optional) Specifies the group ID used for this display.

**<value 1-4>** - Enter the group ID used for this display here. This value must be between 1 and 4.

### Restrictions

None.

### Example

To display mirroring configuration:

```
DGS-3620-28SC:admin#show mirror
Command: show mirror

 Mirror Global State:   Disabled

 Group   State      Target Port   Source Ports
 ------- ---------- ------------- ----------------------------------------------
-
 1       Enabled    1             RX: 2-3
                                  TX: 2-3

DGS-3620-28SC:admin#
```

# Chapter 60 MLD Proxy Commands

**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}

## 60-1 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-3620-28SC:admin#enable mld_proxy
Command: enable mld_proxy

Success.

DGS-3620-28SC:admin#
```

## 60-2 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-3620-28SC:admin#disable mld_proxy
Command: disable mld_proxy

Success.

DGS-3620-28SC:admin#
```

## 60-3 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 Administrator, Operator and Power-User level users can issue this command.

### Example

To configure the MLD Proxy's downstream interface:

```
DGS-3620-28SC:admin#config mld_proxy downstream_if add vlan vlanid 2-7
Command: config mld_proxy downstream_if add vlan vlanid 2-7
```

```
Success.

DGS-3620-28SC:admin#
```

## 60-4 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 Administrator, Operator and Power-User level users can issue this command.

### Example

To configure the router port of MLD proxy’s upstream interface:

```
DGS-3620-28SC:admin#config mld_proxy upstream_if vlan default router_ports add
3
Command: config mld_proxy upstream_if vlan default router_ports add 3

Success.

DGS-3620-28SC:admin#
```

## 60-5 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. | |

**Note:** If the **group** is not specified, the MLD proxy configuration will be displayed.

### Restrictions

None.

### Example

To display the MLD proxy's information:

```
DGS-3620-28SC:admin#show mld_proxy
Command: show mld_proxy

MLD Proxy Global State          : Enabled

Upstream Interface
 VLAN ID                         : 1
 Dynamic Router Ports            : 1-4
 Static Router Ports             : 5-6
 Unsolicited Report Interval     : 10
 Source IP Address               : ::

Downstream Interface
 VLAN List                       : 2-4

DGS-3620-28SC:admin#
```

To display the MLD proxy's group information:

```
DGS-3620-28SC: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-3620-28SC:admin#
```

# Chapter 61 MLD Snooping Commands

**config mld_snooping** [vlan_name <vlan_name 32> | vlanid <vlanid_list> | all] {state [enable | disable] | fast_done [enable | disable] | proxy_reporting {state [enable | disable]| source_ip <ipv6addr>}(1)}(1)

**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>]

**create 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>

**delete mld_snooping static_group** [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipv6addr>

**show mld_snooping static_group** {[vlan <vlan_name 32> | vlanid <vlanid_list>] <ipv6addr>}

**show mld_snooping statistic counter** [vlan <vlan_name 32> | vlanid <vlanid_list> | ports <portlist>]

**clear mld_snooping statistics counter**

**config mld_snooping querier** [vlan_name <vlan_name 32> | vlanid <vlanid_list> | all] {query_interval <sec 1-65535> | max_response_time <sec 1-25> | robustness_variable <value 1-7> | last_listener_query_interval <sec 1-25> | state [enable | disable] | version <value 1-2>}(1)

**config mld_snooping mrouter_ports** [vlan <vlan_name 32> | vlanid <vlanid_list>] [add | delete] <portlist>

**config mld_snooping mrouter_ports_forbidden** [vlan <vlan_name 32> | vlanid <vlanid_list>] [add | delete] <portlist>

**enable mld_snooping**

**disable mld_snooping**

**show mld_snooping** {[vlan <vlan_name 32> | vlanid <vlanid_list >]}

**show mld_snooping group** {[vlan <vlan_name 32> | vlanid <vlanid_list> | ports <portlist>] {<ipv6addr>}}

**show mld_snooping mrouter_ports** [vlan <vlan_name 32> | vlanid <vlanid_list> | all] {[static | dynamic | forbidden]}

**show mld_snooping forwarding** {[vlan <vlan_name 32> | vlanid <vlanid_list>]}

## 61-1 config mld_snooping

### Description

This command is used to configure MLD snooping on the switch.

### Format

**config mld_snooping [vlan_name <vlan_name 32> | vlanid <vlanid_list> | all] {state [enable | disable] | fast_done [enable | disable] | 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>** - Specify the VLAN name. The maximum length is 32 characters.

**vlanid** - Specify the VLAN ID list.

- **<vlanid_list>** - Specify the VLAN ID list.

**all** - Specify to configure all VLANs.

**state** - Enable or disable MLD snooping for the chosen VLAN.
- **enable** - Enable MLD snooping for the chosen VLAN.
- **disable** - Disable MLD snooping for the chosen VLAN.

**fast_done** - Enable or disable the MLD snooping fast leave function. If enabled, the membership is immediately removed when the system receive the MLD leave message.
- **enable** - Enable the MLD snooping fast leave function.
- **disable** - Disable the MLD snooping fast leave function.

**proxy_reporting** - Specifies that the proxy reporting function will be configured.
- **state** - Specifies the state of the proxy reporting function.
  - **enable** - Specifies that the proxy reporting function will be enabled.
  - **disable** - Specifies that the proxy reporting function will be disabled.

**source_ip** - Specifies the source IPv6 address used.
- **<ipv6addr>** - Enter the source IPv6 address used here.

### Restrictions

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

### Example

To configure MLD snooping:

```
DGS-3620-28SC:admin#config mld_snooping vlan_name default state enable
Command: config mld_snooping vlan_name default state enable

Success.

DGS-3620-28SC:admin#
```

## 61-2 config mld_snooping rate_limit

### Description

This command is used to configure the upper limit per second for ingress MLD control packets.

### 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>** - Specify a range of ports to be configured.

**vlanid** - Specify a range of VLANs to be configured.
- **<vlanid_list>** - Specify the VLAN ID list.

**<value 1-1000>** - Specify the rate limit of MLD control packet that the switch can process on a specific port/VLAN. The rate is specified in packet per second. The packet that exceeds the limited rate will be dropped.

**no_limit** - The default setting is no limit.

### Restrictions

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

### Example

To configure the MLD snooping packet rate limit on port 1 for 100:

```
DGS-3620-28SC:admin#config mld_snooping rate_limit ports 1 100
Command: config mld_snooping rate_limit ports 1 100

Success.

DGS-3620-28SC:admin#
```

## 61-3 show mld_snooping rate_limit

### Description

This command is used to display the MLD snooping rate limit setting.

### Format

**show mld_snooping rate_limit [ports <portlist> | vlanid <vlanid_list>]**

### Parameters

**ports** - Specify a range of ports to be displayed.
**<portlist>** - Specify a range of ports to be displayed.

**vlanid** - Specify a range of VLANs to be displayed.
**<vlanid_list>** - Specify the VLAN ID list.

### Restrictions

None.

### Example

To display the MLD snooping packet rate limit for ports 1 to 2:

```
DGS-3620-28SC:admin#show mld_snooping rate_limit ports 1-2
Command: show mld_snooping rate_limit ports 1-2

 Port      Rate Limit
--------  ------------
1              No Limit
2              No Limit

Total Entries: 2
DGS-3620-28SC:admin#
```

## 61-4 create mld_snooping static_group

### Description

This command is used to create an MLD snooping multicast 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 MLD snooping is enabled on the VLAN. 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. For a layer 3 device, the device is also responsible to route the packet destined for this specific group to static member ports. The static member port will only affect V2 MLD operation. 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.<br>**<vlan_name 32>** - Specify the VLAN name. The maximum length is 32 characters. |
| **vlanid** - Specify the VLAN ID list.<br>**<vlanid_list>** - Specify the VLAN ID list. |
| **<ipv6addr>** - Specify the multicast group IPv6 address. |

### Restrictions

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

### Example

To create an MLD snooping static group on vlan1, group FF1E::1:

```
DGS-3620-28SC:admin#create mld_snooping static_group vlan vlan1 FF1E::1
Command: create mld_snooping static_group vlan vlan1 FF1E::1

Success.

DGS-3620-28SC:admin#
```

## 61-5 config mld_snooping static_group

### Description

This command is used to configure an MLD snooping static group on the switch. When a port is configured as a static member port, the MLD protocol will not operate on this port. Therefore, 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. The static member port will only affect V1 MLD operation.

### 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>** - Specify the VLAN name. The maximum length is 32 characters.

**vlanid** - Specify the ID of the VLAN on which the static group resides.
**<vlanid_list>** - Specify the VLAN ID list.

**<ipv6addr>** - Specify the multicast group IPv6 address.

**add** - Specify to add the member ports.

**delete** - Specify to delete the member ports.

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

### Restrictions

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

### Example

To unset ports 9 to 10 from MLD Snooping static member ports for group FF1E::1 on default VLAN:

```
DGS-3620-28SC: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-3620-28SC:admin#
```

## 61-6 delete mld_snooping static_group

### Description

This command is used to delete an MLD snooping static group on the switch. The deletion of an MLD snooping static group will not affect the MLD snooping dynamic member ports for a 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>** - Specify the VLAN name. The maximum length is 32 characters.

**vlanid** - Specify the ID of the VLAN on which the static group resides.
**<vlanid_list>** - Specify the VLAN ID list.

**<ipv6addr>** - Specify the multicast group IPv6 address.

### Restrictions

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

### Example

To delete an MLD snooping static group from the default VLAN, group FF1E::1:

```
DGS-3620-28SC:admin#delete mld_snooping static_group vlan default FF1E::1
Command: delete mld_snooping static_group vlan default FF1E::1

Success.

DGS-3620-28SC:admin#
```

## 61-7 show mld_snooping static_group

### Description

This command is used to display the MLD snooping static groups.

### 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.<br>**<vlan_name 32>** - Specify the VLAN name. The maximum length is 32 characters. |
| **vlanid** - (Optional) Specify the ID of the VLAN on which the static group resides.<br>**<vlanid_list>** - Specify the VLAN ID list. |
| **<ipv6addr>** - (Optional) Specify the multicast group IPv6 address. |
| If no parameter is specified, the system will display all MLD snooping static groups. |

If no parameter is specified, the system will display all MLD snooping static groups.

### Restrictions

None.

### Example

To display all the MLD snooping static groups:

```
DGS-3620-28SC: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-3620-28SC:admin#
```

## 61-8 show mld_snooping statistic counter

### Description

This command is used to display the MLD snooping statistics counters for MLD protocol packets that are transmitted or received by the switch since MLD snooping was enabled.

### Format

**show mld_snooping statistic counter [vlan <vlan_name 32> | vlanid <vlanid_list> | ports <portlist>]**

### Parameters

| |
|---|
| **vlan** - Specify a VLAN to be displayed.<br>**<vlan_name 32>** - Specify the VLAN name. The maximum length is 32 characters. |
| **vlanid** - Specify a list of VLANs to be displayed.<br>**<vlanid_list>** - Specify the VLAN ID list. |
| **ports** – Specify a list of ports to be displayed.<br>**<portlist>** - Specify a list of ports. |

### Restrictions

None.

### Example

To display the MLD snooping statistics counters on port 1:

```
DGS-3620-28SC:admin#show mld_snooping statistic counter ports 1
Command: show mld_snooping statistic counter ports 1

Port #           : 1
--------------------------------------------------
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-3620-28SC:admin#
```

## 61-9 clear mld_snooping statistics counter

### Description

This command is used to clear the MLD snooping statistics counters.

### Format

**clear mld_snooping statistics counter**

### Parameters

None.

### Restrictions

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

### Example

To clear the MLD snooping statistics counters:

```
DGS-3620-28SC:admin#clear mld_snooping statistics counter
Command: clear mld_snooping statistics counter

Success.

DGS-3620-28SC:admin#
```

## 61-10 config mld_snooping querier

### Description

This command is used to configure the time, in seconds, between general query transmissions, the maximum time to wait for reports from listeners, and the permitted packet loss that guarantees MLD snooping.

### Format

**config mld_snooping querier [vlan_name <vlan_name 32> | vlanid <vlanid_list> | all] {query_interval <sec 1-65535> | max_response_time <sec 1-25> | robustness_variable <value 1-7> | last_listener_query_interval <sec 1-25> | state [enable | disable] | version <value 1-2>} (1)**

### Parameters

**vlan_name** - Specify the name of the VLAN for which MLD snooping querier is to be configured.

**<vlan_name 32>** - Specify the VLAN name. The maximum length is 32 characters.

**vlanid** - Specify the ID of the VLAN for which MLD snooping querier is to be configured.

**<vlanid_list>** - Specify the VLAN ID list.

**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.

**<sec 1-65535>** - Specify the amount of time in seconds between general query transmissions. The default setting is 125 seconds.

**max_response_time** - Specify the maximum time in seconds to wait for reports from members.

**<sec 1-25>** - Specify the maximum time in seconds to wait for reports from members. The default setting is 10 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:

1. 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).
2. 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).

3. 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.

**<value 1-7>** - Specify the value between 1 and 7. Increase the value if you expect a subnet to be lossy. The robustness variable is set to 2 by default.

**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.

**<sec 1-25>** - Specify the time between 1 and 25 seconds.

**state** - 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** - Allows the switch to be selected as an MLD Querier (sends MLD query packets).

**disable** - When disabled, the switch can not play the role as a querier.

**version** - Specify the version of MLD packet that will be sent by this port. If a MLD packet received by the interface has a version higher than the specified version, this packet will be forward from router ports or VLAN flooding.

**<value 1-2>** - Specify the values between 1 and 2.

### Restrictions

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

### Example

To configure the MLD snooping querier:

```
DGS-3620-28SC: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-3620-28SC:admin#
```

## 61-11 config mld_snooping mrouter_ports

### Description

This command allows users 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>** - Specify the name of the VLAN on which the router port resides. The maximum length is 32 characters. |
| **vlanid** - Specify the ID of the VLAN on which the router port resides.<br>**<vlanid_list>** - Specify a list of VLAN IDs. |
| **add** - Specify to add router ports. |
| **delete** - Specify to delete router ports. |
| **<portlist>** - Specify a range of ports to be configured. |

### Restrictions

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

### Example

To set up static router ports:

```
DGS-3620-28SC:admin#config mld_snooping mrouter_ports vlan default add 1-10
Command: config mld_snooping mrouter_ports vlan default add 1-10

Success.

DGS-3620-28SC:admin#
```

## 61-12 config mld_snooping mrouter_ports_forbidden

### Description

This command allows you 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 router port resides.<br>**<vlan_name 32>** - Specify the name of the VLAN on which the router port resides. The maximum length is 32 characters. |
| **vlanid** - Specify the ID of the VLAN on which the router port resides.<br>**<vlanid_list>** - Specify a list of VLAN IDs. |
| **add** - Specify to add router ports. |
| **delete** - Specify to delete router ports. |
| **<portlist>** - Specify a range of ports to be configured. |

### Restrictions

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

### Example

To set up ports as forbidden router port:

```
DGS-3620-28SC:admin#config mld_snooping mrouter_ports_forbidden vlan default
add 1-10
Command: config mld_snooping mrouter_ports_forbidden vlan default add 1-10

Success.

DGS-3620-28SC:admin#
```

## 61-13 enable mld_snooping

### Description

This command is used to enable MLD snooping on the switch.

### Format

**enable mld_snooping**

### Parameters

None.

### Restrictions

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

### Example

To enable MLD snooping on the switch:

```
DGS-3620-28SC:admin#enable mld_snooping
Command: enable mld_snooping

Success.

DGS-3620-28SC:admin#
```

## 61-14 disable mld_snooping

### Description

This command is used to disable MLD snooping on the switch. MLD snooping can be disabled only if IPv6 multicast routing is not being used. Disabling MLD snooping allows all MLD and IPv6 multicast traffic to flood within a given IPv6 interface.

### Format

**disable mld_snooping**

### Parameters

None.

### Restrictions

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

### Example

To disable MLD snooping on the switch:

```
DGS-3620-28SC:admin#disable mld_snooping
Command: disable mld_snooping

Success.

DGS-3620-28SC:admin#
```

## 61-15 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 to view the MLD snooping configuration.
**<vlan_name 32>** - Specify the name of the VLAN. The maximum length is 32 characters.

**vlanid** - (Optional) Specify the ID of the VLAN for which to view the MLD snooping configuration.
**<vlanid_list>** - Specify a list of VLAN IDs.

**Note:** If no parameter is specified, the system will display all current MLD snooping configurations.

### Restrictions

None.

### Example

To display MLD snooping:

```
DGS-3620-28SC:admin#show mld_snooping
Command: show mld_snooping

MLD Snooping Global State              : Disabled

 VLAN Name                        : default
 Query Interval                   : 125
 Max Response Time             : 10
 Robustness Value              : 2
 Last Listener Query Interval  : 1
 Querier State                 : Disabled
 Querier Role                  : Non-Querier
 Querier IP                    : ::
 Querier Expiry Time           : 0 secs
 State                         : Disabled
 Fast Done                     : Disabled
 Proxy Reporting               : Enabled
 Proxy Reporting Source IP     : ::
 Rate Limit                    : No Limitation
 Version                       : 2

Total Entries: 1

DGS-3620-28SC:admin#
```

## 61-16 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>}}**

### Parameters

**vlan** - (Optional) Specify the name of the VLAN for which 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>** - Specify the VLAN name. The maximum length is 32 characters.

**vlanid** - (Optional) Specify the ID of the VLAN for which to view MLD snooping group information.
**<vlanid_list>** - Specify the VLAN ID list.

**ports** - (Optional) Specify the list of port for which to view MLD snooping group information.
**<portlist>** - Specify a range of ports to be displayed.

**<ipv6addr>** - (Optional) Specify the group IPv6 address for which to view MLD snooping group information.

If no parameter is specified, the system will display all MLD snooping groups on the switch.

### Restrictions

None.

### Example

To display the MLD snooping group:

```
DGS-3620-28SC: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

Total Entries : 3

DGS-3620-28SC:admin#
```

## 61-17 show mld_snooping mrouter_ports

### Description

This command is used to display the 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>** - Specify the name of the VLAN on which the router port resides. The maximum length is 32 characters.

**vlanid** - Specify the ID of the VLAN on which the router port resides.
**<vlanid_list>** - Specify a list of VLAN IDs.

**all** - Specify all VLANs on which the router port resides.

**static** - (Optional) Display router ports that have been statically configured.

**dynamic** - (Optional) Display router ports that have been dynamically learned.

**forbidden** - (Optional) Display forbidden router ports that have been statically configured.

**Note:** If no parameter is specified, the system will display all router ports on the Switch.

### Restrictions

None.

### Example

To display router ports:

```
DGS-3620-28SC:admin#show mld_snooping mrouter_ports all
Command: show mld_snooping mrouter_ports all

VLAN Name               : default
Static Router Port      :
Dynamic Router Port     :
Router IP               :
Forbidden Router Port   :

Total Entries: 1

DGS-3620-28SC:admin#
```

## 61-18 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 comes from specific sources will be forwarded to. The packet comes from the source VLAN. They will be forwarded to the forwarding ports.

### Format

**show mld_snooping forwarding {[vlan <vlan_name 32> | vlanid <vlanid_list>]}**

### Parameters

**vlan** - (Optional) Specify the name of the VLAN for which to view MLD snooping forwarding table information.
**<vlan_name 32>** - Specify the VLAN name. The maximum length is 32 characters.

**vlanid** - (Optional) Specify the ID of the VLAN for which to view MLD snooping forwarding table information.
**<vlanid_list>** - Specify the VLAN ID list.

**Note:** If no parameter is specified, the system will display all currently configured MLD snooping forwarding entries.

### Restrictions

None.

### Example

To display all MLD snooping forwarding entries located on the switch:

```
DGS-3620-28SC:admin#show mld_snooping forwarding
Command: show mld_snooping forwarding

VLAN Name    : default
Source IP    : 2001::1
Multicast Group: FE1E::1
Port Member  : 2,7

VLAN Name    : default
Source IP    : 2001::1
Multicast Group: FE1E::2
Port Member  : 5

Total Entries: 2

DGS-3620-28SC:admin#
```

# Chapter 62 MLD Snooping Multicast (MSM) VLAN Commands

**create mld_snooping multicast_vlan** <vlan_name 32> <vlanid 2-4094> {remap_priority [<value 0-7> | none] {replace_priority}}

**config mld_snooping multicast_vlan** <vlan_name 32> {[add | delete] [member_port <portlist> | [source_port <portlist> | untag_source_port <portlist>] | tag_member_port <portlist>] | state [enable | disable] | replace_source_ipv6 <ipv6addr> | remap_priority [<value 0-7> | none] {replace_priority}} (1)

**create mld_snooping multicast_vlan_group_profile** <profile_name 1-32>

**config mld_snooping multicast_vlan_group_profile** <profile_name 1-32> [add | delete] <mcastv6_address_list>

**delete mld_snooping multicast_vlan_group_profile** [profile_name <profile_name 1-32> | all]

**show mld_snooping multicast_vlan_group_profile** {<profile_name 1-32>}

**config mld_snooping multicast_vlan_group** <vlan_name 32> [add | delete] profile_name <profile_name 1-32>

**show mld_snooping multicast_vlan_group** {<vlan_name 32>}

**delete mld_snooping multicast_vlan** <vlan_name 32>

**enable mld_snooping multicast_vlan**

**disable mld_snooping multicast_vlan**

**show mld_snooping multicast_vlan** {<vlan_name 32>}

**config mld_snooping multicast_vlan forward_unmatched** [disable | enable]

## 62-1 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 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>** - Specify 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>** - Specify 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>** - Specify 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 Administrator, Operator and Power-User level users can issue this command.

### Example

To create an MLD snooping multicast VLAN with the VLAN name mv1 and the VID 2:

```
DGS-3620-28SC:admin#create mld_snooping multicast_vlan mv1 2
Command: create mld_snooping multicast_vlan mv1 2

Success.

DGS-3620-28SC:admin#
```

## 62-2 config mld_snooping multicast_vlan

### Description

This command is used to configure MLD snooping multicast VLAN parameters. The member port list and source port list cannot overlap. However, the member port of one multicast VLAN can overlap with another multicast VLAN. The multicast VLAN must be created first using the **create mld_snooping multicast_vlan** command before the multicast VLAN can be configured.

### Format

**config mld_snooping multicast_vlan <vlan_name 32> {[add | delete] [member_port <portlist> | [source_port <portlist> | untag_source_port <portlist>] | tag_member_port <portlist>] | state [enable | disable] | replace_source_ipv6 <ipv6addr> | remap_priority [<value 0-7> | none] {replace_priority}} (1)**

### Parameters

**<vlan_name 32>** - Specify 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>** - Specify a range of ports to be configured.

**source_port** - Specify source port where the multicast traffic is entering the Switch.
**<portlist>** - Specify 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>** - Specify a range of ports to be configured.

**tag_member_port** - Specify the tagged member port of the multicast VLAN.

**<portlist>** - Specify 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 use :: ip address
**<ipv6addr>** - Enter the IP address here.

**remap_priority** - Specify the remap priority here.
**<value 0-7>** - The remap priority value (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 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 Administrator, Operator and Power-User level 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-3620-28SC: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-3620-28SC:admin#
```

## 62-3 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>** - Specify the multicast VLAN profile name. The maximum length is 32 characters.

### Restrictions

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

### Example

To create an MLD snooping multicast group profile with the name “Knicks”:

```
DGS-3620-28SC:admin#create mld_snooping multicast_vlan_group_profile Knicks
Command: create mld_snooping multicast_vlan_group_profile Knicks

Success.

DGS-3620-28SC:admin#
```

## 62-4 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>** - Specify 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>** - Specify 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 Administrator, Operator and Power-User level 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-3620-28SC: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-3620-28SC:admin#
```

## 62-5 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>** - Specify 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 Administrator, Operator and Power-User level users can issue this command.

### Example

To delete an MLD snooping multicast group profile named “Knicks”:

```
DGS-3620-28SC:admin#delete mld_snooping multicast_vlan_group_profile
profile_name Knicks
Command: delete mld_snooping multicast_vlan_group_profile profile_name Knicks

Success.

DGS-3620-28SC:admin#
```

## 62-6 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) Specify the multicast VLAN profile name. The maximum length is 32 characters.

If no parameter is specified, the system will display all multicast VLAN group profiles.

### Restrictions

None.

### Example

To display all MLD snooping multicast VLAN profiles:

```
DGS-3620-28SC: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-3620-28SC:admin#
```

## 62-7 config mld_snooping multicast_vlan_group

### Description

This command is used to configure the multicast group which will be learned with the specific multicast VLAN. There are two cases that need to be considered. For the first case, suppose that a multicast group is not configured and multicast VLANs do not have overlapped member ports. That means the join packets received by the member port will only be learned with the multicast VLAN that this port belongs to. If not, which is the second case, the join packet will be learned with the multicast VLAN that contains the destination multicast group. If the destination multicast group of the join packet can not be classified into any multicast VLAN that this port belongs to, then the join packet will be learned with the natural VLAN of the packet. Please note that the same profile can not overlap different multicast VLANs. Multiple profiles can be added to a multicast VLAN, however.

### Format

**config mld_snooping multicast_vlan_group <vlan_name 32> [add | delete] profile_name <profile_name 1-32>**

### Parameters

| |
|---|
| **<vlan_name 32>** - Specify the name of the multicast VLAN to be configured. Each multicast VLAN is given a name that can be up to 32 characters.<br>**add** - Specify to associate a profile to a multicast VLAN.<br>**delete** - Specify to de-associate a profile from a multicast VLAN. |
| **profile_name** - Specify the multicast VLAN profile name. The maximum length is 32 characters.<br>**<profile_name 1-32>** - Specify the multicast VLAN profile name. The profile name can be up to 32 characters long. |

### Restrictions

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

### Example

To add an MLD snooping profile to a multicast VLAN group with the name “v1”:

```
DGS-3620-28SC:admin#config mld_snooping multicast_vlan_group v1 add
profile_name channel_1
Command: config mld_snooping multicast_vlan_group v1 add profile_name channel_1
Success.

DGS-3620-28SC:admin#
```

## 62-8 show mld_snooping multicast_vlan_group

### Description

This command allows 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) Specify the name of the group profile’s multicast VLAN to be displayed.

If no parameter is specified, the system will display all multicast VLAN groups on the switch.

### Restrictions

None.

### Example

To display all MLD snooping multicast VLANs’ group profile information:

```
DGS-3620-28SC: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-3620-28SC:admin#
```

## 62-9 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>** - Specify the name of the multicast VLAN to be deleted.

### Restrictions

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

### Example

To delete an MLD snooping multicast VLAN called “v1”:

```
DGS-3620-28SC:admin#delete mld_snooping multicast_vlan v1
Command: delete mld_snooping multicast_vlan v1

Success.

DGS-3620-28SC:admin#
```

## 62-10 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 Administrator, Operator and Power-User level users can issue this command.

### Example

To enable MLD snooping multicast VLAN:

```
DGS-3620-28SC:admin#enable mld_snooping multicast_vlan
Command: enable mld_snooping multicast_vlan

Success.

DGS-3620-28SC:admin#
```

## 62-11 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 Administrator, Operator and Power-User level users can issue this command.

### Example

To disable MLD snooping multicast VLAN:

```
DGS-3620-28SC:admin#disable mld_snooping multicast_vlan
Command: disable mld_snooping multicast_vlan

Success.

DGS-3620-28SC:admin#
```

## 62-12 show mld_snooping multicast_vlan

### Description

This command allows information for a specific multicast VLAN to be displayed.

### Format

**show mld_snooping multicast_vlan {<vlan_name 32>}**

### Parameters

**<vlan_name 32>** - (Optional) Specify the name of the multicast VLAN to be displayed.

If no parameter is specified, the system will display all multicast VLANs on the switch.

### Restrictions

None.

### Example

To display all MLD snooping multicast VLANs:

```
DGS-3620-28SC:admin#show mld_snooping multicast_vlan
Command: show mld_snooping multicast_vlan

MLD Multicast VLAN Global State        : Disabled
MLD Multicast VLAN Forward Unmatched   : Disabled

VLAN Name                :test
VID                      :100

Member(Untagged) Ports    :1
Tagged Member Ports       :
Source Ports              :3
Untagged Source Ports     :
Status                    :Disabled
Replace Source IP         :::
Remap Priority            :None

Total Entries: 1

DGS-3620-28SC:admin#
```

## 62-13 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

| |
|---|
| **enable** - The packet will be flooded on the VLAN. |
| **disable** - The packet will be dropped. |

## Restrictions

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

## Example

To configure the forwarding mode for MLD snooping multicast VLAN unmatched packets:

```
DGS-3620-28SC:admin#config mld_snooping multicast_vlan forward_unmatched enable
Command: config mld_snooping multicast_vlan forward_unmatched enable

Success.

DGS-3620-28SC:admin#
```

# Chapter 63 Modify Login Banner and Prompt Commands

**config greeting_message** {default}
**show greeting_message**
**config command_prompt** [<string 16> **|** username | default]

## 63-1 config greeting_message

### Description

This command is used to modify the login banner.

### Format

**config greeting_message {default}**

### Parameters

**default** – (Optional) Adding this parameter to the config greeting_message command will return the greeting message (banner) to its original factory default entry.

### Restrictions

- When users issue the “reset” command, the modified banner will remain in tact. Yet, issuing the “reset system” will return the banner to its original default value.
- The maximum character capacity for the banner is 24 lines with 80 characters per line.
- In the following example, Ctrl+W will save the modified banner only to the DRAM. Users must enter the “save” command to save this entry to the Flash memory.
- Only Administrator and Operator-level users can issue this command.

### Example

To edit the banner:

```
DGS-3620-28SC:admin#config greeting_message
Command: config greeting_message

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


                      DGS-3620-28SC Gigabit Ethernet Switch
                             Command Line Interface

                            Firmware: Build 2.00.015
           Copyright(C) 2012 D-Link Corporation. All rights reserved.
```

```
===============================================================================

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

## 63-2 show greeting_message

### Description

This command is used to display the currently configured greeting message on the switch.

### Format

**show greeting_message**

### Parameters

None.

### Restrictions

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

### Example

To display the currently configured greeting message:

```
DGS-3620-28SC:admin#show greeting_message
Command: show greeting_message
===============================================================================

                      DGS-3620-28SC Gigabit Ethernet Switch
                             Command Line Interface

                            Firmware: Build 2.00.015
           Copyright(C) 2012 D-Link Corporation. All rights reserved.

















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

DGS-3620-28SC:admin#
```

## 63-3 config command_prompt

### Description

This command is used to modify the command prompt. The current command prompt consists of four parts: “product name” + “:” + ”user level” + ”#” (e.g. “**`DGS-3620-28SC:admin#`**″). This command is used to modify the first part (1. “product name”) with a string consisting of a maximum of 16 characters, or to be replaced with the users’ login user name.

### Format

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

### Parameters

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

## Restrictions

When users issue the “reset” command, the current command prompt will remain in tact. Issuing the “reset system” will return the command prompt to its original factory default value.

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

## Example

To edit the command prompt:

```
DGS-3620-28SC:admin#config command_prompt HQ0001
Command: config command_prompt HQ0001

Success.

HQ0001:admin#
```

# Chapter 64 Multicast Listener Discovery (MLD) Commands

| |
|---|
| **config mld** [ipif <ipif_name 12> \| all] {query_interval <sec 1-31744> \| max_response_time <sec 1-25> \| robustness_variable <value 2-7> \| last_listener_query_interval <sec 1-25> \| version <value 1-2> \| state [enable \| disable]} (1) |
| **show mld** {ipif <ipif_name 12>} |
| **show mld group** {ipif <ipif_name 12> \| group <ipv6addr>} |

## 64-1 config mld

### Description

This command is used to configure MLD on the Switch.

### Format

**config mld [ipif <ipif_name 12> | all] {query_interval <sec 1-31744> | max_response_time <sec 1-25> | robustness_variable <value 2-7> | last_listener_query_interval <sec 1-25> | version <value 1-2> | state [enable | disable]} (1)**

### Parameters

| |
|---|
| **ipif** - Specifies the IP interface name used for this configuration.<br>**<ipif_name 12>** - Enter the IP interface name used here. This name can be up to 12 characters long.<br>**all** - Specifies that all the IP interfaces will be used. |
| **query_interval** - (Optional) Specifies the time in seconds between the general query transmissions.<br>**<sec 1-31744>** - Enter the general query interval value used here. This value must be between 1 and 31744 seconds. The default value is 125 seconds. |
| **max_response_time** - (Optional) Specifies the maximum time in seconds to wait for reports from listeners.<br>**<sec 1-25>** - Enter the maximum response time value used here. The value must be between 1 and 25 seconds. The default value is 10 seconds. |
| **robustness_variable** - (Optional) Specifies the permitted packet loss that guarantees the MLD.<br>**<value 2-7>** - Enter the robustness variable value used here. This value must be between 2 and 7. The default value is 2. |
| **last_listener_query_interval** - (Optional) Specifies the maximum response time inserted into the Multicast address specific query sent in response to 'done group' messages. This is also the amount of time between Multicast address specific query messages.<br>**<sec 1-25>** - Enter the last listener query interval value used here. This value must be between 1 and 25 seconds. The default value is 1 second. |
| **version** - (Optional) Specifies the MLD version number.<br>**<value 1-2>** - Enter the MLD version number used here. This number must be between 1 and 2. The default value is 2. |
| **state** - (Optional) Specifies the MLD state for the specified route interface.<br>**enable** - Specifies that the MLD state for the specified interface will be enabled. |

**disable** - Specifies that the MLD state for the specified interface will be disabled.

### Restrictions

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

### Example

To configure the MLD on the IP interface “System”:

```
DGS-3620-28SC:admin# config mld ipif System version 1 state enabled
Command: config mld ipif System version 1 state enabled

Success.

DGS-3620-28SC:admin#
```

To configure the MLD version to v1 on all IP interfaces:

```
DGS-3620-28SC:admin# config mld all version 1
Command: config mld all version 1

Success.

DGS-3620-28SC:admin#
```

To configure the MLD last listener query interval to 10 seconds on all interfaces:

```
DGS-3620-28SC:admin# config mld all last_listener_query_interval 10
Command: config mld all last_listener_query_interval 10

Success.

DGS-3620-28SC:admin#
```

## 64-2 show mld

### Description

This command is used to display the MLD configurations on the Switch.

### Format

**show mld {ipif <ipif_name 12>}**

### Parameters

**ipif** – (Optional) Specifies the IP interface name used for this configuration.
**<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 MLD configurations.

### Restrictions

None.

### Example

To display the MLD configurations on all interfaces:

```
DGS-3620-28SC:admin# show mld
Command: show mld

MLD Interface Configurations

MRT = Maximum Response Time, LLQI = Last Listener Query Interval

Interface  Version Query  MRT  Robustness LLQI  State
---------- ------ ------ ---- ---------- -----  --------
System      2       125     10   2         1     Disabled
n10         2       125     10   2         1     Enabled
n11         2       125     10   2         1     Disabled
n12         2       125     10   2         1     Disabled

Total Entries: 4

DGS-3620-28SC:admin#
```

To display the MLD configurations for interface “n10”:

```
DGS-3620-28SC:admin# show mld ipif n10
Command: show mld ipif n10

MLD Interface Details

Interface                      : n10
IPv6 Link-Local Address        : FE80::123D:34AC/128
Querier                        : FE80::1E45:2310
Status                         : Enabled
Version                        : 2
Query Interval                 : 125 sec
Max Response Time              : 10 sec
Robustness                     : 2
Last Listener Query Interval   : 1 sec
Last Listener Query Count      : 2
Startup Query Count            : 2
Startup Query Interval         : 31 sec

DGS-3620-28SC:admin#
```

## 64-3 show mld group

### Description

This command is used to display the MLD group member table.

## Format

**show mld group {ipif <ipif_name 12> | group <ipv6addr>}**

## Parameters

| |
|---|
| **ipif** – (Optional) Specifies the IP interface name used for this configuration.<br>**<ipif_name 12>** - Enter the IP interface name used here. This name can be up to 12 characters long. |
| **group** - (Optional) Specifies the IPv6 multicast group address used.<br>**<ipv6addr>** - Enter the IPv6 multicast group address used here. |

If no parameter is specified, the system will display all MLD configurations.

## Restrictions

None.

## Example

To display all the MLD group member information on the switch, the "Expiry" uses second as the unit:

```
DGS-3620-28SC:admin# show mld group
Command: show mld group

Interface      Multicast Group      Expiry
------------  -----------------    -----
System          FF1E::100:0:0:20     260
n10             FF1E::1001:1234      255
n20             FF1E::2AC4:0:452     260
n10             FF1E::5A3D:11:23C1   260

Total Entries : 4

DGS-3620-28SC:admin#
```

To display all the MLD group member information of interface "n10", the "Expiry" uses second as the unit:

```
DGS-3620-28SC:admin# show mld group ipif n10
Command: show mld group ipif n10

Interface      Multicast Group       Expiry
------------  ------------------    -----
n10             FF1E::1001:1234      255
n10             FF1E::5A3D:11:23C1   260

Total Entries : 2

DGS-3620-28SC:admin#
```

To display the group source address list for interface “n10” with the group address “FF1E::100:0:20”, the “Expiry” uses second as the unit:

```
DGS-3620-28SC:admin# show mld group ipif n10 group FF1E::100:0:20
Command: show mld group ipif n10 group FF1E::100:0:20

MLD Group Details

Interface                 : n10
Multicast Group           : FF1E::100:0:20
Last Reporter             : FE80::2345:FE39
Up Time                   : 00:00:32
Expiry Time               : 00:30:02
Filter Mode               : Exclude
V1 Host Time              : 0 sec

Source List Table:

    Source Address             Expiry
    -----------------         -------
    2001::1234:EF23            10

    Total Source Entries: 1

Total Entries: 1

DGS-3620-28SC:admin#
```

To display all the MLD group member information for multicast group “FF1E::1001:1234”, the “Expiry” uses second as the unit:

```
DGS-3620-28SC:admin# show mld group group FF1E::1001:1234
Command: show mld group group FF1E::1001:1234

Interface      Multicast Group       Expiry
------------  ------------------    -----
n10             FF1E::1001:1234       215
n11             FF1E::1001:1234       200
n20             FF1E::1001:1234       240

Total Entries : 3

DGS-3620-28SC:admin#
```

# Chapter 65 Network Load Balancing (NLB) Commands

| |
|---|
| **create nlb multicast_fdb** [<vlan_name 32> \| vlanid <vlanid>] <macaddr> |
| **delete nlb multicast_fdb** [<vlan_name 32> \| vlanid <vlanid>] <macaddr> |
| **config nlb multicast_fdb** [<vlan_name 32> \| vlanid <vlanid>] <macaddr> [add \| delete] <portlist> |
| **show nlb fdb** |

## 65-1 create nlb multicast_fdb

### Description

This command is used to create the Switch's NLB multicast 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. 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 multicast_fdb [<vlan_name 32> | vlanid <vlanid>] <macaddr>**

### Parameters

| |
|---|
| **<vlan_name 32>** - Enter the VLAN name of the NLB multicast FDB entry here. This name can be up to 32 characters long.<br>**vlanid** - Specifies the VLAN ID used.<br>**<vlanid>** - Enter the VLAN ID used here. |
| **<macaddr>** - Specifies the MAC address of the NLB multicast FDB entry to be created. |

### Restrictions

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

### Example

To create a NLB multicast FDB entry:

```
DGS-3620-28SC: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-3620-28SC:admin#
```

## 65-2 delete nlb multicast_fdb

### Description

This command is used to delete the Switch’s NLB multicast FDB entry.

### Format

**delete nlb multicast_fdb [<vlan_name 32> | vlanid <vlanid>] <macaddr>**

### Parameters

**<vlan_name 32>** - Enter the VLAN name of the NLB multicast FDB entry here. This name can be up to 32 characters long.
**vlanid** - Specifies the VLAN ID used.
**<vlanid>** - Enter the VLAN ID used here.

**<macaddr>** - Specifies the MAC address of the NLB multicast FDB entry to be deleted.

### Restrictions

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

### Example

To delete NLB multicast FDB entry:

```
DGS-3620-28SC: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-3620-28SC:admin#
```

## 65-3 config nlb multicast_fdb

### Description

This command is used to configure the Switch’s NLB multicast FDB entry.

### Format

**config nlb multicast_fdb [<vlan_name 32> | vlanid <vlanid>] <macaddr> [add | delete] <portlist>**

### Parameters

**<vlan_name 32>** - Enter the VLAN name of the NLB multicast FDB entry here. This name can be up to 32 characters long.
**vlanid** - Specifies the VLAN ID used.
    **<vlanid>** - Enter the VLAN ID used here.

**<macaddr>** - Specifies the MAC address of the NLB multicast FDB entry to be configured.

**add** - Specifies a list of forwarding ports to be added.
**delete** - Specifies a list of forwarding ports to be deleted.

**<portlist>** - Specifies a list of forwarding ports to be added or deleted.

### Restrictions

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

### Example

To configure NLB multicast MAC forwarding database:

```
DGS-3620-28SC:admin# config nlb multicast_fdb default 03-bf-01-01-01-01 add
1:1-1:5
Command: config nlb multicast_fdb default 03-bf-01-01-01-01 add 1:1-1:5

Success.

DGS-3620-28SC:admin#
```

## 65-4 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-3620-28SC:admin# show nlb fdb
Command: show nlb fdb

MAC Address         VLAN ID        Egress Ports
----------------- ----------  ----------------------------------
02-bf-01-01-01-01    -           1:1-1:5,1:26,2:26
02-bf-01-01-01-02    -           1:1-1:5,1:26,2:26
03-bf-01-01-01-01   100          1:1-1:5,1:26,2:26
03-bf-01-01-01-01    1           1:1-1:5,1:26,2:26

Total Entries : 4

DGS-3620-28SC:admin#
```

# Chapter 66 Network Management Commands

**enable snmp**

**disable snmp**

**create trusted_host** [<ipaddr> | <ipv6addr> | network <network_address> | ipv6_prefix <ipv6networkaddr>] {snmp | telnet | ssh | http | https | ping}

**config trusted_host** [<ipaddr> | <ipv6addr> | network <network_address> | ipv6_prefix <ipv6networkaddr>] [add | delete] {snmp | telnet | ssh | http | https | ping | all}

**delete trusted_host** [ipaddr <ipaddr> | ipv6address <ipv6addr> | network <network_address>| ipv6_prefix <ipv6networkaddr> | all]

**show trusted_host**

**config snmp system_name** <sw_name>

**config snmp system_location** <sw_location>

**config snmp system_contact** <sw_contact>

**enable snmp traps**

**disable snmp traps**

**enable snmp authenticate_traps**

**disable snmp authenticate_traps**

**enable snmp linkchange_traps**

**disable snmp linkchange_traps**

**show snmp traps** {linkchange_traps {ports <portlist>}}

**config snmp linkchange_traps ports** [all | <portlist>] [enable | disable]

**config snmp coldstart_traps** [enable | disable]

**config snmp warmstart_traps** [enable | disable]

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

**show trap source_ipif**

**config rmon trap** {rising_alarm [enable | disable] | falling_alarm [enable | disable]}

**show rmon**

## 66-1 enable snmp

### Description

This command is used to enable the SNMP function. When SNMP function is disabled, the network manager will not be able to access SNMP MIB objects. The device will not send traps or notification to network manager either.

### Format

**enable snmp**

### Parameters

None.

### Restrictions

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

### Example

To enable SNMP:

```
DGS-3620-28SC:admin#enable snmp
Command: enable snmp

Success.

DGS-3620-28SC:admin#
```

## 66-2 disable snmp

### Description

This command is used to disable the SNMP function. When SNMP function is disabled, the network manager will not be able to access SNMP MIB objects. The device will not send traps or notification to network manager either.

### Format

**disable snmp**

### Parameters

None. By default, SNMP is disabled.

### Restrictions

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

### Example

To disable SNMP:

```
DGS-3620-28SC:admin#disable snmp
Command: disable snmp

Success.

DGS-3620-28SC:admin#
```

## 66-3 create trusted_host

### Description

This command is used to create the trusted host. The switch allows you to specify up to twenty IP addresses (or IP ranges) that are allowed to manage the switch via in-band SNMP or Telnet based management software. These IP addresses must be members of the Management VLAN. If no IP addresses are specified, then there is nothing to prevent any IP address from accessing the switch, provided the user knows the Username and Password.

### Format

**create trusted_host [<ipaddr> | <ipv6addr> | network <network_address> | ipv6_prefix <ipv6networkaddr>] {snmp | telnet | ssh | http | https | ping}**

### Parameters

**<ipaddr>** - Specify the IP address of the trusted host.

**<ipv6addr>** - Specify the IPv6 address of the trusted host.

**network** - Specify the network address of the trusted network. The form of network address is xxx.xxx.xxx.xxx/y.

**<network_address>** - Specify the network address of the trusted network. The form of network address is xxx.xxx.xxx.xxx/y.

**ipv6_prefix** - Specify the IPv6 network address of the trusted network.

**<ipv6networkaddr>** - Specify the IPv6 network address of the trusted network.

**snmp** - (Optional) Specify the trusted host for SNMP.

**telnet** - (Optional) Specify the trusted host for Telnet.

**ssh** - (Optional) Specify the trusted host for SSH.

**http** - (Optional) Specify the trusted host for HTTP.

**https** - (Optional) Specify the trusted host for HTTPs.

**ping** - (Optional) Specify the trusted host for Ping.

**Note:** If no management method is specified, the IP (range) can access the Switch through any method.

### Restrictions

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

### Example

To create a trusted host:

```
DGS-3620-28SC:admin#create trusted_host 10.48.74.121
Command: create trusted_host 10.48.74.121

Success.

DGS-3620-28SC:admin#
```

## 66-4 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>** - Specify the IP address of the trusted host.

**<ipv6addr>** - Specify the IPv6 address of the trusted host.

**network** - Specify the network address of the trusted network. The form of network address is xxx.xxx.xxx.xxx/y.
  **<network_address>** - Specify the network address of the trusted network. The form of network address is xxx.xxx.xxx.xxx/y.

**ipv6_prefix** - Specify the IPv6 network address of the trusted network.
  **<ipv6networkaddr>** - Specify the IPv6 network address of the trusted network.

**add** - Allow to manage applications for a trusted host.

**delete** - Prevent from managing applications for a trusted host.

**snmp** - (Optional) Specify the trusted host for SNMP.

**telnet** - (Optional) Specify the trusted host for Telnet.

**ssh** - (Optional) Specify the trusted host for SSH.

**http** - (Optional) Specify the trusted host for HTTP.

**https** - (Optional) Specify the trusted host for HTTPs.

**ping** - (Optional) Specify the trusted host for Ping.

**all** - Specify the trusted host for all applications.

### Restrictions

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

### Example

To configure the trusted host:

```
DGS-3620-28SC:admin#config trusted_host 10.48.74.121 add ssh telnet
Command: config trusted_host 10.48.74.121 add ssh telnet

Success.

DGS-3620-28SC:admin#
```

## 66-5 delete trusted_host

### Description

This command is used to delete a trusted host entry.

### Format

**delete trusted_host [ipaddr <ipaddr> | ipv6address <ipv6addr> | network <network_address> | ipv6_prefix <ipv6networkaddr> | all]**

### Parameters

**ipaddr** - Specify the IP address of the trusted host.
  **<ipaddr>** - Specify the IP address of the trusted host.

**ipv6address** - Specify the IPv6 address of the trusted host.
  **<ipv6addr>** - Specify the IPv6 address of the trusted host.

**network** - Specify the network address of the trusted network. The form of network address is xxx.xxx.xxx.xxx/y.

**<network_address>** - Specify the network address of the trusted network. The form of network address is xxx.xxx.xxx.xxx/y.

**ipv6_prefix** - Specify the IPv6 network address of the trusted network.
**<ipv6networkaddr>** - Specify the IPv6 network address of the trusted network.

**all** - Specify that all trusted hosts will be deleted.

### Restrictions

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

### Example

To delete a trusted host:

```
DGS-3620-28SC:admin#delete trusted_host ipaddr 10.48.74.121
Command: delete trusted_host ipaddr 10.48.74.121

Success.

DGS-3620-28SC:admin#
```

## 66-6 show trusted_host

### Description

This command is used to display the trusted hosts.

### Format

**show trusted_host**

### Parameters

None.

### Restrictions

None.

### Example

To display trusted hosts:

```
DGS-3620-28SC:admin#show trusted_host
Command: show trusted_host

Management Stations

IP Address                                           Access Interface
----------------------------------------------------------------------------
10.48.93.100
10.51.17.1
```

```
10.50.95.90

Total Entries : 3

DGS-3620-28SC:admin#
```

## 66-7 config snmp system_name

### Description

This command is used to configure the SNMP system name of the switch.

### Format

**config snmp system_name <sw_name>**

### Parameters

**<sw_name>** - Specify an SNMP system name for the switch. A maximum of 255 characters is allowed.

### Restrictions

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

### Example

To configure the switch SNMP name for “DGS-3620-28SC Gigabit Ethernet Switch”:

```
DGS-3620-28SC:admin# config snmp system_name DGS-3620-28SC Gigabit Ethernet
Switch
Command: config snmp system_name DGS-3620-28SC Gigabit Ethernet Switch

Success.

DGS-3620-28SC:admin#
```

## 66-8 config snmp system_location

### Description

This command is used to enter a description of the SNMP system location of the switch. A maximum of 255 characters can be used.

### Format

**config snmp system_location <sw_location>**

### Parameters

**<sw_location>** - Specify an SNMP system location for the switch. A maximum of 255 characters is allowed.

### Restrictions

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

### Example

To configure the switch location for “HQ 5F”:

```
DGS-3620-28SC:admin#config snmp system_location HQ 5F
Command: config snmp system_location HQ 5F

Success.

DGS-3620-28SC:admin#
```

## 66-9 config snmp system_contact

### Description

This command is used to enter the name and/or other information to identify an SNMP system contact person who is responsible for the switch. A maximum of 255 characters can be used.

### Format

**config snmp system_contact <sw_contact>**

### Parameters

**<sw_contact>** - Specify an SNMP system contact person. A maximum of 255 characters is allowed.

### Restrictions

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

### Example

To configure the switch contact to “`MIS Department IV`”:

```
DGS-3620-28SC:admin#config snmp system_contact "MIS Department IV"
Command: config snmp system_contact "MIS Department IV"

Success.

DGS-3620-28SC:admin#
```

## 66-10 enable snmp traps

### Description

This command is used to enable SNMP trap support on the switch.

### Format

**enable snmp traps**

### Parameters

None.

### Restrictions

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

### Example

To enable SNMP trap support:

```
DGS-3620-28SC:admin#enable snmp traps
Command: enable snmp traps

Success.

DGS-3620-28SC:admin#
```

## 66-11 disable snmp traps

### Description

This command is used to disable SNMP trap support on the switch.

### Format

**disable snmp traps**

### Parameters

None.

### Restrictions

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

### Example

To prevent SNMP traps from being sent from the switch:

```
DGS-3620-28SC:admin#disable snmp traps
Command: disable snmp traps

Success.

DGS-3620-28SC:admin#
```

## 66-12 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 Administrator and Operator-level users can issue this command.

### Example

To enable SNMP authentication trap support:

```
DGS-3620-28SC:admin#enable snmp authenticate_traps
Command: enable snmp authenticate_traps

Success.

DGS-3620-28SC:admin#
```

## 66-13 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 Administrator and Operator-level users can issue this command.

### Example

To disable SNMP authentication trap support:

```
DGS-3620-28SC:admin#disable snmp authenticate_traps
```

```
Command: disable snmp authenticate_traps

Success.

DGS-3620-28SC:admin#
```

## 66-14 enable snmp linkchange_traps

### Description

This command is used to enable SNMP linkchange trap support.

### Format

**enable snmp linkchange_traps**

### Parameters

None.

### Restrictions

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

### Example

To enable SNMP linkchange trap support:

```
DGS-3620-28SC:admin#enable snmp linkchange_traps
Command: enable snmp linkchange_traps

Success.

DGS-3620-28SC:admin#
```

## 66-15 disable snmp linkchange_traps

### Description

This command is used to disable SNMP linkchange trap support.

### Format

**disable snmp linkchange_traps**

### Parameters

None.

### Restrictions

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

### Example

To disable SNMP linkchange trap support:

```
DGS-3620-28SC:admin#disable snmp linkchange_traps
Command: disable snmp linkchange_traps

Success.

DGS-3620-28SC:admin#
```

## 66-16 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 traps.

### Format

**config snmp linkchange_traps ports [all | <portlist>] [enable | disable]**

### Parameters

**all** - Specify all ports.

**<portlist>** - Specify a port or range of ports.

**enable** - Enable sending of the link change trap for this port.
**disable** - Disable sending of the link change trap for this port.

### Restrictions

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

### Example

To enable SNMP linkchange traps for ports 1 to 4:

```
DGS-3620-28SC:admin#config snmp linkchange_traps ports 1-4 enable
Command: config snmp linkchange_traps ports 1-4 enable

Success.

DGS-3620-28SC:admin#
```

## 66-17 show snmp traps

### Description

This command is used to display the SNMP trap state.

### Format

**show snmp traps {linkchange_traps {ports <portlist>}}**

### Parameters

**linkchange_traps** - (Optional) Specify to display the status of linkchange traps.

**ports** - (Optional) Specify a port or port range.
**<portlist>** - Specify a port or port range.

### Restrictions

None.

### Example

To display SNMP traps:

```
DGS-3620-28SC:admin#show snmp traps
Command: show snmp traps

SNMP Traps         : Enabled
Authenticate Trap  : Enabled
Linkchange Traps   : Enabled
Coldstart Traps    : Enabled
Warmstart Traps    : Enabled

DGS-3620-28SC:admin#
```

To display SNMP linkchange traps:

```
DGS-3620-28SC:admin#show snmp traps linkchange_traps
Command: show snmp traps linkchange_traps

Linkchange Traps   : Enabled
  Port 1 : Enabled
  Port 2 : Enabled
  Port 3 : Enabled
  Port 4 : Enabled
  Port 5 : Enabled
  Port 6 : Enabled
  Port 7 : Enabled
  Port 8 : Enabled
  Port 9 : Enabled
  Port 10: Enabled
  Port 11: Enabled
  Port 12: Enabled
  Port 13: Enabled
  Port 14: Enabled
  Port 15: Enabled
  Port 16: Enabled
  Port 17: Enabled
  Port 18: Enabled
  Port 19: Enabled
  Port 20: Enabled
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

## 66-18 config snmp coldstart_traps

### Description

This command is used to configure the trap state for coldstart events.

### Format

**config snmp coldstart_traps [enable | disable]**

### Parameters

**enable** - Enable traps for coldstart events. The default state is enabled.

**disable** - Disable traps for coldstart events.

### Restrictions

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

### Example

To enable traps for coldstart events:

```
DGS-3620-28SC:admin#config snmp coldstart_traps enable
Command: config snmp coldstart_traps enable

```

```
Success.

DGS-3620-28SC:admin#
```

## 66-19 config snmp warmstart_traps

### Description

This command is used to configure the trap state for warmstart events.

### Format

**config snmp warmstart_traps [enable | disable]**

### Parameters

**enable** - Enable traps for warmstart events. The default state is enabled.

**disable** - Disable traps for warmstart events.

### Restrictions

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

### Example

To enable traps for warmstart events:

```
DGS-3620-28SC:admin#config snmp warmstart_traps enable
Command: config snmp warmstart_traps enable

Success.

DGS-3620-28SC:admin#
```

## 66-20 config trap source_ipif

### Description

This command is used to force change the ipif information in trap messages. By default, trap messages will carry the information of the ipif they belong to.

### Format

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

### Parameters

**<ipif_name 12> -** Specify the IP interface name. If only this parameter is specified, the IPv4 address and the smallest IPv6 address of ipif_name will be used as source IP addresses.

**<ipaddr>** - (Optional) Specify the IPv4 address.

**<ipv6addr>** - (Optional) Specify the IPv6 address.

**none** - Specify to clear the configured source IP interface.

### Restrictions

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

### Example

To configure the trap source IP interface:

```
DGS-3620-28SC:admin#config trap source_ipif inter4
Command: config trap source_ipif inter4

Success.

DGS-3620-28SC:admin#
```

To clear the configured trap source IP interface:

```
DGS-3620-28SC:admin#config trap source_ipif none
Command: config trap source_ipif none

Success.

DGS-3620-28SC:admin#
```

## 66-21 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

To display the trap source IP interface:

```
DGS-3620-28SC:admin#show trap source_ipif
Command: show trap source_ipif

Trap Source IP Interface Configuration:

```

```
IP Interface        : ipif4
IPv4 Address        : None
IPv6 Address        : 3000::52

DGS-3620-28SC:admin#
```

## 66-22 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]}**

### Parameters

**rising_alarm** - (Optional) Specify the trap state for rising alarm. The default state is enabled.
  **enable** - Enable the trap state for rising alarm.
  **disable** - Disable the trap state for rising alarm.

**falling_alarm** - (Optional) Specify the trap state for falling alarm. The default state is enabled.
  **enable** - Enable the trap state for falling alarm.
  **disable** - Disable the trap state for falling alarm.

### Restrictions

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

### Example

To disable the trap state for RMON:

```
DGS-3620-28SC:admin#config rmon trap rising_alarm disable
Command: config rmon trap rising_alarm disable

Success.

DGS-3620-28SC:admin#
```

## 66-23 show rmon

### Description

This command is used to display RMON related settings.

### Format

**show rmon**

### Parameters

None.

### Restrictions

None.

### Example

To display current RMON settings:

```
DGS-3620-28SC:admin#show rmon
Command: show rmon

RMON Rising Alarm Trap   : Enabled
RMON Falling Alarm Trap  : Enabled

DGS-3620-28SC:admin#
```

# Chapter 67 Network Monitoring Commands

**show packet ports** <portlist>

**show error ports** <portlist>

**show utilization** [ports | cpu]

**show utilization dram** {unit <unit_id>}

**show utilization flash** {unit <unit_id>}

**clear counters** {ports <portlist>}

**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_save_timing**

**show log_software_module**

**config log_save_timing** [time_interval <min 1-65535> | on_demand | log_trigger]

**enable syslog**

**disable syslog**

**show syslog**

**config syslog host** [<index> | all] {severity [emergency | alert | critical | error | warning | notice | informational | debug | <level 0-7>] | facility [local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7] | udp_port <udp_port_number> | ipaddress [<ipaddr> | <ipv6addr>] | state [enable | disable]}(1)

**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]}

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

**show syslog host** {<index 1-4>}

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

**show syslog source_ipif**

**show attack_log** {index <value_list>}

**clear attack_log**

## 67-1 show packet ports

### Description

This command is used to display statistics about the packets sent and received by the switch.

### Format

**show packet ports <portlist>**

### Parameters

**<portlist>** - Specify a port or range of ports to be displayed.

### Restrictions

None.

### Example

To display the packets analysis for port 7:

```
DGS-3620-28SC:admin#show packet ports 7
Command: show packet ports 7

 Port number : 7
 Frame Size/Type       Frame Counts                  Frames/sec
 ---------------       ----------------------        -----------
 64                    0                             0
 65-127                0                             0
 128-255               0                             0
 256-511               0                             0
 512-1023              0                             0
 1024-1518             0                             0
 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

Port number : 7
 Frame Type            Total                         Total/sec
 ---------------       ----------------------        -----------
 RX Bytes              0                             0
 RX Frames             0                             0
 TX Bytes              0                             0
 TX Frames             0                             0

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

## 67-2 show error ports

### Description

This command is used to display error statistics for a range of ports.

### Format

**show errors ports <portlist>**

### Parameters

**<portlist>** - Specify a port or range of ports to be displayed.

## Restrictions

None.

## Example

To display the errors of port 3:

```
DGS-3620-28SC:admin#show error ports 3
Command: show error ports 3

 Port Number : 3
                 RX Frames                                   TX Frames
                 ---------                                   ---------
 CRC Error       0                     Excessive Deferral    0
 Undersize       0                     CRC Error             0
 Oversize        0                     Late Collision        0
 Fragment        0                     Excessive Collision   0
 Jabber          0                     Single Collision      0
 Drop Pkts       0                     Collision             0
 Symbol Error    0

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

# 67-3 show utilization

## Description

This command is used to display real-time port utilization or CPU statistics.

## Format

**show utilization [ports | cpu]**

## Parameters

| | |
|---|---|
| **ports** - Specify to display real-time port statistics. | |
| **cpu** - Specify to display real-time CPU statistics. | |

## Restrictions

None.

## Example

To display port utilization:

```
DGS-3620-28SC: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       27     0           0           0
8       0           0           0      28     0           0           0
9      0          0          0
10     0          0          0
11     0          0          0
12     0          0          0
13     0          0          0
14     0          0          0
15     0          0          0
16     0          0          0
17     0          0          0
18     0          0          0
19     0          0          0
20     0          0          0
CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

To display CPU utilization:

```
DGS-3620-28SC:admin# show utilization cpu
Command: show utilization cpu

CPU utilization :
-------------------------------------------------------------------------------
Five seconds - 20%        One minute - 10%         Five minutes - 70%


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

## 67-4 show utilization dram

### Description

This command is used to display real-time DRAM utilization statistics.

### Format

**show utilization dram {unit <unit_id>}**

### Parameters

**unit** - Specifies which unit on the stacking system. If it is not specified, it refers to the master unit.
**<unit_id>** - Enter the unit ID used here.

### Restrictions

None.

### Example

To display DRAM utilization:

```
DGS-3620-28SC:admin# show utilization dram
Command: show utilization dram

DRAM utilization :
           Total DRAM     : 262144   KB
           Used DRAM      :  119586   KB
           Utilization    :  45%


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

## 67-5 show utilization flash

### Description

This command is used to display real-time Flash utilization statistics.

### Format

**show utilization flash {unit <unit_id>}**

### Parameters

**unit** - Specifies which unit on the stacking system. If it is not specified, it refers to the master unit.
**<unit_id>** - Enter the unit ID used here.

### Restrictions

None.

### Example

To display Flash utilization:

```
DGS-3620-28SC:admin# show utilization flash
Command: show utilization flash

FLASH Memory Utilization :
           Total FLASH     : 30608   KB
           Used FLASH      :  4786    KB
           Utilization     :  15%


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

## 67-6 clear counters

### Description

This command is used to clear the switch’s statistics counters.

### Format

**clear counters {ports <portlist>}**

### Parameters

**ports** - Specify a range of ports to be configured. The beginning and end of the port list range are separated by a dash.
**<portlist>** - Specify a range of ports to be configured.

**Note:** If no parameter is specified, the system will count all of the ports.

### Restrictions

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

### Example

To clear the switch's statistics counters for ports 7 to 9:

```
DGS-3620-28SC:admin#clear counters ports 7-9
Command: clear counters ports 7-9

Success.

DGS-3620-28SC:admin#
```

## 67-7 clear log

### Description

This command is used to clear the switch's history log.

### Format

**clear log**

### Parameters

None.

### Restrictions

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

### Example

To clear the switch's history log:

```
DGS-3620-28SC:admin#clear log
```

```
Command: clear log

Success

DGS-3620-28SC:admin#
```

## 67-8 show log

### Description

This command is used to display the switch 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 to display the history log between two values.
**<value_list>** - Specify to display the history log between two values. For example, show log index 1-5 will display the history log from 1 to 5.

**severity** - (Optional) Specify the severity level: emergency, alert, critical, error, warning, notice, informational, or debug.
**module** – (Optional) Specify the modules to be displayed. The module can be obtained by the show log_software_module command. Use commas to separate multiple modules.
**<module_list>** - Specify the modules to be displayed.

**emergency** - (Optional) Specify severity level 0.

**alert** - (Optional) Specify severity level 1.

**critical** - (Optional) Specify severity level 2.

**error** - (Optional) Specify severity level 3.

**warning** - (Optional) Specify severity level 4.

**notice** - (Optional) Specify severity level 5.

**informational** - (Optional) Specify severity level 6.

**debug** - (Optional) Specify severity level 7.

**<level_list 0-7>** - (Optional) Specify a list of severity levels to be displayed. If more than one severty level, separate them by comma. The level numbers are from 0 to 7.

**module** - Specify the modules to be displayed. The module can be obtained by the show log_software_module command. Use commas to separate multiple modules.
**<module_list>** - Specify the modules to be displayed.

**Note:** If no parameter is specified, all history log entries will be displayed.

### Restrictions

None.

### Example

To display the switch history log:

```
DGS-3620-28SC:admin#show log index 1-5
Command: show log index 1-5
```

```
Index Date       Time     Level   Log Text
----- ---------- -------- ------- --------------------------------------------

3     2000-03-01 00:26:51 INFO(6) Successful login through Console (Username:
Anonymous)
2     2000-03-01 00:26:49 CRIT(2) System started up
1     2000-03-01 00:26:49 CRIT(2) System warm start

DGS-3620-28SC:admin#
```

## 67-9 show log_save_timing

### Description

This command is used to display the method to save log.

### Format

**show log_save_log_timing**

### Parameters

None.

### Restrictions

None.

### Example

To display the method to save log:

```
DGS-3620-28SC:admin#show log_save_timing
Command: show log_save_timing

Saving Log Method:  On_demand

DGS-3620-28SC:admin#
```

## 67-10 show log_software_module

### Description

This command is used to display the protocols or applications that support the enhanced log.

### Format

**show log_software_module**

## Parameters

None.

## Restrictions

None.

## Example

To display the the protocols or applications that support the enhanced log:

```
DGS-3620-28SC:admin#show log_software_module
Command: show log_software_module

CFM_EXT             DHCPv6_CLIENT       DHCPv6_RELAY        DHCPv6_SERVER
ERPS                ERROR_LOG           MSTP                OSPFV2
VRRP

DGS-3620-28SC:admin#
```

# 67-11 config log_save_timing

## Description

This command is used to set the method to save log.

## Format

**config log_save_timing [time_interval <min 1-65535> | on_demand | log_trigger]**

## Parameters

| |
|---|
| **time_interval** - Specify to save log to Flash every xxx minutes. If no log occurs in this period, nothing will be saved.<br>**<min 1-65535>** - Specify the time between 1 and 65535 minutes. |
| **on_demand** - Specify to save log to Flash whenever the user types "save log" or "save all". This is the default. |
| **log_trigger** - Specify to save log to Flash whenever log arrives. |

## Restrictions

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

## Example

To configure method to save log as on demand:

```
DGS-3620-28SC:admin# config log_save_timing on_demand
Command: config log_save_timing on_demand

Success.
```

```
DGS-3620-28SC:admin#
```

## 67-12 enable syslog

### Description

This command is used to globally enable syslog to send log messages to a remote server.

### Format

**enable syslog**

### Parameters

None.

### Restrictions

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

### Example

To enable syslog to send a message:

```
DGS-3620-28SC:admin#enable syslog
Command: enable syslog

Success

DGS-3620-28SC:admin#
```

## 67-13 disable syslog

### Description

This command is used to disable syslog from sending a message.

### Format

**disable syslog**

### Parameters

None.

### Restrictions

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

### Example

To disable syslog sending a message:

```
DGS-3620-28SC:admin#disable syslog
Command: disable syslog

Success

DGS-3620-28SC:admin#
```

## 67-14 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-3620-28SC:admin#show syslog
Command: show syslog

Syslog Global State: Enabled

DGS-3620-28SC:admin#
```

## 67-15 config syslog host

### Description

This command is used to configure the syslog host configuration.

### Format

**config syslog host [<index> | all] {severity [emergency | alert | critical | error | warning | notice | informational | debug | <level 0-7>] | facility [local0 | local1 | local2 | local3 | local4 |**

**local5 | local6 | local7] | udp_port <udp_port_number> | ipaddress[ <ipaddr> | <ipv6addr>] | state [enable | disable]} (1)**

## Parameters

**<index>** - Specify the host index.

**all** - Specify all hosts.

**severity** - (Optional) Specify the severity level supported: emergency, alert, critical, error, warning, notice, informational, or debug.
**emergency** - Specify emergency messages.
**alert** - Specify alert messages.
**critical** - Specify critical messages.
**error** - Specify error messages.
**warning** - Specify warning messages.
**notice** - Specify notice messages.
**informational** - Specify informational messages.
**debug** - Specify debug messages.
**<level 0-7>** - Specify a level 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 in the following:
**local0** - User-defined facility.
**local1** - User-defined facility.
**local2** - User-defined facility.
**local3** - User-defined facility.
**local4** - User-defined facility.
**local5** - User-defined facility.
**local6** - User-defined facility.
**local7** - User-defined facility.

**udp_port** - Specify the UDP port number.
**<udp_port_number>** - Specify the UDP port number.

**ipaddress** - Specify the IPv4 address or IPv6 address of the host.
**<ipaddr>** - Specify the IPv4 address of the host.
**<ipv6addr>** - Specify the IPv6 address of the host.

**state** - The syslog protocol has been used for the transmission of event notification messages across networks to host. This option enables or disables the host to receive such messages.
**enable** - Enable the host to receive messages.
**disable** - Disable the host to receive messages.

## Restrictions

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

## Example

To configure the syslog host configuration:

```
DGS-3620-28SC:admin# config syslog host all severity informational facility
local0
Command: config syslog host all severity informational facility local0


Success.


DGS-3620-28SC:admin#
```

## 67-16 create syslog host

### Description

This command is used to create a new syslog 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>** - Specify the host index.

**ipaddress** - Specify the IPv4 address or IPv6 address of the host.
**<ipaddr>** - Specify the IPv4 address of the host.
**<ipv6addr>** - Specify the IPv6 address of the host.

**severity** - (Optional) Specify the severity level supported: emergency, alert, critical, error, warning, notice, informational, or debug.
**emergency** - Specify emergency messages.
**alert** - Specify alert messages.
**critical** - Specify critical messages.
**error** - Specify error messages.
**warning** - Specify warning messages.
**notice** - Specify notice messages.
**informational** - Specify informational messages.
**debug** - Specify debug messages.
**<level 0-7>** - Specify a level 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 in the following:
**local0** - User-defined facility.
**local1** - User-defined facility.
**local2** - User-defined facility.
**local3** - User-defined facility.
**local4** - User-defined facility.
**local5** - User-defined facility.
**local6** - User-defined facility.
**local7** - User-defined facility.

**udp_port** - Specify the UDP port number.
**<udp_port_number>** - Specify the UDP port number.

**state** - The syslog protocol has been used for the transmission of event notification messages across networks to host. This option enables or disables the host to receive such messages.
**enable** - Enable the host to receive messages.
**disable** - Disable the host to receive messages.

### Restrictions

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

### Example

To create a new syslog host:

```
DGS-3620-28SC:admin# create syslog host 1 ipaddress 10.1.1.1
Command: create syslog host 1 ipaddress 10.1.1.1

Success.

DGS-3620-28SC:admin#
```

## 67-17 delete syslog host

### Description

This command is used to delete syslog host(s).

### Format

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

### Parameters

| |
|---|
| **<inex 1-4>** - Specify the host index. |
| **all** - Specify all hosts. |

### Restrictions

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

### Example

To delete a syslog host:

```
DGS-3620-28SC:admin#delete syslog host 4
Command: delete syslog host 4

Success

DGS-3620-28SC:admin#
```

## 67-18 show syslog host

### Description

This command is used to display syslog host configurations.

### Format

**show syslog host {<index 1-4>}**

### Parameters

| |
|---|
| **<index 1-4>** - (Optional) Specify the host index. |

**Note:** If no parameter is specified, all hosts will be displayed.

### Restrictions

None.

### Example

To display syslog host configurations:

```
DGS-3620-28SC:admin#show syslog host
Command: show syslog host

Syslog Global State: Disabled

Host 1
  IP Address      : 10.1.1.2
  Severity        : Warning
  Facility        : Local10
  UDP port        : 514
  Status          : Disabled

Host 2
  IP Address      : 3000:501:100:ffff:101:202:303:1
  Severity        : Emergency
  Facility        : Local10
  UDP port        : 514
  Status          : Disabled

Total Entries : 2

DGS-3620-28SC:admin#
```

## 67-19 config syslog source_ipif

### Description

This command is used to force change the ipif information in syslogs. By default, syslogs will carry the information of the ipif they belong to.

### Format

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

### Parameters

**<ipif_name 12>** - Specify the IP interface name. If only this parameter is specified, the IPv4 address and the smallest IPv6 address of ipif_name will be used as source IP addresses.

**<ipaddr>** - (Optional) Specify the IP4 address.

**<ipv6addr>** - (Optional) Specify the IPv6 global address.

**none** - Specify to clear the configured source IP interface.

### Restrictions

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

### Example

To configure the syslog source IP interface:

```
DGS-3620-28SC:admin#config syslog source_ipif Sysetm
Command: config syslog source_ipif System

Success.

DGS-3620-28SC:admin#
```

To clear the configured source IP interface for syslog:

```
DGS-3620-28SC:admin#config syslog source_ipif none
Command: config syslog source_ipif none

Success.

DGS-3620-28SC:admin#
```

## 67-20 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

To display the syslog source interface:

```
DGS-3620-28SC:admin#show syslog source_ipif
Command: show syslog source_ipif

Syslog Source IP Interface Configuration:

IP Interface        : System
IPv4 Address        : None
```

```
IPv6 Address        : None

DGS-3620-28SC:admin#
```

## 67-21 show attack_log

### Description

This command is used to display the switch's attack log.

### Format

**show attack_log {index <value_list>}**

### Parameters

**index** - (Optional) Specify the list of index of the entries that need to be displayed.
**<value_list>** - Specify the list of index 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.

**Note:** If no parameter is specified, all entries in the attack log will be displayed.

### Restrictions

None.

### Example

To display the switch's attack log:

```
DGS-3620-28SC:admin#show attack_log index 1-3
Command: show attack_log index 1-3

Index Date       Time      Level     Log Text
----- ---------- -------- --------- ---------------------------------------------
--
3     2009-12-26 14:15:45  WARN(4)   Port security violation mac addrss 00-18-
F3-10-94-89 on locking address full port 28
2     2009-12-26 14:15:45  WARN(4)  Port security violation mac addrss 00-18-
F3-10-94-89 on locking address full port 28
1     2009-12-26 14:15:45  WARN(4)  Port security violation mac addrss 00-18-
F3-10-94-89 on locking address full port 28

DGS-3620-28SC:admin#
```

## 67-22 clear attack_log

### Description

This command is used to clear the switch's attack log.

## Format

**clear attack_log**

## Parameters

None.

## Restrictions

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

## Example

To clear the switch's attack log:

```
DGS-3620-28SC:admin#clear attack_log
Command: clear attack_log

Success.

DGS-3620-28SC:admin#
```

# Chapter 68 OAM Commands

**config ethernet_oam ports** [<portlist> | all] [mode [active | passive] | state [enable | disable] | link_monitor [error_symbol {threshold <range 0-4294967295> | window <millisecond 1000-60000> | notify_state [enable | disable]}(1) | error_frame {threshold <range 0-4294967295> | window <millisecond 1000-60000> | notify_state [enable | disable]}(1) | error_frame_seconds {threshold <range 1-900> | window <millisecond 10000-900000> | notify_state [enable | disable]}(1) | error_frame_period {threshold <range 0-4294967295> | window <number 148810-100000000> | notify_state [enable | disable]}(1)] | critical_link_event [dying_gasp | critical_event] notify_state [enable | disable] | remote_loopback [start | stop] | received_remote_loopback [process | ignore]]

**show ethernet_oam ports** {<portlist>} [status | configuration | statistics | event_log {index <value_list>}]

**clear ethernet_oam ports** [<portlist> | all] [event_log | statistics]

## 68-1 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: When a port is OAM-enabled, changing the OAM mode will cause the OAM discovery to be re-started.

The command used to enable or disable port's Ethernet OAM function. The parameter enabling a port's OAM will cause the port to start OAM discovery. If a port's is active, it initiates the discovery. Otherwise it reacts to the discovery received from peer. Disabling a port's OAM will cause the port to send out a dying gasp event to peers and then disconnect the established OAM link.

The link monitoring parameter is used to configure port Ethernet OAM link monitoring error symbols. The link monitoring function provides a mechanism to detect and indicate link faults under a variety of conditions. OAM monitors the statistics on the number of frame errors as well as the number of coding symbol errors. When the number of symbol errors is equal to or greater than the specified threshold in a period and the event notification state is enabled, it generates an error symbol period event to notify the remote OAM peer. The Ethernet OAM link monitoring error frames parameter provides a mechanism to detect and indicate link faults under a variety of conditions. OAM monitors the counter on the number of frame errors as well as the number of coding symbol errors. When the number of frame errors is equal to or greater than the specified threshold in a period and the event notification state is enabled, it generates an error frame event to notify the remote OAM peer.

The link event parameter configures the capability of the Ethernet OAM critical link event. If the capability for an event is disabled, the port will never send out the corresponding critical link event. The command is used to configure the client to process or to ignore the received Ethernet OAM remote loopback command. In remote loopback mode, all user traffic will not be processed. Ignoring the received remote loopback command will prevent the port from entering remote loopback mode.

## Format

**config ethernet_oam ports [<portlist> | all] [mode [active | passive] | state [enable | disable] | link_monitor [error_symbol {threshold <range 0-4294967295> | window <millisecond 1000-60000> | notify_state [enable | disable]} (1) | error_frame {threshold <range 0-4294967295> | window <millisecond 1000-60000> | notify_state [enable | disable]} (1) | error_frame_seconds {threshold <range 1-900> | window <millisecond 10000-900000> | notify_state [enable | disable]} (1) | error_frame_period {threshold <range 0-4294967295> | window <number 148810-100000000> | notify_state [enable | disable]}(1)] | critical_link_event [dying_gasp | critical_event] notify_state [enable | disable] | remote_loopback [start | stop] | received_remote_loopback [process | ignore]]**

## Parameters

| |
|---|
| **<portlist>** - Used to specify a range of ports to be configured. |
| **all** - Used to specify all ports are to be configured. |
| **mode** - Specify the operation mode. The default mode is active.<br>**active** - Specify to operate in active mode.<br>**passive -** Specify to operate in passive mode. |
| **state** - Specify the OAM function status.<br>**enable** - Specify to enable the OAM function.<br>**disable** - Specify to disable the OAM function. |
| **link_monitor -** Used to detect and indicate link faults under a variety of conditions.<br>**error_symbol** - Used to generate an error symbol period event to notify the remote OAM peer.<br>**threshold** - 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.<br>**<range 0-4294967295>** - Specify the range from 0 to 4294967295.<br>**window** - The range is 1000 to 60000 ms. The default value is 1000ms.<br>**<millisecond 1000-60000>** -The range is 1000 to 60000 ms.<br>**notify_state** - Specify the event notification status. The default state is enable.<br>**enable** -Specify to enable event notification.<br>**disable** -Specify to disable event notification.<br>**error_frame** - Specify the error frame.<br>**threshold** - Specify a threshold range.<br>**<range 0-4294967295>** - Specify a threshold range between 0 and 4294967295.<br>**window** - The range is 1000 to 60000 ms. The default value is 1000ms.<br>**<millisecond 1000-60000> -** The range is 1000 to 60000 ms.<br>**notify_state** - Specify the event notification status. The default state is enable.<br>**enable** - Specify to enable event notification.<br>**disable** - Specify to disable event notification.<br>**error_frame_seconds** - Specify error fram time.<br>**threshold** - Specify a threshold range between 1 and 900.<br>**<range 1-900>** -Specify a threshold range between 1 and 900.<br>**window** - The range is 1000 to 900000 ms.<br>**<millisecond 10000-900000> -** The range is 1000 to 900000 ms.<br>**notify_state** - Specify the event notification status. The default state is enable.<br>**enable** - Specify to enable event notification.<br>**disable** - Specify to disable event notification.<br>**error_frame_period** - Specify error frame period.<br>**threshold** - Specify a threshold range between 0 and 4294967295.<br>**<range 0-4294967295>** -Specify a threshold range between 0 and 4294967295.<br>**window** - The range is 148810 to 100000000 ms.<br>**<number 148810-100000000>** - The range is 148810 to 100000000 ms.<br>**notify_state** - Specify the event notification status. The default state is enable.<br>**enable** - Specify to enable event notification.<br>**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 Administrator, Operator and Power-User level users can issue this command.

## Example

To configure Ethernet OAM on ports 1 to 2 in active mode:

```
DGS-3620-28SC:admin#config ethernet_oam ports 1-2 mode active
Command: config ethernet_oam ports 1-2 mode active

Success.

DGS-3620-28SC:admin#
```

To enable Ethernet OAM on port 1:

```
DGS-3620-28SC:admin#config ethernet_oam ports 1 state enable
Command: config ethernet_oam ports 1 state enable

Success.

DGS-3620-28SC:admin#
```

To configure the error symbol threshold to 2 and period to 1000ms for port 1:

```
DGS-3620-28SC: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-3620-28SC:admin#
```

To configure the error frame threshold to 2 and period to 1000 ms for port 1:

```
DGS-3620-28SC: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-3620-28SC:admin#
```

To configure the error frame seconds threshold to 2 and period to 10000 ms for port 1:

```
DGS-3620-28SC: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-3620-28SC:admin#
```

To configure the error frame threshold to10 and period to 1000000 ms for port 1:

```
DGS-3620-28SC: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-3620-28SC:admin#
```

To configure a dying gasp event for port 1:

```
DGS-3620-28SC: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-3620-28SC:admin#
```

To start remote loopback on port 1:

```
DGS-3620-28SC:admin#config ethernet_oam ports 1 remote_loopback start
Command: config ethernet_oam ports 1 remote_loopback start

Success.

DGS-3620-28SC:admin#
```

To configure the method of processing the received remote loopback command as “process” on port 1:

```
DGS-3620-28SC:admin#config ethernet_oam ports 1 received_remote_loopback
process
Command: config ethernet_oam ports 1 received_remote_loopback process

```

```
Success.

DGS-3620-28SC:admin#
```

## 68-2 show ethernet_oam ports

### Description

This command is used to display Ethernet OAM information, including status, configuration, statistics, and event log, on specified ports.

The status information includes:

(1) OAM administration status: enabled or disabled.

(2) OAM operation status. It maybe the below value:

- Disable: OAM is disabled on this port.
- LinkFault: The link has detected a fault and is transmitting OAMPDUs with a link fault indication.
- PassiveWait: The port is passive and is waiting to see if the peer device is OAM capable.
- ActiveSendLocal: The port is active and is sending local information.
- SendLocalAndRemote: The local port has discovered the peer but has not yet accepted or rejected the configuration of the peer.
- SendLocalAndRemoteOk: The local device agrees the OAM peer entity.
- PeeringLocallyRejected: The local OAM entity rejects the remote peer OAM entity.
- PeeringRemotelyRejected: The remote OAM entity rejects the local device.
- Operational: The local OAM entity learns that both it and the remote OAM entity have accepted the peering.
- NonOperHalfDuplex: Since Ethernet OAM functions are not designed to work completely over half-duplex port. This value indicates Ethernet OAM is enabled but the port is in half-duplex operation.

(3) OAM mode: passive or active.

(4) Maximum OAMPDU size: The largest OAMPDU that the OAM entity supports. OAM entities exchange maximum OAMPDU sizes and negotiate to use the smaller of the two maximum OAMPDU sizes between the peers.

(5) OAM configuration revision: The configuration revision of the OAM entity as reflected in the latest OAMPDU sent by the OAM entity. The config revision is used by OAM entities to indicate that configuration changes have occurred, which might require the peer OAM entity to re-evaluate whether OAM peering is allowed.

(6) OAM mode change.

(7) OAM Functions Supported: The OAM functions supported on this port. These functions include:

1. Unidirectional: It indicates that the OAM entity supports the transmission of OAMPDUs on links that are operating in unidirectional mode (traffic flowing in one direction only).
2. Loopback: It indicates that the OAM entity can initiate and respond to loopback commands.
3. Link Monitoring: It indicates that the OAM entity can send and receive Event Notification OAMPDUs.
4. Variable: It indicates that the OAM entity can send and receive variable requests to monitor the attribute value as described in the IEEE 802.3 Clause 30 MIB.

The event log displays Ethernet OAM event log information. The switch can buffer 1000 event logs. The event log is different from sys-log as it provides more detailed information than sys-log. Each OAM event will be recorded in both OAM event log and syslog.

## Format

**show ethernet_oam ports {<portlist>} [status | configuration | statistics | event_log {index <value_list>}]**

## Parameters

**<portlist>** - (Optional) Specify 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>** - (Optional) Specify an index range to display.

## Restrictions

None.

## Example

To display Ethernet OAM statistics information for port 1:

```
DGS-3620-28SC: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-3620-28SC:admin#
```

## 68-3 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>** - Specify 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 Administrator, Operator and Power-User level users can issue this command.

### Example

To clear port 1 OAM statistics:

```
DGS-3620-28SC:admin#clear ethernet_oam ports 1 statistics
Command: clear ethernet_oam ports 1 statistics

Success.

DGS-3620-28SC:admin#
```

To clear port 1 OAM events:

```
DGS-3620-28SC:admin#clear ethernet_oam ports 1 event_log
Command: clear ethernet_oam ports 1 event_log

Success.

DGS-3620-28SC:admin#
```

# Chapter 69 Open Shortest Path First (OSPF) Command List

**config ospf** [ipif <ipif_name 12> | all] {area <area_id> | priority <value> | hello_interval <sec 1-65535> | dead_interval <sec 1-65535> | authentication [none | simple <password 8> | md5 <key_id 1-255>] | metric <value 1-65535> | state [enable | disable] | passive [enable | disable]}(1)

**create ospf aggregation** <area_id> <network_address> lsdb_type [summary {advertise [enable | disable]} | nssa_ext {advertise [enable | disable]}]

**config ospf aggregation** <area_id> <network_address> lsdb_type [summary {advertise [enable | disable]} | nssa_ext {advertise [enable | disable]}]

**delete ospf aggregation** <area_id> <network_address> lsdb_type [summary | nssa_ext]

**show ospf aggregation** {<area_id>}

**create ospf area** <area_id> type [normal | [stub | nssa {translate [enable | disable]}] {stub_summary [enable | disable] | metric <value 0-65535>}]

**config ospf area** <area_id> type [normal | [stub | nssa {translate [enable | disable]}] {stub_summary [enable | disable] | metric <value 0-65535>}]

**delete ospf area** <area_id>

**show ospf area** {<area_id>}

**create ospf host_route** <ipaddr> {area <area_id> | metric <value 1-65535>}

**config ospf host_route** <ipaddr> {area <area_id> | metric <value 1-65535>}(1)

**delete ospf host_route** <ipaddr>

**show ospf host_route** {<ipaddr>}

**config ospf router_id** <ipaddr>

**create ospf virtual_link** <area_id> <neighbor_id> {hello_interval <sec 1-65535> | dead_interval <sec 1-65535> | authentication [none | simple <password 8> | md5 <key_id 1-255>]}

**config ospf virtual_link** <area_id> <neighbor_id> {hello_interval <sec 1-65535> | dead_interval <sec 1-65535> | authentication [none | simple <password 8> | md5 <key_id 1-255>]}(1)

**delete ospf virtual_link** <area_id> <neighbor_id>

**show ospf virtual_link** {<area_id> <neighbor_id>}

**enable ospf**

**show ospf** {[ipif <ipif_name 12> | all]}

**disable ospf**

**show ospf lsdb** {area <area_id> | advertise_router <ipaddr> | type [rtrlink | netlink | summary | assummary | asextlink | nssa_ext | stub]}

**show ospf neighbor** {<ipaddr>}

**show ospf virtual_neighbor** {<area_id> <neighbor_id>}

## 69-1 config ospf

### Description

This command is used to configure the OSPF interface settings.

### Format

**config ospf [ipif <ipif_name 12> | all] {area <area_id> | priority <value> | hello_interval <sec 1-65535> | dead_interval <sec 1-65535> | authentication [none | simple <password 8> | md5**

**<key_id 1-255>] | metric <value 1-65535> | state [enable | disable] | passive [enable | disable]}(1)**

### Parameters

**ipif** - Specifies the name of the IP interface.
**<ipif_name 12>** - Enter the IP interface name here. This name can be up to 12 characters long.
**all** - Specifies that all the IP interfaces will be used.

**area** - (Optional) Specifies the area to which the interface is assigned. An Area ID is a 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.
**<area_id>** - Enter the area ID used here.

**priority** - (Optional) Specifies the priority value for the Designated Router election. If a Router Priority of 0 is set, the Switch cannot be elected as the DR for the network.
**<value>** - Enter the priority value used here.

**hello_interval** - (Optional) Allows the specification of the interval between the transmission of OSPF Hello packets, in seconds. Between 1 and 65535 seconds can be specified. The Hello Interval, Dead Interval, Authorization Type, and Authorization Key should be the same for all routers on the same network.
**<sec 1-65535>** - Enter the hello packet interval value here. This value must be between 1 and 65535 seconds.

**dead_interval** - (Optional) Allows the specification of the length of time between the receipt of Hello packets from a neighbor router before the selected area declares that router down. An interval between 1 and 65535 seconds can be specified. The Dead Interval must be evenly divisable by the Hello Interval.
**<sec 1-65535>** - Enter the dead packet interval value here. This value must be between 1 and 65535 seconds.

**authentication** - (Optional) Specifies that authentication value.
**none** - Specifies that the authentication value will be set to none.
**simple** - Specifies that a simple text password must be specified.
**<password 8>** - Enter the simple text password value here.
**md5** - Specifies that the authentication will be set to use an MD5 key ID.
**<key_id 1-255>** - Enter the MD5 key used here. This key must be between 1 and 255.

**metric** - (Optional) Specifies the interface metric used.
**<value 1-65535>** - Enter the metric value here. This value must be between 1 and 65535.

**state** - (Optional) Specifies the OSPF interface state here.
**enable** - Specifies that the state will be set to enabled.
**disable** - Specifies that the state will be set to disabled.

**passive** - (Optional) Specifies whether the designated entry to be a passive interface or not. When the interface is specified to be passive, OSPF protocol packets will neither be sent out or received.
**enable** - Specifies that the passive interface will be enabled.
**disable** - Specifies that the passive interface will be disabled.

### Restrictions

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

### Example

To configure OSPF interface settings:

```
DGS-3620-28SC:admin# config ospf ipif System priority 2 hello_interval 20
metric 2 state enabled
Command: config ospf ipif System priority 2 hello_interval 20 metric 2 state
enabled

Success.

DGS-3620-28SC:admin#
```

## 69-2 create ospf aggregation

### Description

This command is used to create an OSPF area aggregation entry.

### Format

**create ospf aggregation <area_id> <network_address> lsdb_type [summary {advertise [enable | disable]} | nssa_ext {advertise [enable | disable]}]**

### Parameters

**<area_id>** - A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.

**<network_address>** - The IP address that uniquely identifies the network that corresponds to the OSPF Area. The network address format is 'IP address/prefix length'.

**lsdb_type** - Specifies the Link-State Database (LSDB) type of address aggregation.
 **summary** - Specifies the LSDB type as summary.
  **advertise** - (Optional) Allows for the advertisement of the summary LSDB.
   **enable** - Specifies that the advertisement trigger will be enabled.
   **disable** - Specifies that the advertisement trigger will be disabled.
 **nssa_ext** - Specifies the LSDB type as a Not-So-Stub Area External Route (NSSA EXT).
  **advertise** - (Optional) Allows for the advertisement of aggregated NSSA external route.
   **enable** - Specifies that the advertisement trigger will be enabled.
   **disable** - Specifies that the advertisement trigger will be disabled.

### Restrictions

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

### Example

To create OSPF area aggregation settings:

```
DGS-3620-28SC:admin# create ospf aggregation 10.1.1.1 192.168.0.0/16 lsdb_type
summary
Command: create ospf aggresgation 10.1.1.1 192.168.0.0/16 lsdb_type summary

Success.

DGS-3620-28SC:admin#
```

## 69-3 config ospf aggregation

### Description

This command is used to configure the OSPF area aggregation settings.

### Format

**config ospf aggregation <area_id> <network_address> lsdb_type [summary {advertise [enable | disable]} | nssa_ext {advertise [enable | disable]}]**

### Parameters

**<area_id>** - A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.

**<network_address>** - The IP address that uniquely identifies the network that corresponds to the OSPF Area. The network address format is 'IP address/prefix length'.

**lsdb_type** - Specifies the Link-State Database (LSDB) type of address aggregation.
- **summary** - Specifies the LSDB type as summary.
  - **advertise** - (Optional) Allows for the advertisement of the summary LSDB.
    - **enable** - Specifies that the advertisement trigger will be enabled.
    - **disable** - Specifies that the advertisement trigger will be disabled.
- **nssa_ext** - Specifies the LSDB type as a Not-So-Stub Area External Route (NSSA EXT).
  - **advertise** - (Optional) Allows for the advertisement of aggregated NSSA external route.
    - **enable** - Specifies that the advertisement trigger will be enabled.
    - **disable** - Specifies that the advertisement trigger will be disabled.

### Restrictions

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

### Example

To configure the OSPF area aggregation settings:

```
DGS-3620-28SC:admin# config ospf aggregation 10.1.1.1 10.48.76.122/16 lsdb_type
summary advertise enabled
Command: config ospf aggregation 10.1.1.1 10.48.76.122/16 lsdb_type summary
advertise enabled


Success.


DGS-3620-28SC:admin#
```

## 69-4 delete ospf aggregation

### Description

This command is used to delete an OSPF area aggregation configuration.

### Format

**delete ospf aggregation <area_id> <network_address> lsdb_type [summary | nssa_ext]**

### Parameters

**<area_id>** - A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.

**<network_address>** - The IP address that uniquely identifies the network that corresponds to the OSPF Area. The network address format is 'IP address/prefix length'.

**lsdb_type** - Specifies the LSDB type.
**summary** - Specifies the LSDB type as summary.
**nssa_ext** - Specifies the LSDB type as NSSA EXT.

### Restrictions

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

### Example

To delete an OSPF area aggregation settings:

```
DGS-3620-28SC:admin# delete ospf aggregation 10.1.1.1 10.48.76.122/16 lsdb_type
summary
Command: delete ospf aggregation 10.1.1.1 10.48.76.122/16 lsdb_type summary

Success.

DGS-3620-28SC:admin#
```

## 69-5 show ospf aggregation

### Description

This command is used to display the current OSPF aggregation table.

### Format

**show ospf aggregation {<area_id>}**

### Parameters

**<area_id>** - (Optional) Enter the area ID used here.

### Restrictions

None.

### Example

To display OSPF aggregation settings:

```
DGS-3620-28SC:admin#show ospf aggregation
Command: show ospf aggregation

OSPF Area Aggregation Settings

Area ID         Aggregated         LSDB     Advertise
                Network Address    Type
--------------- ------------------ -------- ---------
0.0.0.0         10.90.0.0/16       Summary  Enabled
0.0.0.0         10.90.0.0/17       Summary  Enabled
0.0.0.0         10.90.64.0/18      Summary  Enabled

Total Entries : 3

DGS-3620-28SC:admin#
```

## 69-6 create ospf area

### Description

This command is used to create an OSPF area. OSPF allows collections of contiguous networks and hosts to be grouped together. Such a group, together with the routers having interfaces to any one of the included networks, is called an area.

### Format

**create ospf area <area_id> type [normal | [stub | nssa {translate [enable | disable]}] {stub_summary [enable | disable] | metric <value 0-65535>}]**

### Parameters

| |
|---|
| **<area_id>** - Enter the OSPF area ID used here. |
| **type** - Specifies the OSPF area operation type. In some Autonomous Systems, the majority of the topological database may consist of AS external advertisements. An OSPF AS external advertisement is usually flooded throughout the entire AS.  However, OSPF allows certain areas to be configured as "stub areas".  AS external advertisements are not flooded into/throughout stub areas; routing to AS external destinations in these areas is based on a (per-area) default only.  This reduces the topological database size, and therefore the memory requirements, for a stub area's internal routers.<br>**normal** - Specifies that the OSPF area type will be set to normal.<br>**stub** - Specifies that the OSPF area type will be set to STUB.<br>**nssa** - Specifies that the OSPF area type will be set to NSSA.<br>**translate** - (Optional) Specifies whether translation will be enabled or disabled.<br>**enable** - Specifies that the translate option will be enabled.<br>**disable** - Specifies that the translate option will be disabled. |
| **stub_summary** - (Optional) Specifies whether the summary LSA is effective for this area.<br>**enable** - Specifies that the STUB summary option will be enabled.<br>**disable** - Specifies that the STUB summary option will be disabled. |
| **metric** - (Optional) Specifies the metric (1 - 65535; 0 for auto cost) of this area.<br>**<value 0-65535>** - Enter the metric value used here. This value must be between 0 and 65535. |

### Restrictions

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

### Example

To create an OSPF area:

```
DGS-3620-28SC:admin# create ospf area 10.48.74.122 type stub stub_summary
enabled metric 1
Command: create ospf area 10.48.74.122 type stub stub_summary enabled metric 1

Success.

DGS-3620-28SC:admin#
```

## 69-7 config ospf area

### Description

This command is used to configure an OSPF area’s settings.

### Format

**config ospf area <area_id> type [normal | [stub | nssa {translate [enable | disable]}] {stub_summary [enable | disable] | metric <value 0-65535>}]**

### Parameters

**<area_id>** - Enter the OSPF area ID used here.

**type** - Specifies the OSPF area operation type. In some Autonomous Systems, the majority of the topological database may consist of AS external advertisements. An OSPF AS external advertisement is usually flooded throughout the entire AS. However, OSPF allows certain areas to be configured as "stub areas". AS external advertisements are not flooded into/throughout stub areas; routing to AS external destinations in these areas is based on a (per-area) default only. This reduces the topological database size, and therefore the memory requirements, for a stub area's internal routers.
**normal** - Specifies that the OSPF area type will be set to normal.
**stub** - Specifies that the OSPF area type will be set to STUB.
**nssa** - Specifies that the OSPF area type will be set to NSSA.
**translate** - (Optional) Specifies whether translation will be enabled or disabled.
**enable** - Specifies that the translate option will be enabled.
**disable** - Specifies that the translate option will be disabled.

**stub_summary** - (Optional) Specifies whether the summary LSA is effective for this area.
**enable** - Specifies that the STUB summary option will be enabled.
**disable** - Specifies that the STUB summary option will be disabled.

**metric** - (Optional) Specifies the metric (1 - 65535; 0 for auto cost) of this area.
**<value 0-65535>** - Enter the metric value used here. This value must be between 0 and 65535.

### Restrictions

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

### Example

To configure an OSPF area's settings:

```
DGS-3620-28SC:admin# config ospf area 10.48.74.122 type stub stub_summary
enabled metric 1
Command: config ospf area 10.48.74.122 type stub stub_summary enabled metric 1

Success.

DGS-3620-28SC:admin#
```

## 69-8 delete ospf area

### Description

This command is used to delete an OSPF area.

### Format

**delete ospf area <area_id>**

### Parameters

**<area_id>** - Enter the OSPF area ID used here.

### Restrictions

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

### Example

To delete an OSPF area:

```
DGS-3620-28SC:admin# delete ospf area 10.48.74.122
Command: delete ospf area 10.48.74.122

Success.

DGS-3620-28SC:admin#
```

## 69-9 show ospf area

### Description

This command is used to display an OSPF area's configuration.

### Format

**show ospf area {<area_id>}**

### Parameters

**<area_id>** - (Optional) Enter the OSPF area ID used here.

### Restrictions

None.

### Example

To display OSPF area's configuration:

```
DGS-3620-28SC:admin# show ospf area
Command: show ospf area

OSPF Area Settings

Area ID         Type   Stub Import Summary LSA Stub Default Cost Translate
--------------- ------ ----------------------- ----------------- ---------
0.0.0.0         Normal None                    None              None
1.1.1.1         Normal None                    None              None
4.4.4.4         Normal None                    None              None
5.5.5.5         Stub   Enabled                 1                 None

Total Entries : 4

DGS-3620-28SC:admin#
```

## 69-10 create ospf host_route

### Description

This command is used to create an OSPF host route.

### Format

**create ospf host_route <ipaddr> {area <area_id> | metric <value 1-65535>}**

### Parameters

**<ipaddr>** - Enter the host's IP address used here.

**area** - (Optional) Specifies a 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.
**<area_id>** - Enter the area ID value here.

**metric** - (Optional) Specifies a metric that will be advertised.
**<value 1-65535>** - Enter the metric value used here. This value must be between 1 and 65535.

### Restrictions

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

### Example

To create an OSPF host route:

```
DGS-3620-28SC:admin# create ospf host_route 10.48.74.122 area 10.1.1.1 metric 2
Command: create ospf host_route 10.48.74.122 area 10.1.1.1 metric 2

Success.

DGS-3620-28SC:admin#
```

## 69-11 config ospf host_route

### Description

This command is used to configure an OSPF host route.

### Format

**config ospf host_route <ipaddr> {area <area_id> | metric <value 1-65535>}(1)**

### Parameters

**<ipaddr>** - Enter the host's IP address used here.

**area** - (Optional) Specifies a 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.
**<area_id>** - Enter the area ID value here.

**metric** - (Optional) Specifies a metric that will be advertised.
**<value 1-65535>** - Enter the metric value used here. This value must be between 1 and 65535.

### Restrictions

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

### Example

To configure an OSPF host route:

```
DGS-3620-28SC:admin# config ospf host_route 10.48.74.122 area 10.1.1.1 metric 2
Command: config ospf host_route 10.48.74.122 area 10.1.1.1 metric 2

Success.

DGS-3620-28SC:admin#
```

## 69-12 delete ospf host_route

### Description

This command is used to delete an OSPF host route.

### Format

**delete ospf host_route <ipaddr>**

### Parameters

**<ipaddr>** - Enter the host’s IP address used here.

### Restrictions

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

### Example

To delete an OSPF host route:

```
DGS-3620-28SC:admin# delete ospf host_route 10.48.74.122
Command: delete ospf host_route 10.48.74.122

Success.

DGS-3620-28SC:admin#
```

## 69-13 show ospf host_route

### Description

This command is used to display the current OSPF host route table.

### Format

**show ospf host_route {<ipaddr>}**

### Parameters

**<ipaddr>** - (Optional) Enter the host’s IP address used here.

### Restrictions

None.

### Example

To display the OSPF host route settings:

```
DGS-3620-28SC:admin# show ospf host_route
Command: show ospf host_route

OSPF Host Route Settings

Host Address    Metric Area ID
--------------- ------ ---------------
10.48.73.21        2   10.1.1.1
10.48.74.122       1   10.1.1.1

Total Entries : 2

DGS-3620-28SC:admin#
```

## 69-14 config ospf router_id

### Description

The command is used to configure the router ID for the switch. Each switch that is configured to run OSPF must have a unique router ID.

### Format

**config ospf router_id <ipaddr>**

### Parameters

**<ipaddr>** - Enter the router's IP address here.

### Restrictions

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

### Example

To configure the router ID for the switch:

```
DGS-3620-28SC:admin# config ospf router_id 10.48.74.122
Command: config ospf router_id 10.48.74.122

Success.

DGS-3620-28SC:admin#
```

## 69-15 create ospf virtual_link

### Description

This command is used to create an OSPF virtual link.

### Format

**create ospf virtual_link <area_id> <neighbor_id> {hello_interval <sec 1-65535> | dead_interval <sec 1-65535> | authentication [none | simple <password 8> | md5 <key_id 1-255>]}**

### Parameters

**<area_id>** - Specifies a 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.

**<neighbor_id>** - Specifies the OSPF router ID for the remote area. This is a 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the remote area's Area Border Router. This is the router ID of the neighbor router.

**hello_interval** - (Optional) Allows the specification of the interval between the transmission of OSPF Hello packets, in seconds. The Hello Interval, Dead Interval, Authorization Type, and Authorization Key should be the same for all routers on the same network.

**<sec 1-65535>** - Enter the hello packet interval used here. This value must be between 1 and 65535.

**dead_interval** - (Optional) Allows the specification of the length of time between the receipt of Hello packets from a neighbor router before the selected area declares that router down. An interval between 1 and 65535 seconds can be specified. The Dead Interval must be evenly divisable by the Hello Interval.

**<sec 1-65535>** - Enter the dead packet interval used here. This value must be between 1 and 65535.

**authentication** - (Optional) Specifies the authentication type used.

**none** - Specifies that the authentication type will be set to none.

**simple** - Specifies that a simple text password will be used in the authentication.

**<password 8>** - Enter the simple text password value here. This value can be up to 8 characters long.

**md5** - Specifies that an MD5 key ID will be used for the authentication.

**<key_id 1-255>** - Enter the MD5 key ID value used here. This value can be between 1 and 255.

### Restrictions

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

### Example

To create a virtual link to another ABR:

```
DGS-3620-28SC:admin# create ospf virtual_link 10.1.1.12 20.1.1.1 hello_interval
10
Command: create ospf virtual_link 10.1.1.12 20.1.1.1 hello_interval 10

Success.

DGS-3620-28SC:admin#
```

## 69-16 config ospf virtual_link

### Description

This command is used to configure the OSPF virtual link.

### Format

**config ospf virtual_link <area_id> <neighbor_id> {hello_interval <sec 1-65535> | dead_interval <sec 1-65535> | authentication [none | simple <password 8> | md5 <key_id 1-255>]} (1)**

### Parameters

**<area_id>** - Specifies a 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.

**<neighbor_id>** - Specifies the OSPF router ID for the remote area. This is a 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the remote area's Area Border Router. This is the router ID of the neighbor router.

**hello_interval** - (Optional) Allows the specification of the interval between the transmission of OSPF Hello packets, in seconds. The Hello Interval, Dead Interval, Authorization Type, and Authorization Key should be the same for all routers on the same network.
- **<sec 1-65535>** - Enter the hello packet interval used here. This value must be between 1 and 65535.

**dead_interval** - (Optional) Allows the specification of the length of time between the receipt of Hello packets from a neighbor router before the selected area declares that router down. An interval between 1 and 65535 seconds can be specified. The Dead Interval must be evenly divisable by the Hello Interval.
- **<sec 1-65535>** - Enter the dead packet interval used here. This value must be between 1 and 65535.

**authentication** - (Optional) Specifies the authentication type used.
- **none** - Specifies that the authentication type will be set to none.
- **simple** - Specifies that a simple text password will be used in the authentication.
  - **<password 8>** - Enter the simple text password value here. This value can be up to 8 characters long.
- **md5** - Specifies that an MD5 key ID will be used for the authentication.
  - **<key_id 1-255>** - Enter the MD5 key ID value used here. This value can be between 1 and 255.

### Restrictions

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

### Example

To configure the OSPF virtual link:

```
DGS-3620-28SC:admin# config ospf virtual_link 10.1.1.2 20.1.1.1 hello_interval
10
Command: config ospf virtual_link 10.1.1.2 20.1.1.1 hello_interval 10

Success.

DGS-3620-28SC:admin#
```

## 69-17 delete ospf virtual_link

### Description

This command is used to delete an OSPF virtual link.

### Format

**delete ospf virtual_link <area_id> <neighbor_id>**

### Parameters

**<area_id>** - Specifies a 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.

**<neighbor_id>** - Specifies the OSPF router ID for the remote area. This is a 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the remote area's Area Border Router. This is the router ID of the neighbor router.

### Restrictions

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

### Example

To delete an OSPF virtual link:

```
DGS-3620-28SC:admin# delete ospf virtual_link 10.1.1.12 20.1.1.1
Command: delete ospf virtual_link 10.1.1.12 20.1.1.1

Success.

DGS-3620-28SC:admin#
```

## 69-18 show ospf virtual_link

### Description

This command is used to display the current OSPF virtual interface configuration.

### Format

**show ospf virtual_link {<area_id> <neighbor_id>}**

### Parameters

**<area_id>** - (Optional) Specifies a 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.

**<neighbor_id>** - (Optional) The OSPF router ID for the remote area. This is a 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the remote area's Area Border Router. This is the router ID of the neighbor router.

If no parameter is specified, the system will display all current OSPF virtual interface configuration.

### Restrictions

None.

### Example

To display the current OSPF virtual interface configuration:

```
DGS-3620-28SC:admin#show ospf virtual_link
Command: show ospf virtual_link

Virtual Interface Configuration

Transit         Virtual         Hello    Dead     Authentication Link
Area ID         Neighbor Router Interval Interval                Status
--------------- --------------- -------- -------- -------------- ------
4.4.4.4         1.1.1.1         10       60       MD5            Up
4.4.4.4         6.6.6.6         10       250      Simple         Down

Total Entries : 2

DGS-3620-28SC:admin#
```

## 69-19 enable ospf

### Description

This command is used to enable OSPF on the switch.

### Format

**enable ospf**

### Parameters

None.

### Restrictions

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

### Example

To enable OSPF on the switch:

```
DGS-3620-28SC:admin# enable ospf
Command: enable ospf

Success.

DGS-3620-28SC:admin#
```

## 69-20 show ospf

### Description

This command is used to display the current OSPF settings on the switch.

## Format

**show ospf {[ipif <ipif_name 12> | all]}**

## Parameters

| |
|---|
| **ipif** - (Optional) Specifies the IP interface name.<br>**<ipif_name 12>** - Enter the IP interface name here. This name can be up to 12 characters long.<br>**all** - (Optional) Specifies that all the IP interfaces will be displayed. |
| If no parameter is specified, the system will display the current OSPF settings. |

## Restrictions

None.

## Example

To display the current OSPF state:

```
DGS-3620-28SC:admin# show ospf
Command: show ospf

OSPF Router ID : 10.90.90.90 (Auto selected)
State          : Enabled

OSPF Interface Settings

Interface    IP Address         Area ID         State    Link      Metric
                                                         Status
------------ ------------------ --------------- -------- --------- ---------
System       10.90.90.90/8      0.0.0.0         Disabled Link Down 1

Total Entries : 1

OSPF Area Settings

Area ID         Type   Stub Import Summary LSA Stub Default Cost Translate
--------------- ------ ----------------------- ----------------- ---------
0.0.0.0         Normal None                    None              None
10.0.0.0        Normal None                    None              None
10.0.0.1        NSSA   Enabled                 1                 Disabled
10.0.0.2        Stub   Enabled                 1                 None

Total Entries : 4

Virtual Interface Configuration

Transit         Virtual         Hello    Dead     Authentication Link
Area ID         Neighbor Router Interval Interval                Status
--------------- --------------- -------- -------- -------------- ------
10.0.0.0        10.0.0.1        10       60       None           Down
```

```

Total Entries : 1

OSPF Area Aggregation Settings

Area ID         Aggregated         LSDB     Advertise
                Network Address    Type
--------------- ------------------ -------- ---------
10.0.0.2        10.0.0.0/8         Summary  Enabled

Total Entries : 1

OSPF Host Route Settings

Host Address    Metric Area ID
--------------- ------ ---------------
10.90.91.90     1      0.0.0.0

Total Entries : 1

DGS-3620-28SC:admin#
```

## 69-21 disable ospf

### Description

This command is used to disable OSPF on the switch.

### Format

**disable ospf**

### Parameters

None.

### Restrictions

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

### Example

To disable OSPF on the switch:

```
DGS-3620-28SC:admin# disable ospf
Command: disable ospf

Success.

DGS-3620-28SC:admin#
```

## 69-22 show ospf lsdb

### Description

This command is used to display the OSPF Link State Database (LSDB).

### Format

**show ospf lsdb {area <area_id> | advertise_router <ipaddr> | type [rtrlink | netlink | summary | assummary | asextlink | nssa_ext | stub]}**

### Parameters

**area** - (Optional) Specifies a 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.
**<area_id>** - Enter the area ID used here.

**advertise_router** - (Optional) Specifies the IP address of the advertising router.
**<ipaddr>** - Enter the advertising router's IP address here.

**type** - (Optional) Specifies the type of link displayed.
**rtrlink** - Specifies the type to be displayed as router link.
**netlink** - Specifies the type to be displayed as network link.
**summary** - Specifies the type to be displayed as summary.
**assummary** - Specifies the type to be displayed as AS summary.
**asextlink** - Specifies the type to be displayed as AS external link.
**nssa_ext** - Specifies the type to be displayed as NSSA external information.
**stub** - Specifies the type to be displayed as STUB link.

### Restrictions

None.

### Example

To display the link state database of OSPF:

```
DGS-3620-28SC:admin# show ospf lsdb
Command: show ospf lsdb

Area ID           LSDB        Advertising  Link State    Cost  Sequence
                   Type        Router ID    ID                       Number
-------------  ----------  ------------  ------------  ----  ----------------
0.0.0.0          RTRLink     50.48.75.73   50.48.75.73   *     0x80000002
0.0.0.0          Summary     50.48.75.73   10.0.0.0/8    1     0x80000001
1.0.0.0          RTRLink     50.48.75.73   50.48.75.73   *     0x80000001
1.0.0.0          Summary     50.48.75.73   40.0.0.0/8    1     0x80000001
1.0.0.0          Summary     50.48.75.73   50.0.0.0/8    1     0x80000001
0.0.0.0          ASExtLink   50.48.75.73   1.2.0.0/16    20    0x80000001

Total Entries : 6

DGS-3620-28SC:admin#
```

## 69-23 show ospf neighbor

### Description

This command is used to display the OSPF-neighbor information on a per-interface basis.

### Format

**show ospf neighbor {<ipaddr>}**

### Parameters

**<ipaddr>** - (Optional) Specifies the IP address of the neighbor router.

If no parameter is specified, the system will display all OSPF neighbor information.

### Restrictions

None.

### Example

To display OSPF neighbor information:

```
DGS-3620-28SC:admin# show ospf neighbor
Command: show ospf neighbor

IP Address of   Router ID of    Neighbor Neighbor
Neighbor        Neighbor        Priority State
--------------- --------------- -------- -------------
10.48.74.122    10.2.2.2        1        Initial

Total Entries : 1

DGS-3620-28SC:admin#
```

## 69-24 show ospf virtual_neighbor

### Description

This command is used to display the OSPF-neighbor information of OSPF virtual links.

### Format

**show ospf virtual_neighbor {<area_id> <neighbor_id>}**

### Parameters

**<area_id>** - (Optional) Specifies a 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.

**<neighbor_id>** - (Optional) Specifies the OSPF router ID for the remote area. This is a 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the remote area's Area Border Router.

If no parameter is specified, the system will display all OSPF virtual-link neighbor information.

### Restrictions

None.

### Example

To display OSPF virtual-link neighbor information:

```
DGS-3620-28SC:admin# show ospf virtual_neighbor
Command: show ospf virtual_neighbor

Transit          Router ID of          IP Address of      Virtual Neighbor
Area ID          Virtual Neighbor     Virtual Neighbor        State
---------------  ----------------   ----------------  ----------------
10.1.1.1         10.2.3.4              10.48.74.111           Exchange

Total Entries : 1

DGS-3620-28SC:admin#
```

# Chapter 70 OSPFv3 Commands

**enable ospfv3**

**disable ospfv3**

**show ospfv3** {[ipif <ipif_name 12> | all]}

**config ospfv3 router_id** <ipaddr>

**create ospfv3 area** <area_id> type [normal | stub {stub_summary [enable | disable] | metric <value 0-65535>}]

**delete ospfv3 area** <area_id>

**config ospfv3 area** <area_id> type [normal | stub {stub_summary [enable | disable] | metric <value 0-65535>}]

**show ospfv3 area** {<area_id>}

**create ospfv3 aggregation** <area_id> <ipv6networkaddr> advertise [enable | disable]

**delete ospfv3 aggregation** <area_id> <ipv6networkaddr>

**config ospfv3 aggregation** <area_id> <ipv6networkaddr> advertise [enable | disable]

**show ospfv3 aggregation** {<area_id>}

**show ospfv3 lsdb** {area <area_id> | type [rtrlink | netlink | inter_area_prefix | inter_area_router | asextlink | link_lsa | intra_area_prefix]}

**show ospfv3 neighbor** {<neighbor_id> ipif <ipif_name 12>}

**show ospfv3 virtual_neighbor** {<area_id> <neighbor_id>}

**config ospfv3** [ipif <ipif_name 12> | all] {area <area_id> | priority <value 0-255> | hello_interval <sec 1-65535> | dead_interval <sec 1-65535> | instance <value 0-255> | metric <value 1-65535>| state [enable | disable] | passive [enable | disable]} (1)

**create ospfv3 virtual_link** <area_id> <neighbor_id> {hello_interval <sec 1-65535> | dead_interval <sec 1-65535> | instance <value 0-255>}

**config ospfv3 virtual_link** <area_id> <neighbor_id> {hello_interval <sec 1-65535> | dead_interval <sec 1-65535> | instance <value 0-255>} (1)

**delete ospfv3 virtual_link** <area_id> <neighbor_id>

**show ospfv3 virtual_link** {<area_id> <neighbor_id>}

## 70-1 enable ospfv3

### Description

This command is used to enable OSPFv3 on the Switch.

### Format

**enable ospfv3**

### Parameters

None.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

To enable OSPFv3:

```
DGS-3620-28SC:admin# enable ospfv3
Command: enable ospfv3

Success.

DGS-3620-28SC:admin#
```

## 70-2 disable ospfv3

### Description

This command is used to disable OSPFv3 on the Switch.

### Format

**disable ospfv3**

### Parameters

None.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

To disable OSPFv3:

```
DGS-3620-28SC:admin# disable ospfv3
Command: disable ospfv3

Success.

DGS-3620-28SC:admin#
```

## 70-3 show ospfv3

### Description

This command is used to display the OSPFv3 configurations or OSPFv3 interfaces information.

### Format

**show ospfv3 {[ipif <ipif_name 12> | all]}**

## Parameters

**ipif** - (Optional) Specifies the OSPFv3 IP interface name used.
  **<ipif_name 12>** - Enter the OSPFv3 IP interface name used here. This name can be up to 12 characters long.
  **all** - (Optional) Specifies that all the OSPFv3 IP interfaces will be used.

## Restrictions

None. (EI Mode Only Command)

## Example

To display OSPFv3 configurations or interfaces information:

```
DGS-3620-28SC:admin# show ospfv3
Command: show ospfv3

OSPFv3 Router ID: 1.1.1.1
State           : Enabled

OSPFv3 Interface Settings

Interface    Area ID         State    Link      Metric    Instance ID
                                      Status
------------ --------------- -------- --------- --------- -----------
System       0.0.0.0         Disabled Link Up   10        0


Total Entries: 1

OSPFv3 Area Settings

Area ID         Type   Stub Import Summary LSA Stub Default Cost
--------------- ------ ----------------------- -----------------
0.0.0.0         Normal None                    None

Total Entries: 1

Virtual Interface Configuration

Transit         Virtual         Hello    Dead     Instance ID Link
Area ID         Neighbor Router Interval Interval             Status
--------------- --------------- -------- -------- ----------- ------

Total Entries: 0

OSPFv3 Area Aggregation Settings

Area ID         Aggregated                                  LSDB     Advertise
                Network Address                             Type
--------------- ------------------------------------------- -------- ---------

```

```
Total Entries: 0

DGS-3620-28SC:admin# show ospfv3 all
Command: show ospfv3 all

Interface Name: System                  Link Local Address:
FE80::201:2FF:FE03:400 (Link Up)
Network Medium Type: BROADCAST          Metric: 10
Area ID: 0.0.0.0                        Administrative State: Disabled
Priority: 1                             DR State: DOWN
DR ID: None                             Backup DR ID: None
Hello Interval: 10                      Dead Interval: 40
Transmit Delay: 1                       Retransmit Time: 5
Passive Mode: Disabled                  Instance ID: 0

Total Entries: 1

DGS-3620-28SC:admin# show ospfv3 ipif System
Command: show ospfv3 ipif System

Interface Name: System                  Link Local Address:
FE80::201:2FF:FE03:400 (Link Up)
Network Medium Type: BROADCAST          Metric: 10
Area ID: 0.0.0.0                        Administrative State: Disabled
Priority: 1                             DR State: DOWN
DR ID: None                             Backup DR ID: None
Hello Interval: 10                      Dead Interval: 40
Transmit Delay: 1                       Retransmit Time: 5
Passive Mode: Disabled                  Instance ID: 0

Total Entries: 1

DGS-3620-28SC:admin#
```

## 70-4 config ospfv3 router_id

### Description

This command is used to configure the OSPFv3 router ID.

### Format

**config ospfv3 router_id <ipaddr>**

### Parameters

**<ipaddr>** - Specifies that the user may enter a 32-bit number in the form of an IPv4 address that uniquely identifies the router in the OSPFv3 domain. Setting it to be 0.0.0.0 means auto-selected. The Switch will select the largest IPv4 address among the IP interfaces to be the router ID. The default for the OSPFv3 router ID is 0.0.0.0 (auto-selected). Only by executing this command, can the OSPFv3 router ID be changed.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

To set OSPFv3 router ID:

```
DGS-3620-28SC:admin# config ospfv3 router_id 1.1.1.1
Command: config ospfv3 router_id 1.1.1.1

Success.

DGS-3620-28SC:admin#
```

## 70-5 create ospfv3 area

### Description

This command is used to create an OSPFv3 area.

### Format

**create ospfv3 area <area_id> type [normal | stub {stub_summary [enable | disable] | metric <value 0-65535>}]**

### Parameters

**<area_id>** - Specifies the OSPFv3 area's ID. It is a 32-bit number in the form of an IPv4 address that uniquely identifies the OSPFv3 area in the OSPFv3 domain.

**type** - Specifies the OSPFv3 area mode of operation. There are two types:
- **normal** - Specifies that the OSPFv3 area will be created as a normal area.
- **stub** - Specifies that the OSPFv3 area will be created as a stub area.
  - **stub_summary** - (Optional) Specifies the OSPFv3 stub area to import inter-area prefix LSA advertisements or not.
    - **enable** - Import inter-area prefix LSA into this stub area.
    - **disable** - Do not import inter-area prefix LSA into this stub area.
  - **metric** - (Optional) Specifies the default cost of OSPFv3 stub area.
    - **<value 0-65535>** - Enter the metric value used here. This value must be between 0 and 65535. The default value is 1.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

To create OSPFv3 areas:

```
DGS-3620-28SC:admin# create ospfv3 area 1.1.1.1 type normal
Command: create ospfv3 area 1.1.1.1 type normal

Success.

DGS-3620-28SC:admin# create ospfv3 area 2.2.2.2 type stub stub_summary enable
Command: create ospfv3 area 2.2.2.2 type stub stub_summary enable

Success.

DGS-3620-28SC:admin#
```

## 70-6 delete ospfv3 area

### Description

This command is used to delete an OSPFv3 area. The backbone area (0.0.0.0) can not be deleted.

### Format

**delete ospfv3 area <area_id>**

### Parameters

**<area_id>** - Enter the OSPFv3 area's ID here. It is a 32-bit number in the form of an IPv4 address that uniquely identifies the OSPFv3 area in the OSPFv3 domain.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

To delete an OSPFv3 area:

```
DGS-3620-28SC:admin# delete ospfv3 area 1.1.1.1
Command: delete ospfv3 area 1.1.1.1

Success.

DGS-3620-28SC:admin#
```

## 70-7 config ospfv3 area

### Description

This command is used to configure an OSPFv3 area. The backbone area (0.0.0.0) can not be configured to be stub area.

### Format

**config ospfv3 area <area_id> type [normal | stub {stub_summary [enable | disable] | metric <value 0-65535>}]**

### Parameters

**<area_id>** - Specifies the OSPFv3 area's ID. It is a 32-bit number in the form of an IPv4 address that uniquely identifies the OSPFv3 area in the OSPFv3 domain.

**type** - Specifies the OSPFv3 area mode of operation. There are two types:
- **normal** - Specifies that the OSPFv3 area will be configured as a normal area.
- **stub** - Specifies that the OSPFv3 area will be configured as a stub area.
  - **stub_summary** - (Optional) Specifies the OSPFv3 stub area to import inter-area prefix LSA advertisements or not.
    - **enable** - Import inter-area prefix LSA into this stub area.
    - **disable** - Do not import inter-area prefix LSA into this stub area.
  - **metric** - (Optional) Specifies the default cost of OSPFv3 stub area.
    - **<value 0-65535>** - Enter the metric value used here. This value must be between 0 and 65535. The default value is 1.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

To configure an OSPFv3 area:

```
DGS-3620-28SC:admin# config ospfv3 area 2.2.2.2 type normal
Command: config ospfv3 area 2.2.2.2 type normal

Success.

DGS-3620-28SC:admin#
```

## 70-8 show ospfv3 area

### Description

This command is used to display OSPFv3 area configurations or information.

### Format

**show ospfv3 area {<area_id>}**

### Parameters

**<area_id>** - (Optional) Specifies the OSPFv3 area's ID. It is a 32-bit number in the form of an IPv4 address that uniquely identifies the OSPFv3 area in the OSPFv3 domain.

### Restrictions

None. (EI Mode Only Command)

### Example

To display OSPFv3 areas:

```
DGS-3620-28SC:admin# show ospfv3 area
Command: show ospfv3 area

OSPFv3 Area Settings

Area ID         Type   Stub Import Summary LSA Stub Default Cost
--------------- ------ ----------------------- -----------------
0.0.0.0         Normal None                    None
2.2.2.2         Normal None                    None

Total Entries: 2

DGS-3620-28SC:admin# show ospfv3 area 0.0.0.0
Command: show ospfv3 area 0.0.0.0

Area ID: 0.0.0.0                        Area Type: Normal

SPF Algorithm Runs For Area 0.0.0.0: 1 time
Number Of LSA In This Area: 2           Checksum Sum: 0x0
Number Of ABR In This Area: 0           Number Of ASBR In This Area: 0

Total Entries: 1


DGS-3620-28SC:admin#
```

## 70-9 create ospfv3 aggregation

### Description

This command is used to create an OSPFv3 area aggregation.

### Format

**create ospfv3 aggregation <area_id> <ipv6networkaddr> advertise [enable | disable]**

### Parameters

**<area_id>** - Specifies the OSPFv3 area's ID. It is a 32-bit number in the form of an IPv4 address that uniquely identifies the OSPFv3 area in the OSPFv3 domain.

**<ipv6networkaddr>** - Specifies the IPv6 network address of the aggregation.

**advertise** - Specifies whether the OSPFv3 ABR will use this aggregation to aggregate the intra-area routes or not.

**enable** - Specifies that the OSPFv3 ABR will use this aggregation to aggregate the intra-area routes when it advertises these routes to another area.

**disable** - Specifies that the OSPFv3 ABR will not use this aggregation to aggregate the intra-area routes when it advertises these routes to another area.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

To create an OSPFv3 area aggregation:

```
DGS-3620-28SC:admin# create ospfv3 aggregation 2.2.2.2 2000::/16 advertise
enable
Command: create ospfv3 aggregation 2.2.2.2 2000::/16 advertise enable

Success.

DGS-3620-28SC:admin#
```

## 70-10 delete ospfv3 aggregation

### Description

This command is used to delete an OSPFv3 area aggregation.

### Format

**delete ospfv3 aggregation <area_id> <ipv6networkaddr>**

### Parameters

**<area_id>** - Specifies the OSPFv3 area's ID. It is a 32-bit number in the form of an IPv4 address that uniquely identifies the OSPFv3 area in the OSPFv3 domain.

**<ipv6networkaddr>** - Specifies the IPv6 network address of the aggregation.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

To delete an OSPFv3 area aggregation:

```
DGS-3620-28SC:admin# delete ospfv3 aggregation 2.2.2.2 2000::/16
Command: delete ospfv3 aggregation 2.2.2.2 2000::/16

Success.

DGS-3620-28SC:admin#
```

## 70-11 config ospfv3 aggregation

### Description

This command is used to configure an OSPFv3 area aggregation.

### Format

**config ospfv3 aggregation <area_id> <ipv6networkaddr> advertise [enable | disable]**

### Parameters

**<area_id>** - Specifies the OSPFv3 area's ID. It is a 32-bit number in the form of an IPv4 address that uniquely identifies the OSPFv3 area in the OSPFv3 domain.

**<ipv6networkaddr>** - Specifies the IPv6 network address of the aggregation.

**advertise** - Specifies whether the OSPFv3 ABR will use this aggregation to aggregate the intra-area routes or not.

**enable** - Specifies that the OSPFv3 ABR will use this aggregation to aggregate the intra-area routes when it advertises these routes to another area.

**disable** - Specifies that the OSPFv3 ABR will not use this aggregation to aggregate the intra-area routes when it advertises these routes to another area.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

To configure an OSPFv3 area aggregation:

```
DGS-3620-28SC:admin# config ospfv3 aggregation 2.2.2.2 2000::/16 advertise
disable
Command: config ospfv3 aggregation 2.2.2.2 2000::/16 advertise disable

Success.

DGS-3620-28SC:admin#
```

## 70-12 show ospfv3 aggregation

### Description

This command is used to display OSPFv3 area aggregation configurations.

### Format

**show ospfv3 aggregation {<area_id>}**

### Parameters

**<area_id>** - (Optional) Specifies the OSPFv3 area's ID. It is a 32-bit number in the form of an IPv4 address that uniquely identifies the OSPFv3 area in the OSPFv3 domain.

### Restrictions

None. (EI Mode Only Command)

### Example

To display OSPFv3 area aggregations:

```
DGS-3620-28SC:admin# show ospfv3 aggregation
Command: show ospfv3 aggregation

OSPFv3 Area Aggregation Settings

Area ID         Aggregated                                  LSDB     Advertise
                Network Address                             Type
--------------- ------------------------------------------- -------- ---------
1.1.1.1         1000::/16                                   Summary  Disabled
2.2.2.2         2000::/16                                   Summary  Disabled

Total Entries: 2

DGS-3620-28SC:admin# show ospfv3 aggregation 2.2.2.2
Command: show ospfv3 aggregation 2.2.2.2

OSPFv3 Area Aggregation Settings

Area ID         Aggregated                                  LSDB     Advertise
                Network Address                             Type
--------------- ------------------------------------------- -------- ---------
2.2.2.2         2000::/16                                   Summary  Disabled

Total Entries: 1

DGS-3620-28SC:admin#
```

## 70-13 show ospfv3 lsdb

### Description

This command is used to display OSPFv3 Link-State Database.

### Format

**show ospfv3 lsdb {area <area_id> | type [rtrlink | netlink | inter_area_prefix | inter_area_router | asextlink | link_lsa | intra_area_prefix]}**

### Parameters

**area** - (Optional) Specifies that only the LSAs that belong to this area will be displayed.
**<area_id>** - Enter the area ID used here.

**type** - (Optional) Specifies that only this type of LSAs will be displayed and detail information for these LSAs will be displayed at the same time.
**rtrlink** - Specifies that the Router LSA will be displayed.
**netlink** - Specifies that the Network LSA will be displayed.
**inter_area_prefix** - Specifies that the Inter-Area-Prefix LSA will be displayed.
**inter_area_router** - Specifies that the Inter-Area-Router LSA will be displayed.
**asextlink** - Specifies that the AS external LSA will be displayed.
**link_lsa** - Specifies that the Link LSA will be displayed.

**intra_area_prefix** - Specifies that the Intra-Area-Prefix LSA will be displayed.

### Restrictions

None. (EI Mode Only Command)

### Example

To display OSPFv3 Link-State Database:

```
DGS-3620-28SC:admin# show ospfv3 lsdb
Command: show ospfv3 lsdb

                Router LSA (Area 0.0.0.0)
Link State ID   ADV Router      Age  Seq#        Link
0.0.0.0         2.2.2.2         696  0x80000003  0

                Link LSA (Interface System)
Link State ID   ADV Router      Age  Seq#        Prefix
0.0.0.1         2.2.2.2         696  0x80000003  1

                Intra-Area-Prefix LSA (Area 0.0.0.0)
Link State ID   ADV Router      Age  Seq#        Ref LSA Type
0.0.0.1         2.2.2.2         684  0x80000004  0x2001

Total Entries: 3

DGS-3620-28SC:admin# show ospfv3 lsdb type rtrlink
Command: show ospfv3 lsdb type rtrlink

  LS Age: 782
  LS Type: Router-LSA
  Link State ID: 0.0.0.0
  Advertising Router: 2.2.2.2
  LS Seq Number: 0x80000003
  Checksum: 0xED3A
  Length: 24
  Flags: 0x0: - - - -
  Options: 0x13: - R - - E V6

Total Entries: 1

DGS-3620-28SC:admin#
```

## 70-14 show ospfv3 neighbor

### Description

This command is used to display OSPFv3 neighbor information.

### Format

**show ospfv3 neighbor {<neighbor_id> ipif <ipif_name 12>}**

### Parameters

**<neighbor_id>** - (Optional) Specifies the ID of the neighbor.

**ipif** - (Optional) Specifies the IP interface where the neighbor is built.
    **<ipif_name 12>** - Enter the IP interface name used here. This name can be up to 12 characters long.

### Restrictions

None. (EI Mode Only Command)

### Example

To display OSPFv3 neighbor:

```
DGS-3620-28SC:admin# show ospfv3 neighbor
Command: show ospfv3 neighbor

Router ID of    Interface    Neighbor Neighbor
Neighbor        Name         Priority State
--------------- ------------ -------- -------------
10.10.10.10     System       1        Full
20.20.20.20     ip1          10       Full

Total Entries: 2

DGS-3620-28SC:admin# show ospfv3 neighbor 10.10.10.10 ipif System
Command: show ospfv3 neighbor 10.10.10.10 ipif System

Neighbor ID: 10.10.10.10                Interface Name: System
Neighbor Options: 19                    Neighbor Priority: 255
Neighbor State: Full                    State Changes: 6 times
Interface ID: 1

DGS-3620-28SC:admin#
```

## 70-15 show ospfv3 virtual_neighbor

### Description

This command is used to display OSPFv3 virtual neighbor information.

### Format

**show ospfv3 virtual_neighbor {<area_id> <neighbor_id>}**

### Parameters

**<area_id>** - (Optional) Specifies the transit area where the virtual neighbor is built.

**<neighbor_id>** - (Optional) Specifies the ID of the virtual neighbor. If none of the parameters are set, all the virtual neighbors will be displayed.

### Restrictions

None. (EI Mode Only Command)

### Example

To display OSPFv3 virtual neighbor:

```
DGS-3620-28SC:admin# show ospfv3 virtual_neighbor
Command: show ospfv3 virtual_neighbor

Transit         Router ID Of     Virtual Neighbor
Area ID         Virtual Neighbor State
--------------- ---------------- ----------------
1.1.1.1         30.30.30.30      Full

Total Entries: 1

DGS-3620-28SC:admin# show ospfv3 virtual_neighbor 6.6.6.6 20.20.20.20
Command: show ospfv3 virtual_neighbor 6.6.6.6 20.20.20.20

Transit Area ID: 6.6.6.6
Virtual Neighbor ID: 20.20.20.20
Virtual Neighbor Options: 19
Virtual Neighbor State: Full            State Changes: 9 times

Total Entries: 1

DGS-3620-28SC:admin#
```

## 70-16 config ospfv3

### Description

This command is used to configure an OSPFv3 interface.

### Format

**config ospfv3 [ipif <ipif_name 12> | all] {area <area_id> | priority <value 0-255> | hello_interval <sec 1-65535> | dead_interval <sec 1-65535> | instance <value 0-255> | metric <value 1-65535>| state [enable | disable] | passive [enable | disable]} (1)**

### Parameters

**ipif** - Specifies the OSPFv3 IP interface name used.
**<ipif_name 12>** - Enter the OSPFv3 IP interface name used here. This name can be up to 12 characters long.
**all** - Specifies that all the OSPFv3 IP interfaces will be used.

**area** - (Optional) Specifies a 32-bit number in the form of an IPv4 address that uniquely identifies the OSPFv3 area in the OSPFv3 domain.
**<area_id>** - Enter the area ID used here.

**priority** - (Optional) Specifies the priority used in the election of the Designated Router (DR).
**<value 0-255>** - Enter the priority value used here. This value must be between 0 and 255. The default value is 1.

**hello_interval** - (Optional) Specifies to allow the specification of the interval between the transmission of OSPFv3 Hello packets, in seconds. The Hello Interval and Dead Interval should be the same for all routers on the same link.

**<sec 1-65535>** - Enter the hello interval value here. This value must be between 1 and 65535 seconds. The default value is 10 seconds.

**dead_interval** - (Optional) Specifies to allow the specification of the length of time between the receipt of Hello packets from a neighbor router before the selected area declares that router down. The Dead Interval must be evenly divisible by the Hello Interval.

**<sec 1-65535>** - Enter the dead interval value used here. This value must be between 1 and 65535 seconds. The default value is 40 seconds.

**instance** - (Optional) Specifies the instance ID of the interface.

**<value 0-255>** - Enter the instance ID used here. This value must be between 0 and 255. The default value is 0.

**metric** - (Optional) Specifies the field that allows the entry that is the representative of the OSPFv3 cost of reaching the selected OSPFv3 interface.

**<value 1-65535>** - Enter the metric value used here. This value must be between 1 and 65535. The default value is 10.

**state** - (Optional) Specifies to enable or disable this interface to run OSPFv3.

**enable** - Specifies that the OSPFv3 state, for this interface, will be enabled.

**disable** - Specifies that the OSPFv3 state, for this interface, will be disabled.

**passive** - (Optional) Specifies that the user may select Active or Passive for this OSPFv3 interface. Active interfaces actively advertise OSPFv3 to routers on other Intranets that are not part of this specific OSPFv3 group. Passive interfaces will not advertise to any other routers than those within its OSPFv3 intranet. When this field is disabled, it denotes an active interface.

**enable** - Specifies that the passive state will be enabled.

**disable** - Specifies that the passive state will be disabled.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

To configure an OSPFv3 interface:

```
DGS-3620-28SC:admin# config ospfv3 ipif System area 0.0.0.0 priority 100
hello_interval 20 dead_interval 60 instance 1 metric 20 state enable passive
disable
Command: config ospfv3 ipif System area 0.0.0.0 priority 100 hello_interval 20
dead_interval 60 instance 1 metric 20 state enable passive disable


Success.


DGS-3620-28SC:admin#
```

## 70-17 create ospfv3 virtual_link

### Description

This command is used to create an OSPFv3 virtual link.

### Format

**create ospfv3 virtual_link <area_id> <neighbor_id> {hello_interval <sec 1-65535> | dead_interval <sec 1-65535> | instance <value 0-255>}**

## Parameters

**<area_id>** - Specifies a 32-bit number in the form of an IPv4 address that uniquely identifies the OSPFv3 area in the OSPFv3 domain. This area is the transit area where the virtual link is built.

**<neighbor_id>** - Specifies a 32-bit number in the form of an IPv4 address that uniquely identifies the OSPFv3 virtual neighbor in the OSPFv3 domain.

**hello_interval** - (Optional) Specifies to allow the specification of the interval between the transmission of OSPFv3 Hello packets. The Hello Interval and Dead Interval should be the same for all routers on the same link.

- **<sec 1-65535>** - Enter the hello interval value used here. This value must be between 1 and 65535 seconds. The default value is 10 seconds.

**dead_interval** - (Optional) Specifies to allow the specification of the length of time between the receipt of Hello packets from a neighbor router before the selected area declares that router down. The Dead Interval must be evenly divisible by the Hello Interval.

- **<sec 1-65535>** - Enter the dead interval value used here. This value must be between 1 and 65535 seconds. The default value is 60 seconds.

**instance** - (Optional) Specifies the instance ID on the virtual link.

- **<value 0-255>** - Enter the instance ID value here. This value must be between 0 and 255. The default value is 0.

## Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

## Example

To create OSPFv3 virtual link:

```
DGS-3620-28SC:admin# create ospfv3 virtual_link 1.1.1.1 60.60.60.60
Command: create ospfv3 virtual_link 1.1.1.1 60.60.60.60

Success.

DGS-3620-28SC:admin#
```

# 70-18 config ospfv3 virtual_link

## Description

This command is used to configure an OSPFv3 virtual link.

## Format

**config ospfv3 virtual_link <area_id> <neighbor_id> {hello_interval <sec 1-65535> | dead_interval <sec 1-65535> | instance <value 0-255>} (1)**

## Parameters

**<area_id>** - Specifies a 32-bit number in the form of an IPv4 address that uniquely identifies the OSPFv3 area in the OSPFv3 domain. This area is the transit area where the virtual link is built.

**<neighbor_id>** - Specifies a 32-bit number in the form of an IPv4 address that uniquely identifies the OSPFv3 virtual neighbor in the OSPFv3 domain.

**hello_interval** - (Optional) Specifies to allow the specification of the interval between the transmission of OSPFv3 Hello packets. The Hello Interval and Dead Interval should be the same for all routers on the same link.

**<sec 1-65535>** - Enter the hello interval value used here. This value must be between 1 and 65535 seconds. The default value is 10 seconds.

**dead_interval** - (Optional) Specifies to allow the specification of the length of time between the receipt of Hello packets from a neighbor router before the selected area declares that router down. The Dead Interval must be evenly divisible by the Hello Interval.

**<sec 1-65535>** - Enter the dead interval value used here. This value must be between 1 and 65535 seconds. The default value is 60 seconds.

**instance** - (Optional) Specifies the instance ID on the virtual link.

**<value 0-255>** - Enter the instance ID value here. This value must be between 0 and 255. The default value is 0.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

To configure an OSPFv3 virtual link:

```
DGS-3620-28SC:admin# config ospfv3 virtual_link 1.1.1.1 60.60.60.60
hello_interval 20 dead_interval 80 instance 1
Command: config ospfv3 virtual_link 1.1.1.1 60.60.60.60 hello_interval 20
dead_interval 80 instance 1


Success.


DGS-3620-28SC:admin#
```

## 70-19 delete ospfv3 virtual_link

### Description

This command is used to delete an OSPFv3 virtual link.

### Format

**delete ospfv3 virtual_link <area_id> <neighbor_id>**

### Parameters

**<area_id>** - Specifies a 32-bit number in the form of an IPv4 address that uniquely identifies the OSPFv3 area in the OSPFv3 domain. This area is the transit area where the virtual link is built.

**<neighbor_id>** - Specifies a 32-bit number in the form of an IPv4 address that uniquely identifies the OSPFv3 virtual neighbor in the OSPFv3 domain.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

To delete an OSPFv3 virtual link:

```
DGS-3620-28SC:admin# delete ospfv3 virtual_link 1.1.1.1 60.60.60.60
Command: delete ospfv3 virtual_link 1.1.1.1 60.60.60.60

Success.

DGS-3620-28SC:admin#
```

## 70-20 show ospfv3 virtual_link

### Description

This command is used to display OSPFv3 virtual link configurations. If no parameters are set, all the virtual links will be displayed.

### Format

**show ospfv3 virtual_link {<area_id> <neighbor_id>}**

### Parameters

**<area_id>** - (Optional) Specifies a 32-bit number in the form of an IPv4 address that uniquely identifies the OSPFv3 area in the OSPFv3 domain. This area is the transit area where the virtual link is built.

**<neighbor_id>** - (Optional) Specifies a 32-bit number in the form of an IPv4 address that uniquely identifies the OSPFv3 virtual neighbor in the OSPFv3 domain.

### Restrictions

None. (EI Mode Only Command)

### Example

To display an OSPFv3 virtual link:

```
DGS-3620-28SC:admin# show ospfv3 virtual_link
Command: show ospfv3 virtual_link

Virtual Interface Configuration

Transit         Virtual         Hello    Dead     Instance ID Link
Area ID         Neighbor Router Interval Interval             Status
--------------- --------------- -------- -------- ----------- ------
1.1.1.1         60.60.60.60     10       60       0           DOWN
1.1.1.1         70.70.70.70     10       60       0           DOWN

Total Entries: 2

DGS-3620-28SC:admin# show ospfv3 virtual_link 1.1.1.1 60.60.60.60
```

```
Command: show ospfv3 virtual_link 1.1.1.1 60.60.60.60

Transit Area ID: 1.1.1.1           Virtual Neighbor Router ID: 60.60.60.60
Hello Interval: 10                 Dead Interval: 60
Transmit Delay: 1                  Retransmit Time: 5
Instance ID: 0
Virtual Link Status: DOWN

Total Entries: 1

DGS-3620-28SC:admin#
```

# Chapter 71 Packet Storm Commands

| |
|---|
| **config traffic control** [<portlist> \| all] {broadcast [enable \| disable] \| multicast [enable \| disable] \| unicast [enable \| disable] \| action [drop \| shutdown] \| threshold <value 0-255000> \| countdown [<min 0> \| <min 3-30> \| disable] \| time_interval <sec 5-600>}(1) |
| **config traffic control auto_recover_time** [<min 0> \| <min 1-65535>] |
| **config traffic control log state** [enable \| disable] |
| **config traffic trap** [none \| storm_occurred \| storm_cleared \| both] |
| **show traffic control** {<portlist>} |

## 71-1 config traffic control

### Description

This command is used to configure broadcast/multicast/unicast storm control. The broadcast storm control commands provide a hardware storm control mechanism only. These packet storm control commands include hardware and software mechanisms to provide shutdown, recovery, and trap notification functions.

### Format

**config traffic control [<portlist> | all] {broadcast [enable | disable] | multicast [enable | disable] | unicast [enable | disable] | action [drop | shutdown] | threshold <value 0-255000> | countdown [<min 0> | <min 3-30> | disable] | time_interval <sec 5-600>}(1)**

### Parameters

| |
|---|
| **<portlist>** - Specify a range of ports to be configured. |
| **all** - Specify all ports are to be configured. |
| **broadcast** - Specify the broadcast storm status.<br>**enable** - Enable broadcast storm control.<br>**disable** - Disable broadcast storm control. |
| **multicast** - Specify the multicast storm status.<br>**enable** - Enable multicast storm control.<br>**disable** - Disable multicast storm control. |
| **unicast** - Specify the unknown unicast packet storm status.<br>**enable** - Enable unknown unicast packet storm control (only support drop action).<br>**disable** - Disable unknown unicast packet storm control. |
| **action** - Specify the action.<br>**drop** - This is implemented in hardware.<br>**shutdown** - This is implemented in software. If this is chosen, threshold, countdown, and time_interval also need to be configured. |
| **threshold** - The upper threshold at which the specified storm control will turn on.<br>This is the number of broadcast/multicast/unknown unicast packets per second received by the switch that will trigger the storm traffic control measure. It must be an unsigned integer.<br>**<value 0-255000>** - Specify the value between 0 and 255000. |
| **countdown** - The timer for shutdown mode. When a port enters a shutdown RX state, and if this times out, the port will shut down the port forever. The default is 0 minutes.<br>**<min 0>** - Zero is the disable forever state. |

**<min 3-30>** - Enter a value between 3 and 30 minutes.
**disable** – Specifies that when the action is shutdown and the countdown is disabled, when the Switch detects a storm, it will shutdown the port directly.

**time_interval** - The sampling interval of received packet counts. This parameter is meaningless for dropping packets is selected as action.
**<value 5-600>** - Specify the value between 5 and 600.

### Restrictions

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

### Example

To configure traffic control and state:

```
DGS-3620-28SC:admin#config traffic control 1-10 broadcast enable action
shutdown threshold 640 time_interval 10
Command: config traffic control 1-10 broadcast enable action shutdown threshold
640 time_interval 10

Success.

DGS-3620-28SC:admin#
```

## 71-2 config traffic control auto_recover_time

### Description

This command is used to configure the traffic auto recover time that allowed for a port to recover from shutdown forever status. The time allowed for auto recovery from shutdown for a port. The default value is 0, so no auto recovery is possible; the port remains in shutdown forever mode. This requires manual entry of the CLI command “**config ports [ <portlist> | all ] state enable**" to return the port to a forwarding state. The default value is 0, which means disable auto recover mode, shutdown forever.

### Format

**config traffic control auto_recover_time [<min 0> | <min 1-65535>]**

### Parameters

**<min 0>** - Enter the automatic recovery time used here. This value will specifies the time to be 0 otherwise known as 'no recovery mode'.
**<min 1-65535>** - Enter the automatic recovery time used here. This value must be between 1 and 65535 minutes.

### Restrictions

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

### Example

To configure the auto recover time to 5 minutes:

```
DGS-3620-28SC:admin# config traffic control auto_recover_time 5
Command: config traffic control auto_recover_time 5

Success.

DGS-3620-28SC:admin#
```

## 71-3 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.

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

**state** - Specifies the traffic control log state.
**enable** - Specifies that traffic control state will be logged when a storm occurs.
**disable** - Specifies that the traffic control state will be disabled.

### Restrictions

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

### Example

To configure the traffic log state on the Switch:

```
DGS-3620-28SC:admin# config traffic control log state enable
Command: config traffic control log state enable

Success.

DGS-3620-28SC:admin#
```

## 71-4 config traffic trap

### Description

This command is used to configure whether storm control notification will be generated or not while traffic storm events are detected by a SW traffic storm control mechanism.

**Note:** A traffic control trap is active only when the control action is configured as shutdown. If the control action is drop there will no traps issue while storm event is detected.

### Format

**config traffic trap [none | storm_occurred | storm_cleared | both]**

### Parameters

**none** - No notification will be generated when storm event is detected or cleared.

**storm_occurred** - A notification will be generated when a storm event is detected.

**storm_cleared** - A notification will be generated when a storm event is cleared.

**both** - A notification will be generated both when a storm event is detected and cleared.

### Restrictions

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

### Example

To configure a traffic control trap:

```
DGS-3620-28SC:admin#config traffic trap both
Command: config traffic trap both

Success.

DGS-3620-28SC:admin#
```

## 71-5 show traffic control

### Description

This command is used to display current traffic control settings.

### Format

**show traffic control {<portlist>}**

### Parameters

**<portlist>** - (Optional) Specify a range of ports to be shown.

**Note:** If no parameter is specified, the system will display all port packet storm control configurations.

### Restrictions

None.

## Example

To display the packet storm control setting for ports 1 to 3:

```
DGS-3620-28SC:admin#show traffic control 1-3
Command: show traffic control 1-3

Traffic Control Trap             : [None]
Traffic Control Log              : Enabled
Traffic Control Auto Recover Time: 0 Minutes

Port Thres  Broadcast Multicast Unicast  Action   Count    Time     Shutdown
     hold   Storm     Storm     Storm             down     Interval Forever
---- ------ --------- --------- -------- -------- -------- -------- --------
1    640    Enabled   Disabled  Disabled shutdown 0        10
2    640    Enabled   Disabled  Disabled shutdown 0        10
3    640    Enabled   Disabled  Disabled shutdown 0        10

DGS-3620-28SC:admin#
```

# Chapter 72 Password Recovery Commands

| |
|---|
| **enable password_recovery** |
| **disable password_recovery** |
| **show password_recovery** |

## 72-1 enable password_recovery

### Description

This command is used to enable the password recovery mode.

**Note:** The configuration does not take effect until saved.

### Format

**enable password_recovery**

### Parameters

None.

### Restrictions

Only Administrator-level users can issue this command.

### Example

To enable the password recovery mode:

```
DGS-3620-28SC:admin# enable password_recovery
Command: enable password_recovery

Success.

DGS-3620-28SC:admin#
```

## 72-2 disable password_recovery

### Description

This command is used to disable the password recovery mode.

**Note:** The configuration does not take effect until saved.

### Format

**disable password_recovery**

### Parameters

None.

### Restrictions

Only Administrator-level users can issue this command.

### Example

To disable the password recovery mode:

```
DGS-3620-28SC:admin# disable password_recovery
Command: disable password_recovery

Success.

DGS-3620-28SC:admin#
```

## 72-3 show password_recovery

### Description

The command is used to display the password recovery state. The displayed content includes both the running configuration and the NV-RAM configuration.

When the password recovery state is enabled a user can reboot the switch and enter into the Password Recovery mode. Otherwise, if the Password Recovery state is disabled a user will not be able to enter into the special recovery mode.

**Note:** Only the NV-RAM configuration will take effect when the switch restarts next time, the running configuration does not take effect until saved. That means the password recovery is determined by the state stored in the NV-RAM and take effect at the next time switch start up. The Running Configuration is the current configured state of the password recovery, it will lost without save, or become the NV-RAM configuration if save the configurations.

### Format

**show password_recovery**

### Parameters

None.

### Restrictions

Only Administrator-level users can issue this command.

### Example

To display the password recovery state:

```
DGS-3620-28SC:admin# show password_recovery
Command: show password_recovery

 Running Configuration     : Disabled
 NV-RAM Configuration      : Enabled

DGS-3620-28SC:admin#
```

# Chapter 73 Protocol Independent Multicast (PIM) Commands

| |
|---|
| **config pim** [[ipif <ipif_name 12> \| all] {hello <sec 1-18724> \| jp_interval <sec 1-18724> \| state [enable \| disable] \| mode [dm \| sm \| sm-dm] \| dr_priority <uint 0-4294967294>}(1) \| register_probe_time <value 1-127> \| register_suppression_time <value 3-255>] |
| **enable pim** |
| **disable pim** |
| **show pim neighbor** {ipif <ipif_name 12> \| ipaddress <network_address>} |
| **show pim** {ipif <ipif_name 12>} |
| **config pim cbsr** [ipif <ipif_name 12> {priority [-1 \| <value 0-255>]} \| hash_masklen <value 0-32> \| bootstrap_period <value 1-255>] |
| **show pim cbsr** {ipif <ipif_name 12>} |
| **config pim crp** {holdtime <value 0-255> \| priority <value 0-255> \| wildcard_prefix_cnt [0 \| 1]} (1) |
| **create pim crp group** <network_address> rp <ipif_name 12> |
| **delete pim crp group** <network_address> |
| **show pim crp** |
| **config pim last_hop_spt_switchover** [never \| immediately] |
| **show pim ipmroute** |
| **create pim static_rp group** <network_address> rp <ipaddr> |
| **delete pim static_rp group** <network_address> |
| **show pim static_rp** |
| **show pim rpset** |
| **create pim register_checksum_include_data rp_address** <ipaddr> |
| **delete pim register_checksum_include_data rp_address** <ipaddr> |
| **show pim register_checksum_include_data_rp_list** |
| **config pim-ssm** {state [enable \| disable] \| group_range [default \| <network_address>]} (1) |
| **show pim-ssm** |

## 73-1 config pim

### Description

This command is used to configure the PIM settings.

### Format

**config pim [[ipif <ipif_name 12> | all] {hello <sec 1-18724> | jp_interval <sec 1-18724> | state [enable | disable] | mode [dm | sm | sm-dm] | dr_priority <uint 0-4294967294>}(1) | register_probe_time <value 1-127> | register_suppression_time <value 3-255>]**

### Parameters

| |
|---|
| **ipif** - Specifies the IP interface name.<br>**<ipif_name 12>** - Enter the IP interface name used here. This name can be up to 12 characters long.<br>**all** - Specifies that all the IP interfaces will be used. |

**hello** - (Optional) Specifies the time between issuing hello packets to find neighboring routers.
**<sec 1-18724>** - Enter the hello time value here. This value must be between 1 and 18724 seconds. The default value is 30 seconds.

**jp_interval** - (Optional) Specifies the interval between transmitting (flooding to all interfaces) multicast messages to downstream routers, and automatically 'pruning' a branch from the multicast delivery tree. This interval also determines the time interval the router uses to automatically remove prune information from a branch of a multicast delivery tree and begin to flood multicast messages to all branches of that delivery tree. These two actions are equivalent. The default is 60 seconds.
**<sec 1-18724>** - Enter the join/prune interval value here. This value must be between 1 and 18724 seconds.

**state** - (Optional) Specifies to allow the PIM function to be disabled or enabled for the above IP interface. The default is disabled.
**enable** - Specifies that the PIM function will be enabled.
**disable** - Specifies that the PIM function will be disabled.

**mode** - (Optional) Specifies the multicast protocol mode used. – dense mode or sparse mode, or sm-dm mode. The default value is dense mode.
**dm** - Specifies that the multicast protocol mode will be set to dense mode.
**sm** - Specifies that the multicast protocol mode will be set to sparse mode.
**sm-dm** - Specifies that the multicast protocol mode will be set to both dense and sparse mode.

**dr_priority** - (Optional) Specifies the priority for DR election.
**<uint 0-4294967294>** - Enter the DR priority value used here. This value must be between 0 and 4294967294.

**register_probe_time** - Specifies the register probe time. The default value is 5 sec.
**<value 1-127>** - Enter the register probe time value here. This value must be between 1 and 127.

**register_suppression_time** - Specifies the register supression time. The default value is 60 sec.
**<value 3-255>** - Enter the register suppression time value here. This value must be between 3 and 255.

### Restrictions

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

### Example

To configure PIM configurations of IP interface System:

```
DGS-3620-28SC:admin# config pim ipif System hello 35 jp_interval 70 state
enable
Command: config pim ipif System hello 35 jp_interval 70 state enable

Success.

DGS-3620-28SC:admin#
```

## 73-2 enable pim

### Description

This command is used to enable PIM on the switch.

### Format

**enable pim**

### Parameters

None.

### Restrictions

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

### Example

To enable PIM:

```
DGS-3620-28SC:admin# enable pim
Command: enable pim

Success.

DGS-3620-28SC:admin#
```

## 73-3 disable pim

### Description

This command is used to disable PIM on the switch.

### Format

**disable pim**

### Parameters

None.

### Restrictions

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

### Example

To disable PIM:

```
DGS-3620-28SC:admin# disable pim
Command: disable pim

Success.

DGS-3620-28SC:admin#
```

## 73-4 show pim neighbor

### Description

This command is used to display the current PIM neighbor router table.

### Format

**show pim neighbor {ipif <ipif_name 12> | ipaddress <network_address>}**

### Parameters

**ipif** - (Optional) Specifies the name of the IP interface for which you want to display the current PIM neighbor router table.

**<ipif_name 12>** - Enter the IP interface name used here. This name can be up to 12 characters long.

**ipaddress** - (Optional) Specifies the IP address and netmask of the destination.

**<network_address>** - Enter the destination IP address used here.

If no parameter is specified, the system will display all the PIM neighbor addresses in the table.

### Restrictions

None.

### Example

To display PIM neighbor address table:

```
DGS-3620-28SC:admin# show pim neighbor
Command: show pim neighbor

PIM Neighbor Address Table
Interface Name   Neighbor Address  Expired Time
---------------  ----------------  ------------
System           10.48.74.122      5

Total Entries : 1

DGS-3620-28SC:admin#
```

## 73-5 show pim

### Description

This command is used to display the current PIM configuration.

### Format

**show pim {ipif <ipif_name 12>}**

### Parameters

**ipif -** (Optional) Specifies the name of the IP interface used to display the PIM configuration.

**<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 the PIM configurations of all IP interfaces.

### Restrictions

None.

### Example

To display PIM configurations of IP interface System:

```
DGS-3620-28SC:admin# show pim
Command: show pim

PIM Global State           : Enabled
Last Hop SPT Switchover    : Never
Register Probe Time        : 5
Register Suppression Time : 60

PIM Interface Table
                             Designated      Hello    J/P
Interface  IP Address        Router          Interval Interval Mode  State
---------- ----------------- --------------- -------- -------- ----- --------
System     10.90.90.101/8    10.90.90.101    35       70       DM    Enabled

Total Entries : 1

DGS-3620-28SC:admin#
```

## 73-6 config pim cbsr

### Description

This command is used to set the priority, hash mask length, and bootstrap period of the candidate bootstrap (C-BSR) router per interface.

### Format

**config pim cbsr [ipif <ipif_name 12> {priority [-1 | <value 0-255>]} | hash_masklen <value 0-32> | bootstrap_period <value 1-255>]**

### Parameters

**ipif** - Specifies the IP interface used for this configuration.
**<ipif_name 12>** - Enter the IP interface name used here. This name can be up to 12 characters long.

**priority** - (Optional) Specifies to set the C-BSR priority. The lower value indicates lower priority. The default value is -1. Note that only one interface can be the C-BSR in one device.
**-1** - Specifies that the interface will be disable to be the BSR.
**<value 0-255>** - Enter the C-BSR priority value used here. This value must be between 0 and 255.

**hash_masklen** - Enter a hash mask length, which will be used with the IP address of the

candidate RP and the multicast group address, to calculate the hash algorithm used by the router to determine which CRP on the PIM-SM enabled network will be the RP.
**<value 0-32>** - Enter the hash mask lenght value here. This value must be between 0 and 32. The default value is 30 seconds.

**bootstrap_period** - Specifies the interval between originating Bootstrap message.
**<value 1-255>** - Enter the bootstrap period value used here. This value must be between 1 and 255. The default value is 60 seconds.

### Restrictions

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

### Example

To configure the C-BSR for the System interface :

```
DGS-3620-28SC:admin# config pim cbsr ipif System priority 255
Command: config pim cbsr ipif System priority 255

Success.

DGS-3620-28SC:admin#
```

## 73-7 show pim cbsr

### Description

This command is used to list the candidate bootstrap router related information.

### Format

**show pim cbsr {ipif <ipif_name 12>}**

### Parameters

**ipif** - Specifies the IP interface used for this configuration.
**<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 C-BSR configurations.

### Restrictions

None.

### Example

To display the C-BSR settings:

```
DGS-3620-28SC:admin# show pim cbsr
Command: show pim cbsr

PIM Candidate-BSR Table

```

```
C-BSR Hash Mask Len        : 30
C-BSR Bootstrap Period     : 60

Interface    IP Address         Priority
------------ ------------------ -------------
System       11.52.33.3/8       -1 (Disabled)

Total Entries: 1

DGS-3620-28SC:admin#
```

## 73-8 config pim crp

### Description

This command is used to set the candidate rendezvous point (RP) related parameters.

### Format

**config pim crp {holdtime <value 0-255> | priority <value 0-255> | wildcard_prefix_cnt [0 | 1]} (1)**

### Parameters

**holdtime** - (Optional) This field is used to set the time Candidate RP (CRP) advertisements are valid on the PIM-SM enabled network. If CRP advertisements are not received by the BSR within this time frame, the CRP is removed from the list of candidates. An entry of 0 will send out one advertisement that states to the BSR that it should be immediately removed from CRP status on the PIM-SM network.
**<value 0-255>** - Enter the hold time for the RP here. This value must be between 0 and 255. The default value is 150 seconds.

**priority** - (Optional) Specifies the priority used for RP election. This priority value will be included in the router's CRP advertisements. A lower value means a higher priority, yet, if there is a tie for the highest priority, the router having the higher IP address will become the RP.
**<value 0-255>** - Enter the priority value used here. This value must be between 0 and 255. The default value is 192.

**wildcard_prefix_cnt** - (Optional) Specifies the Prefix Count value of  the wildcard address (224.0.0.0/24) to be choosed. The default vaule is 0.
**0** - Specifies that the wildcard prefix count value will be set to 0.
**1** - Specifies that the wildcard prefix count value will be set to 1.

### Restrictions

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

### Example

To configure the candidate rendezvous point (RP) holdtime, priority and wildcard prefix count:

```
DGS-3620-28SC:admin# config pim crp holdtime 150 priority 192
wildcard_prefix_cnt 0
Command: config pim crp holdtime 150 priority 192 wildcard_prefix_cnt 0


Success.
```

```

DGS-3620-28SC:admin#
```

## 73-9 create pim crp group

### Description

This command is used to add a multicast group range into a C-RP serve list for PIM-SM.

### Format

**create pim crp group <network_address> rp <ipif_name 12>**

### Parameters

**group** - Specifies the multicast group address for this Switch to become a Candidate RP. This address must be a class D address.
**<network_address>** - Enter the group network address used here.

**rp** - Specifies that the interface will act as C-RP for the group.
**<ipif_name 12>** - Enter the IP interface name used here. This name can be up to 12 characters long.

### Restrictions

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

### Example

To add a multicast group range into a C-RP server list:

```
DGS-3620-28SC:admin# create pim crp group 224.1.2.3/32 rp System
Command: create pim crp group 224.1.2.3/32 rp System

Success.

DGS-3620-28SC:admin#
```

## 73-10 delete pim crp group

### Description

This command is used to delete a multicast group range from the C-RP server list.

### Format

**delete pim crp group <network_address>**

### Parameters

**group** - Specifies the multicast group address for this switch to be removed from being a Candidate RP. This address must be a class D address.
**<network_address>** - Enter the multicast group network address used here.

### Restrictions

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

### Example

To delete a multicast group range from the C-RP server list:

```
DGS-3620-28SC:admin# delete pim crp group 224.1.2.3/32
Command: delete pim crp group 224.1.2.3/32

Success.

DGS-3620-28SC:admin#
```

## 73-11 show pim crp

### Description

This command is used to list all the candidate rendezvous point (C-RP) related information.

### Format

**show pim crp**

### Parameters

None.

### Restrictions

None.

### Example

To list all the candidate rendezvous point (C-RP) related information:

```
DGS-3620-28SC:admin# show pim crp
Command: show pim crp

PIM Candidate-RP Table

C-RP Holdtime                  : 150
C-RP Priority                  : 192
C-RP Wildcard Prefix Count     : 0

Group              Interface
----------------------- ------------------
224.0.0.0/4        System

Total Entries: 1

DGS-3620-28SC:admin#
```

## 73-12 config pim last_hop_spt_switchover

### Description

This command is used by the last hop router to decide whether to receive the multicast data from the shared tree or switch over to the shortest path tree. When the switchover mode is set to be never, the last hop router will always receive the multicast data from the shared tree. When the mode is set to immediately, the last hop router will always receive the multicast data from the shortest path tree.

### Format

**config pim last_hop_spt_switchover [never | immediately]**

### Parameters

**never** - Specifies that the router will always receive multicast data from the shared tree.

**immediately** - Specifies that the router will always receive multicast data from shortest path tree.

### Restrictions

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

### Example

Set the SPT-switchover mode to never:

```
DGS-3620-28SC:admin# config pim last_hop_spt_switchover never
Command: config pim last_hop_spt_switchover never

Success.

DGS-3620-28SC:admin#
```

## 73-13 show pim ipmroute

### Description

This command is used to list all the entries of multicast routing, includes (*,G), (S,G) and (S,G,rpt).

### Format

**show pim ipmroute**

### Parameters

None.

### Restrictions

None.

### Example

To list all the entries of multicast routing:

```
DGS-3620-28SC:admin# show pim ipmroute
Command: show pim ipmroute

PIM IP Multicast Route Table

UA = Upstream AssertTimer
AM = Assert Metric
AMPref = Assert MetricPref
ARB    = Assert RPTBit

Group Address    Source Address    UA    AM   AMPref  ARB  Flag Type    Mode
---------------- ----------------- ---- ---- ------ ---- ---- ------- ----
225.0.0.0        12.90.90.90/32    0     0     0      0      RPT  (*.G)   ASM
225.0.0.1        12.90.90.90/32    0     0     0      0      RPT  (*.G)   ASM
225.0.0.5        12.90.90.90/32    0     0     0      0      RPT  (*.G)   ASM
225.7.7.5        12.90.90.90/32    0     0     0      0      RPT  (*.G)   ASM
226.0.0.0        12.90.90.90/32    0     0     0      0      RPT  (*.G)   ASM
227.0.0.3        12.90.90.90/32    0     0     0      0      RPT  (*.G)   ASM
232.0.0.0        12.90.90.114/32   0     0     0      0      SPT  (S.G)   SSM
239.255.255.250  12.90.90.90/32    0     0     0      0      RPT  (*.G)   ASM

Total Entries: 8


DGS-3620-28SC:admin#
```

## 73-14 create pim static_rp group

### Description

This command is used to create a static RP.

### Format

**create pim static_rp group <network_address> rp <ipaddr>**

### Parameters

| |
|---|
| **group** - Specifies to assign the multicast group address for this static RP.<br>**<network_address>** - Enter the multicast group address used here. |
| **rp** - Specifies the  IP address used by this static RP.<br>**<ipaddr>** - Enter the IP address used here. |

### Restrictions

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

### Example

To create a static RP:

```
DGS-3620-28SC:admin# create pim static_rp group 239.1.1.0/24 rp 10.52.33.18
Command: create pim static_rp group 239.1.1.0/24 rp 10.52.33.18

Success.

DGS-3620-28SC:admin#
```

## 73-15 delete pim static_rp group

### Description

This command is used to delete a static RP.

### Format

**delete pim static_rp group <network_address>**

### Parameters

**group** - Specifies the multicast group address that will removed from the static RP.
**<network_address>** - Enter the multicast group address used here.

### Restrictions

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

### Example

To delete a static RP:

```
DGS-3620-28SC:admin# delete pim static_rp group 224.1.2.0/24
Command: delete pim static_rp group 224.1.2.0/24

Success.

DGS-3620-28SC:admin#
```

## 73-16 show pim static_rp

### Description

This command is used to list all the static RP settings.

### Format

**show pim static_rp**

### Parameters

None.

### Restrictions

None.

### Example

To list all the static RP settings:

```
DGS-3620-28SC:admin# show pim static_rp
Command: show pim static_rp

PIM Static RP Table

Group              RP Address
------------------ ------------------
224.1.2.0/24       10.52.33.4
239.1.1.0/24       10.52.33.18

Total Entries: 2

DGS-3620-28SC:admin#
```

## 73-17 show pim rpset

### Description

This command is used to list all the RPset information.

### Format

**show pim rpset**

### Parameters

None.

### Restrictions

None.

### Example

To list all the RPset information:

```
DGS-3620-28SC:admin# show pim rpset
Command: show pim rpset

PIM RP-Set Table
```

```
Bootstrap Router: 10.54.71.9

Group Address      RP Address     Holdtime  Expired Time   Type
---------------    ----------     --------  ------------   ----
224.0.0.0/4        10.20.6.36     210       196            Dynamic
224.0.0.0/4        10.54.71.9     0         0              Static

Total Entries: 2

DGS-3620-28SC:admin#
```

## 73-18 create pim register_checksum_include_data rp_address

### Description

This command is used to decide the checksum in register packet will include the data portion or not. As defined in RFC 4601, the checksum for Registers is done only on the first 8 bytes of the packet, including the PIM header and the next 4 bytes, excluding the data packet portion. Some earlier PIM-SM routers will calculate checksum for register packet including data portion. This configuration makes our routers communicate with those earlier routers smoothly. The default set is not including data portion.

### Format

**create pim register_checksum_include_data rp_address <ipaddr>**

### Parameters

**rp_address** - Specifies that the RP will expect to receive a register packet in which the checksum will be included in the data portion .
**<ipaddr>** - Enter the IP address used here.

### Restrictions

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

### Example

To create an entry for a specific RP in which the checksum in the registered packet will include the data portion:

```
DGS-3620-28SC:admin# create pim register_checksum_include_data rp_address
24.1.2.3
Command: create pim register_checksum_include_data rp_address 24.1.2.3

Success.

DGS-3620-28SC:admin#
```

## 73-19 delete pim register_checksum_include_data rp_address

### Description

This command is used to delete the register checksum including the data for the specific RP address.

### Format

**delete pim register_checksum_include_data rp_address <ipaddr>**

### Parameters

**rp_address** - Specifies the RP address that will be removed from the checksum, including the data portion list.
**<ipaddr>** - Enter the RP address used here.

### Restrictions

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

### Example

To delete the register checksum including the data for the specific RP address:

```
DGS-3620-28SC:admin# delete pim register_checksum_include_data rp_address
10.54.71.9
Command: delete pim register_checksum_include_data rp_address 10.54.71.9

Success.

DGS-3620-28SC:admin#
```

## 73-20 show pim register_checksum_include_data_rp_list

### Description

This command is used to list all the RPs of the registered checksum, including the data.

### Format

**show pim register_checksum_include_data_rp_list**

### Parameters

None.

### Restrictions

None.

### Example

To list all the RPs of the registered checksum, including the data:

```
DGS-3620-28SC:admin# show pim register_checksum_include_data_rp_list
Command: show pim register_checksum_include_data_rp_list

PIM Register Checksum Include Data

RP Address
------------------
24.0.0.0
24.1.2.3

Total Entries: 2

DGS-3620-28SC:admin#
```

## 73-21 config pim-ssm

### Description

This command is used to enable the SSM (Source-Specific Multicast) service model in PIM-SM on the switch. The PIM-SSM function will take active only when SSM service model and PIM-SM state both enabled.

### Format

**config pim-ssm {state [enable | disable] | group_range [default | <network_address>]} (1)**

### Parameters

**state** - (Optional) Specifies to enable or disable the SSM service model on the Switch.
  **enable** - Specifies that the SSM service model will be enabled.
  **disable** - Specifies that the SSM service model will be disabled.

**group_range** - (Optional) Specifies the group address range for the SSM service in IPv4.
  **default** - The default indicates that the group address range is 232.0.0.0/8.
  **<network_address>** - Enter the group address range for the SSM service here.

### Restrictions

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

### Example

To configure PIM-SSM state and group range:

```
DGS-3620-28SC:admin# config pim-ssm state enable group_range default
Command: config pim-ssm state enable group_range default

Success.

DGS-3620-28SC:admin#
```

## 73-22 show pim-ssm

### Description

This command is used to list all PIM-SSM protocol related information.

### Format

**show pim-ssm**

### Parameters

None.

### Restrictions

None.

### Example

To display PIM-SSM state and group range:

```
DGS-3620-28SC:admin# show pim-ssm
Command: show pim-ssm

SSM Service Model State    : Enabled
SSM Group                  : 232.0.0.0/8

DGS-3620-28SC:admin#
```

# Chapter 74 PIM6-SM Commands

| |
|---|
| **config pim6** [ipif <ipif_name 12> \| all] {hello_interval <sec 0-18000> \| triggered_hello_delay <sec 0-60> \| propagation_delay <sec 0-32> \| override_interval <sec 0-65> \| jp_interval <sec 0-18000> \| dr_priority <uint 0-4294967294> \| bsr_border [disable \| enable] \| stub_interface [disable \| enable] \| state [enable \| disable]} (1) |
| **show pim6** {ipif <ipif_name 12>} |
| **config pim6 cbsr** {ipif <ipif_name 12> state [enable \| disable] \| priority <value 0-255> \| hash_masklen <value 0-128>} (1) |
| **show pim6 cbsr** |
| **config pim6 crp** [rp <ipif_name 12> \| all] {priority <value 0-255> \| interval <sec 1-16383>} (1) |
| **create pim6 crp group** <ipv6networkaddr> rp <ipif_name 12> |
| **delete pim6 crp group** <ipv6networkaddr> |
| **enable pim6** |
| **disable pim6** |
| **config pim6 last_hop_spt_switchover** [never \| immediately] |
| **show pim6 neighbor** {ipif <ipif_name 12>} |
| **show pim6 mroute** {group <ipv6addr> {source <ipv6addr>}} |
| **create pim6 static_rp group** <ipv6networkaddr> rp <ipv6addr> {override_dynamic} |
| **delete pim6 static_rp group** <ipv6networkaddr> |
| **config pim6 embedded_rp state** [enable \| disable] |
| **show pim6 crp** |
| **show pim6 static_rp** |
| **show pim6 rpset** |
| **config pim6 register_checksum_calculate** [include_data \| not_include_data] |
| **config pim6 register_probe_time** <sec 1-127> |
| **config pim6 register_suppression_time** <sec 0-65535> |
| **config pim6 keepalive_period** <sec 120-65535> |
| **show pim6 mroute s_g** {rpt} {group <ipv6addr> source <ipv6addr> {ipif <ipif_name 12>}} |
| **show pim6 mroute star_g** {group <ipv6addr> {ipif <ipif_name 12>}} |

## 74-1 config pim6

### Description

This command is used to set the PIM6 multicast protocol state and some related parameters in the protocol on some interface.

### Format

**config pim6 [ipif <ipif_name 12> | all] {hello_interval <sec 0-18000> | triggered_hello_delay <sec 0-60> | propagation_delay <sec 0-32> | override_interval <sec 0-65> | jp_interval <sec 0-18000> | dr_priority <uint 0-4294967294> | bsr_border [disable | enable] | stub_interface [disable | enable] | state [enable | disable]} (1)**

### Parameters

| |
|---|
| **ipif** - Specifies the IP interface used for this configuration.<br>**<ipif_name 12>** - Enter the IP interface name used here. This name can be up to 12 characters long.<br>**all** - Specifies that all the IP interfaces will be used. |
| **hello_interval** - (Optional) Specifies the time between transmits hello packets to find neighboring |

routers. A value of zero represents an 'infinite' interval, and indicates that periodic PIM6 Hello message should not be sent on this interface.
**<sec 0-18000>** - Enter the hello packet interval value here. This value must be between 1 and 18000 seconds. The default value is 30 seconds.

**triggered_hello_delay** - (Optional) Specifies the maximum time before the router sends a triggered PIM Hello message on the specified interface. A value of zero has no special meaning and indicates that triggered PIM6 Hello message should always be sent immediately.
**<sec 0-60>** - Enter the triggered hello delay value here. This value must be between 0 and 60 seconds. The default value is 5 seconds.

**propagation_delay** - (Optional) Specifies the expected propagation delay between the PIM6 routers on this network or link.
**<sec 0-32>** - Enter the propagation delay value here. This value must be between 0 and 32 seconds. The default value is 1 second.

**override_interval** - (Optional) Specifies the value this router inserts into the Override_Interval field of the LAN Prune Delay option in the PIM6 Hello messages. When overriding a prune, PIM6 routers pick random time duration up to the value of this object.
**<sec 0-65>** - Enter the override interval value used here. This value must be between 0 and 65 seconds. The default value is 3 seconds.

**jp_interval** - (Optional) Specifies the frequency at which this router sends PIM6 Join/Prune messages on this PIM6 interface. A value of zero represents an 'infinite' interval, and indicates that periodic PIM6 Join/Prune messages should not be sent on this interface.
**<sec 0-18000>** - Enter the Join/Prune interval value used here. This value must be between 0 and 18000 seconds. The default value is 60 seconds.

**dr_priority** - (Optional) Specifies the Designated Router Priority value inserted into the DR Priority option in PIM6 Hello message transmitted on this interface. Numerically higher values for this parameter indicate higher priorities.
**<uint 0-4294967294>** - Enter the Designated Router priority value used here. This value must be between 0 and 4294967294. The default value is 1.

**bsr_border** - (Optional) Specifies whether or not this interface is a PIM6 domain border. If this interface configures a border, which will prevent bootstrap router (BSR) messages from being sent or received through it. By default, an interface is not PIM6 domain border.
**disable** - Specifies that this interface is a PIM6 domain border.
**enable** - Specifies that this interface is not a PIM6 domain border.

**stub_interface** - (Optional) Specifies whether this interface is a STUB interface. If this interface configures a stub interface, then no PIM6 packets are sent out this interface, and any received PIM6 packets are ignored. By default, an interface is not stub interface. When enabled, it is a security measure for interfaces towards untrusted hosts. It protects the PIM router from forged PIM messages on the interface.
**disable** - Specifies that this interface is a STUB interface.
**enable** - Specifies that this interface is not a STUB interface.

**state** - (Optional) Allows the PIM6 to be disabled or enabled for the above IPv6 interface. By default, the PIM6 protocol state is disabled on an interface.
**enable** - Specifies that PIM6 is enabled.
**disable** - Specifies that PIM6 is disabled.

## Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

## Example

To set the jp_interval to 60 seconds, the hello_interval to 60 seconds and enable the PIM6 state for interface "n10":

```
DGS-3620-28SC:admin# config pim6 ipif n10 jp_interval 60 hello_interval 60
state enable
Command: config pim6 ipif n10 jp_interval 60 hello_interval 60 state enable
```

```

Success.

DGS-3620-28SC:admin#
```

## 74-2 show pim6

### Description

This command is used to display the PIM6 configurations.

### Format

**show pim6 {ipif <ipif_name 12>}**

### Parameters

| |
|---|
| **ipif** - (Optional) Specifies the IP interface to be displayed.<br>**<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 the PIM6 parameters on all IPv6 interfaces in brief. |

### Restrictions

None. (EI Mode Only Command)

### Example

To show the brief info of the PIM6 protocol concerned parameters on all interfaces:

```
DGS-3620-28SC:admin# show pim6
Command: show pim6

PIM6 Global State                : Enabled
Last Hop SPT Switchover          : Immediately
Register Probe Interval          : 5 sec
Register Suppression Timeout     : 60 sec
Keepalive Period                 : 210 sec
Register Checksum Calculate      : Include Data
Embedded RP State                : Disabled

PIM6-SM Interface Table

              DR        Hello     J/P                   BSR
Interface     Priority  Interval  Interval   State      Border
----------    --------  --------  ---------  ---------  --------
System        1         3         60         Disabled   Disabled

Total Entries : 1

DGS-3620-28SC:admin#
```

To show the detailed info of the PIM6 protocol concerned parameters on the interface “System”:

```
DGS-3620-28SC:admin# show pim6 ipif System
Command: show pim6 ipif System

Interface Name                        : System
Interface Link-Local Address          : FE80::207:E9FF:81D
PIM6 Mode                             : SM
State                                 : Enabled
Designated Router                     : FE80::207:E9FF:FACC
Designated Router Priority            : 1
Designated Router Priority Enabled    : True
Hello Interval                        : 30 sec
Triggered Hello Interval              : 5 sec
Hello Holdtime                        : 105 sec
Join Prune Interval                   : 60 sec
Join Prune Holdtime                   : 210 sec
LAN Delay Enabled                     : True
Propagation Delay                     : 1 sec
Override Interval                     : 3 sec
Effective Propagation Delay           : 1 sec
Effective Override Interval           : 3 sec
Join Suppression Enabled              : True
Bidirectional Capable                 : False
BSR Domain Border                     : Disabled
Stub Interface                        : Disabled

DGS-3620-28SC:admin#
```

## 74-3 config pim6 cbsr

### Description

This command is used to set the parameters concerned with the candidate bootstrap router.

### Format

**config pim6 cbsr {ipif <ipif_name 12> state [enable | disable] | priority <value 0-255> | hash_masklen <value 0-128>} (1)**

### Parameters

**ipif** - (Optional) Specifies the IP interface used in this configuration.
 **<ipif_name 12>** - Enter the IP interface name used here. This name can be up to 12 characters long.

**state** - (Optional) Specifies whether the input interface can be a C-BSR or not.
 **enable** - Specifies that the input interface will be a C-BSR.
 **disable** - Specifies that the input interface will not be a C-BSR.

**priority** - (Optional) Specifies the C-BSR priority value.
 **<value 0-255>** - Enter the C-BSR priority value here. This value must be between 0 and 255. The default value is 64.

**hash_masklen** - (Optional) Specifies the length (in bits) of the mask. It makes use of a hash function for the case where a group range has multiple RPs with the same priority.
 **<value 0-128>** - Enter the length of the mask value here. This value must be between 0 and

128. The default value is 126.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

To configure the C-BSR on the interface “System”:

```
DGS-3620-28SC:admin# config pim6 cbsr ipif System state enable priority 64
hash_masklen 126
Command: config pim6 cbsr ipif System state enable priority 64 hash_masklen 126

Success.

DGS-3620-28SC:admin#
```

## 74-4 show pim6 cbsr

### Description

This command is used to display the candidate bootstrap router information.

### Format

**show pim6 cbsr**

### Parameters

None.

### Restrictions

None. (EI Mode Only Command)

### Example

To show C-BSR settings on the switch:

```
DGS-3620-28SC:admin# show pim6 cbsr
Command: show pim6 cbsr

PIM6 Candidate-BSR Information
---------------------------------------------
C-BSR Interface Name        : System
C-BSR Priority              : 64
C-BSR Hash Mask Len         : 126

DGS-3620-28SC:admin#
```

## 74-5 config pim6 crp

### Description

This command is used to set the candidate rendezvous point (RP) related parameters.

### Format

**config pim6 crp [rp <ipif_name 12> | all] {priority <value 0-255> | interval <sec 1-16383>} (1)**

### Parameters

**rp** - Specifies the RP IP interface used.
**<ipif_name 12>** - Enter the RP IP interface name used here. This name can be up to 12 characters long.
**all** - Specifies that all the RP IP interfaces will be used.

**priority** - (Optional) Specifies the RP priority value that will be used in the election process. The lower the value, the higher the priority.
**<value 0-255>** - Enter the RP priority value used here. This value must be between 0 and 255. The default value is 192.

**interval** - (Optional) Specifies the C-RP advertisement interval in seconds.
**<sec 1-16383>** - Enter the C-RP advertisement interval value here. This value must be betwee 1 and 16383 seconds. The default value is 60 seconds.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

To set the C-RP priority and the interval on the interface “System”:

```
DGS-3620-28SC:admin# config pim6 crp rp System priority 60 interval 60
Command: config pim6 crp rp System priority 60 interval 60

Success.

DGS-3620-28SC:admin#
```

## 74-6 create pim6 crp group

### Description

This command is used to add a multicast group range into a C-RP serve list.

### Format

**create pim6 crp group <ipv6networkaddr> rp <ipif_name 12>**

### Parameters

**group** - Specifies the IPv6 group address range served by the RP.
**<ipv6networkaddr>** - Enter the IPv6 network address used here.

**rp** - Specifies the interface that will act as the C-RP.
**<ipif_name 12>** - Enter the IP interface name used here. This name can be up to 12 characters long.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

To add a multicast group range “FF1E::12EF:1023/64” into the serve list of the C-RP “System”:

```
DGS-3620-28SC:admin# create pim6 crp group FF1E::12EF:1023/64 rp System
Command: create pim6 crp group FF1E::12EF:1023/64 rp System

Success.

DGS-3620-28SC:admin#
```

## 74-7 delete pim6 crp group

### Description

This command is used to delete a multicast group range from the C-RP server list.

### Format

**delete pim6 crp group <ipv6networkaddr>**

### Parameters

**group** - Specifies the multicast group address range of the C-RP entry that wants to be removed from C-RP serve list.
**<ipv6networkaddr>** - Enter the IPv6 network address used here.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

To delete a multicast group range “FF1E::12EF:1023/64” from the C-RP serve list:

```
DGS-3620-28SC:admin# delete pim6 crp group FF1E::12EF:1023/64
Command: delete pim6 crp group FF1E::12EF:1023/64

Success.

DGS-3620-28SC:admin#
```

## 74-8 enable pim6

### Description

This command is used to enable the PIM global state for IPv6 network.

### Format

**enable pim6**

### Parameters

None.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

To enable PIM global state for IPv6 network:

```
DGS-3620-28SC:admin# enable pim6
Command: enable pim6

Success.

DGS-3620-28SC:admin#
```

## 74-9 disable pim6

### Description

This command is used to disable the PIM global state for IPv6 network.

### Format

**disable pim6**

### Parameters

None.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

To disable PIM-SM for IPv6 network:

```
DGS-3620-28SC:admin# disable pim6
Command: disable pim6

Success.

DGS-3620-28SC:admin#
```

## 74-10 config pim6 last_hop_spt_switchover

### Description

This command is used on the last hop router to decide whether to receive the multicast data from the shared tree or switch over to the shortest path tree.

### Format

**config pim6 last_hop_spt_switchover [never | immediately]**

### Parameters

**last_hop_spt_switchover** - Specifies the SPT switchover mode on the last-hop switch.
**never** - Specifies that the mode will never switch to SPT. This is the default value.
**immediately** - Specifies that the mode will immediately switch to SPT.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

To set the SPT-switchover mode to never:

```
DGS-3620-28SC:admin# config pim6 last_hop_spt_switchover never
Command: config pim6 last_hop_spt_switchover never

Success.

DGS-3620-28SC:admin#
```

## 74-11 show pim6 neighbor

### Description

This command is used to list all neighbors learned by the PIM6 on the switch.

### Format

**show pim6 neighbor {ipif <ipif_name 12>}**

### Parameters

**ipif** - (Optional) Specifies the IP interface used.
**<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 neighbors learned by PIM6.

### Restrictions

None. (EI Mode Only Command)

### Example

To show the PIM6 neighbors:

```
DGS-3620-28SC:admin# show pim6 neighbor
Command: show pim6 neighbor

PIM6 Neighbor Address Table

Interface          Neighbor Address
-----------        ------------------
System             FE80::11FF:4CD8

Total Entries : 1

DGS-3620-28SC:admin#
```

To show the PIM6 neighbors of interface “n20”:

```
DGS-3620-28SC:admin# show pim6 neighbor ipif n20
Command: show pim6 neighbor ipif n20

Neighbor Info on Interface n20
----------------------------------------------------
Neighbor Address                    : FE80::11FF:4CD8
Neighbor Up Time                    : 00:00:50
Neighbor Expiry Time                : 00:01:50
Neighbor DR Priority Present        : True
Neighbor DR Priority                : 1

Total Entries : 1

DGS-3620-28SC:admin#
```

## 74-12 show pim6 mroute

### Description

This command is used to display the multicast routing info generated by the PIM6.

## Format

**show pim6 mroute {group <ipv6addr> {source <ipv6addr>}}**

## Parameters

**group** - (Optional) Specifies the IPv6 multicast group address.
**<ipv6addr>** - Enter the IPv6 multicast group address used here.

**source** - (Optional) Specifies the IPv6 source address. If this parameter is chosen, the (S, G) or (S, G, rpt) entries will be displayed; otherwise the (*, G) entries will be displayed.
**<ipv6addr>** - Enter the IPv6 source address used here.

If no parameter is specified, the system will display all IPv6 multicast routing entries.

## Restrictions

None. (EI Mode Only Command)

## Example

To show the whole IPv6 multicast routing table generated on the switch:

```
DGS-3620-28SC:admin# show pim6 mroute
Command: show pim6 mroute

Total (*,*,RP) Entries :  0
Total (*,G) Entries     :  1
Total (S,G) Entries     :  2
Total (S,G,rpt) Entries:  1

Group      : FF13::100
Source     : *                          Upstream: n1
RP Address: 3FFE:10:10::153
Outgoing  : n10 n30

Group   : FF13::100
Source  : 2001::1111                  Upstream: n2
Outgoing: n10

Group   : FF13::102
Source  : 2001::3F6D                  Upstream: n2
Outgoing: n20

Group      : FF13::100
Source     : 2001::1111,       rpt, Upstream: n1
RP Address: 3FFE:10:10::153
Outgoing  : -

Total Entries: 4

DGS-3620-28SC:admin#
```

You can check the detailed info for a specific multicasting routing entry by specifying the options in the command. To show the detailed info of the multicast routing entries for a specific group, you should specify the group address.

```
DGS-3620-28SC:admin# show pim6 mroute group FF13::100
Command: show pim6 mroute group FF13::100

(*, G) Entry for group FF13::100
---------------------------------------------
RP Address       : 3FFE:10:10::153
Upstream         : n1
Upstream State : Joined
RPF Neighbor   : FE80::68FE
Local Member   : n30
Assert Lost    : -
Assert Won     : -
Outgoing       : n10 n30

(S, G) Entry for group FF13::100
---------------------------------------------
Source  : 2001::1111            Upstream: n2
Outgoing: n10

Source  : 2001::1111     rpt,  Upstream: n1
Outgoing: -

Source  : 2001::3F6D            Upstream: n2
Outgoing: n20

Total Entries: 4

DGS-3620-28SC:admin#
```

To show the detailed info of the multicast routing entries for the specific (S,G), you should specify the group address and the source address.

```
DGS-3620-28SC:admin# show pim6 mroute group FF13::100 source 2001::1111
Command: show pim6 mroute group FF13::100 source 2001::1111

(S, G) Entry for group FF13::100 source 2001::1111
---------------------------------------------
RPT Bit                : False
Upstream               : n2
Upstream State        : Joined
RPF Neighbor          : FE80::12ED
SPT Bit                : True
Keepalive Timer      : 60 sec
Register State       : Prune
Register-Stop Timer : 10 sec
Local Member          : n30
Assert Lost           : n20
Assert Won            : n10
Outgoing              : n10 n30

RPT Bit          : True
RP Address      : 3FFE:10:10::153
Upstream        : n1
Upstream State : RPT not joined
RPF Neighbor    : FE80::68FE
Override Timer : 3 sec
Pruned           : n10
Outgoing        : -

Total Entries: 2

DGS-3620-28SC:admin#
```

## 74-13 create pim6 static_rp group

### Description

This command is used to create a static RP. Generally a static RP can’t override a dynamic RP. If the option ‘override_dynamic’ is chosen, the static RP will override any dynamically learned RP.

### Format

**create pim6 static_rp group <ipv6networkaddr> rp <ipv6addr> {override_dynamic}**

### Parameters

| |
|---|
| **group** - Specifies the multicast group network address for this static RP.<br>**<ipv6networkaddr>** - Enter the IPv6 group network address used here. |
| **rp** - Specifies the IPv6 address to this static RP.<br>**<ipv6addr>** - Enter the IPv6 address used here. |
| **override_dynamic** - (Optional) Specifies that the static RP will override the dynamically learned RP. |

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

To create a static RP:

```
DGS-3620-28SC:admin# create pim6 static_rp group FF1E::/64 rp 3000::12
Command: create pim6 static_rp group FF1E::/64 rp 3000::12

Success.

DGS-3620-28SC:admin#
```

## 74-14 delete pim6 static_rp group

### Description

This command is used to delete a static RP.

### Format

**delete pim6 static_rp group <ipv6networkaddr>**

### Parameters

**group** - Specifies the multicast group network address which will be removed from the static RP.
**<ipv6networkaddr>** - Enter the IPv6 network address used here.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

To delete a static RP:

```
DGS-3620-28SC:admin# delete pim6 static_rp group FF1E::/64
Command: delete pim6 static_rp group FF1E::/64

Success.

DGS-3620-28SC:admin#
```

## 74-15 config pim6 embedded_rp state

### Description

This command is used to set the state of the embedded RP.

### Format

**config pim6 embedded_rp state [enable | disable]**

### Parameters

**state** - Specifies the embedded RP support in the PIM6 state.
**enable** - Specifies that embedded RP support will be enabled.
**disable** - Specifies that embedded RP support will be disabled.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

To enable the embedded RP state:

```
DGS-3620-28SC:admin# config pim6 embedded_rp state enable
Command: config pim6 embedded_rp state enable

Success.

DGS-3620-28SC:admin#
```

## 74-16 show pim6 crp

### Description

This command is used to list all candidate rendezvous pint (RP) related information.

### Format

**show pim6 crp**

### Parameters

None.

### Restrictions

None. (EI Mode Only Command)

### Example

To show the C-RP information:

```
DGS-3620-28SC:admin# show pim6 crp
Command: show pim6 crp

PIM6 Candidate-RP Table

Group               Interface     Priority  Interval
------------------  ------------- --------- ---------
FF1E:90::/64       System        192       150

Total Entries: 1

DGS-3620-28SC:admin#
```

## 74-17 show pim6 static_rp

### Description

This command is used to list all static RP settings.

### Format

**show pim6 static_rp**

### Parameters

None.

### Restrictions

None. (EI Mode Only Command)

### Example

To show the static RP:

```
DGS-3620-28SC:admin# show pim6 static_rp
Command: show pim6 static_rp

PIM6 Static RP Table
---------------------------------------------
Group             : FF1E:9B::/64
RP Address        : 3000::1
Override Dynamic  : True

Group             : FF1E:9C::/64
RP Address        : 3000::5
Override Dynamic  : False

Total Entries: 2

DGS-3620-28SC:admin#
```

## 74-18 show pim6 rpset

### Description

This command is used to list the entire active RP information.

### Format

**show pim6 rpset**

### Parameters

None.

### Restrictions

None. (EI Mode Only Command)

### Example

To show the entire active RP information:

```
DGS-3620-28SC:admin# show pim6 rpset
Command: show pim6 rpset

Bootstrap Router: 2008::1

PIM6 RP-Set Table
-----------------------------------------
Group           : FF3D::/64
RP Address      : 2008::10F2
Hold Time       : 210 sec
Expired Time    : 196 sec
Type            : Dynamic

Group            : FF3D::/64
RP Address       : 3008::2DEF
Override Dynamic : False
Type             : Static

Total Entries: 2

DGS-3620-28SC:admin#
```

## 74-19 config pim6 register_checksum_calculate

### Description

This command is used to decide the checksum in register packet will include the data portion or not. As defined in RFC 4601, the checksum for Registers is done only on the first 8 bytes of the packet, including the PIM header and the next 4 bytes, excluding the data packet portion. Some earlier PIM6-SM routers will calculate checksum for register packet including data portion. This configuration makes our routers communicate with those earlier routers smoothly. The default set is not including data portion.

### Format

**config pim6 register_checksum_calculate [include_data | not_include_data]**

### Parameters

**register_checksum_calculate** - Specifies the register packet checksum calculating mechanism.

- **include_data** - When calculate the checksum in IPv6 PIM register packet, the data portion will be included.
- **not_include_data** - When calculate the checksum in IPv6 PIM register packet, the data portion won’t be included.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

To specify the switch calculates the register packet checksum including data portion:

```
DGS-3620-28SC:admin# config pim6 register_checksum_calculate include_data
Command: config pim6 register_checksum_calculate include_data

Success.

DGS-3620-28SC:admin#
```

## 74-20 config pim6 register_probe_time

### Description

This command is used to configure the PIM6-SM register probe time.

### Format

**config pim6 register_probe_time <sec 1-127>**

### Parameters

**register_probe_time** - Specifies the time before the Register-Stop Timer (RST) expires when a DR may send a Null-Register to the RP to cause it to resend a Register-Stop message.

**<sec 1-127>** - Enter the register probe time value here. This value must be between 1 and 127 seconds. The default value is 5 seconds.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

To configure the register probe time to be 20 seconds:

```
DGS-3620-28SC:admin# config pim6 register_probe_time 20
Command: config pim6 register_probe_time 20

Success.

DGS-3620-28SC:admin#
```

## 74-21 config pim6 register_suppression_time

### Description

This command is used to configure the PIM6-SM register suppression time. This is the period during which a PIM Designated Router (DR) stops sending Register-encapsulated data to the Rendezvous Point (RP) after receiving a Register-Stop message.

### Format

**config pim6 register_suppression_time <sec 0-65535>**

### Parameters

**register_suppression_time** - Specifies the period during which a PIM DR stops sending Register-encapsulated data to the RP after receiving a Register-Stop message.

**<sec 0-65535>** - Enter the register suppression time value here. This value must be between 0 and 65535 seconds. The default value is 60 seconds.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

To configure the PIM6-SM register suppression time to be 120 seconds:

```
DGS-3620-28SC:admin# config pim6 register_suppression_time 120
Command: config pim6 register_suppression_time 120

Success.

DGS-3620-28SC:admin#
```

## 74-22 config pim6 keepalive_period

### Description

This command is used to configure the PIM6-SM multicast routing entry Keepalive Timer. This is the period during which the PIM router will maintain (S, G) state in the absence of explicit (S, G) local membership or (S, G) join messages received to maintain it.

### Format

**config pim6 keepalive_period <sec 120-65535>**

### Parameters

**keepalive_period** - Specifies the period during which the PIM router will maintain (S, G) state in the absence of explicit (S, G) local membership or (S, G) join messages received to maintain it.

**<sec 120-65535>** - Enter the keep-alive period value here. This value must be between 120 and 65535 seconds. The default value is 210 seconds.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

To configure the multicast routing keepalive period to be 220 seconds:

```
DGS-3620-28SC:admin# config pim6 keepalive_period 220
Command: config pim6 keepalive_period 220

Success.

DGS-3620-28SC:admin#
```

## 74-23 show pim6 mroute s_g

### Description

This command is used to display the multicast routing information for (S, G) or (S, G, rpt) entries generated by PIM6.

### Format

**show pim6 mroute s_g {rpt} {group <ipv6addr> source <ipv6addr> {ipif <ipif_name 12>}}**

### Parameters

| |
|---|
| **rpt** - (Optional) Specifies the (S, G, rpt) entry. |
| **group** - (Optional) Specifies the IPv6 multicast group address.<br>**<ipv6addr>** - Enter the IPv6 multicast group address used here. |
| **source** - (Optional) Specifies the source IPv6 interface.<br>**<ipv6addr>** - Enter the IPv6 interface network address used here.<br>**ipif** - Specifies the IPv6 interface name.<br>**<ipif_name 12>** - Enter the IPv6 interface name here. This name can be up to 12 characters long. |
| If no parameter is specified, the switch will display all the (S, G) route entries in the IPv6 multicast routing table in brief. |
| If only specified parameter {rpt}, the switch will display all the (S, G, rpt) route entries in the IPv6 multicast routing table in brief. |

### Restrictions

None. (EI Mode Only Command)

### Example

To show all (S, G) route entries generated on the switch:

```
DGS-3620-28SC:admin# show pim6 mroute s_g
Command: show pim6 mroute s_g

(S, G) Entry Table
------------------------
Group      : FF13::100
Source     : 2001::1111

Group      : FF13::100
Source     : 2001::2222
```

```

Group     : FF13::200
Source    : 2001::1111

Group     : FF13::300
Source    : 2001::1111

Total Entries: 4

DGS-3620-28SC:admin#
```

Check the detailed information for a specific multicasting route entry by specifying the options in the command. To show the detailed information of the multicast route entries of the specific group and source address.

```
DGS-3620-28SC:admin# show pim6 mroute s_g group FF13::100 source 2001::1111
Command: show pim6 mroute s_g group FF13::100 source 2001::1111

Group Address                : FF13::100
Source Address               : 2001::1111
Uptime                       : 150 sec
Upstream Join State          : Joined
Upstream Join Timer          : 20 sec
Upstream Neighbor            : FE80::12ED
RPF Interface                : n20
RPF Next Hop                 : FE80::12ED
RPF Route Protocol           : OSPF
RPF Route Address            : 3FFE:10:10::147
RPF Route Prefix Length      : 64
RPF Route Metric Pref        : 20
RPF Route Metric             : 3
SPT Bit                      : True
Keepalive Timer              : 60 sec
DR Register State            : NoInfo
DR Register Stop Timer       : 0 sec

DGS-3620-28SC:admin#
```

To show the detailed information on a downstream interface of the multicast routing entry (S, G), specify the group address, source address and the interface name.

```
DGS-3620-28SC:admin# show pim6 mroute s_g group FF13::100 source 2001::1111
ipif n20
Command: show pim6 mroute s_g group FF13::100 source 2001::1111 ipif n20

Group Address                : FF13::100
Source Address               : 2001::1111
Interface Name               : n20
Uptime                       : 150 sec
Have Local Membership        : True
Join Prune State             : Join
Prune Pending Timer          : 0 sec
```

```
Join Expiry Timer             : 10 sec
Assert State                  : NoInfo
Assert Timer                  : 0 sec
Assert Winner Address         : -
Assert Winner Metric Pref     : 0
Assert Winner Metric          : 0

DGS-3620-28SC:admin#
```

To show the whole IPv6 multicast routing table of (S, G, rpt) generated on the switch:

```
DGS-3620-28SC:admin# show pim6 mroute s_g rpt
Command: show pim6 mroute s_g

(S, G, rpt) Entry Table
------------------------
Group          : FF13::100
Source         : 2001::1111
RP Address     : 3FFE:10:10::153

Group          : FF13::100
Source         : 2001::2222
RP Address     : 3FFE:10:10::153

Group          : FF13::200
Source         : 2001::1111
RP Address     : 3FFE:10:10::153

Group          : FF13::300
Source         : 2001::1111
RP Address     : 3FFE:10:10::153

Total Entries: 4

DGS-3620-28SC:admin#
```

Check the detailed information for a specific multicasting routing entry by specifying the options in the command. To show the detailed information of a multicast route entry (S, G, rpt), specify the group address and the source address.

```
DGS-3620-28SC:admin# show pim6 mroute s_g rpt group FF13::100 source 2001::1111
Command: show pim6 mroute s_g rpt group FF13::100 source 2001::1111

Group Address              : FF13::100
Source Address             : 2001::1111
Uptime                     : 150 sec
Upstream Prune State       : RPT not joined
Upstream Override Timer    : 0 sec

DGS-3620-28SC:admin#
```

To show the detailed information on a downstream interface of the multicast routing entry (S, G, rpt), specify the group address, source address and interface name.

```
DGS-3620-28SC:admin# show pim6 mroute s_g rpt group FF13::100 source 2001::1111
ipif n20
Command: show pim6 mroute s_g rpt group FF13::100 source 2001::1111 ipif n20

Group Address                : FF13::100
Source Address               : 2001::1111
Interface Name               : n20
Uptime                       : 150 sec
Have Local Membership        : True
Join Prune State             : Prune
Prune Pending Timer          : 0 sec
Prune Expiry Timer           : 15 sec

DGS-3620-28SC:admin#
```

## 74-24 show pim6 mroute star_g

### Description

This command is used to display the multicast routing information for (*, G) entries generated by PIM6. Users can get detailed info of the routing entries by choosing the options in the command.

### Format

**show pim6 mroute star_g {group <ipv6addr> {ipif <ipif_name 12>}}**

### Parameters

**group** - (Optional) Specifies the IPv6 multicast group address.
**<ipv6addr>** - Enter the IPv6 multicast group address used here.

**ipif** - (Optional) Specifies the IPv6 interface name.
**<ipif_name 12>** - Enter the IPv6 interface name used here. This name can be up to 12 characters long.

If no parameter is specified, the switch will display all (*, G) entries of the IPv6 multicast routing table in brief.

### Restrictions

None. (EI Mode Only Command)

### Example

To show the whole IPv6 multicast routing table of (*, G) generated on the switch:

```
DGS-3620-28SC:admin# show pim6 mroute star_g
Command: show pim6 mroute star_g

(*, G) Entry Table
-------------------------
Group           : FF13::100
Upstream        : n2
```

```
RP Address     : 3FFE:10:10::153

Group          : FF13::101
Upstream       : n2
RP Address     : 3FFE:10:10::153

Group          : FF13::102
Upstream       : n2
RP Address     : 3FFE:10:10::153

Total Entries: 3

DGS-3620-28SC:admin#
```

Check the detailed information for a specific multicasting routing entry by specifying the options in the command. To show the detailed information of the multicast routing entries for a specific group, specify the group address.

```
DGS-3620-28SC:admin# show pim6 mroute star_g group FF13::100
Command: show pim6 mroute star_g group FF13::100

Group Address                : FF1E::100
Uptime                       : 150 sec
RP Address                   : 3FFE:10:10::153
RP Is Local                  : False
Upstream Join State          : Joined
Upstream Join Timer          : 20 sec
Upstream Neighbor            : FE80::68FE
RPF Next Hop                 : FE80::68FE
RPF Route Protocol           : OSPF
RPF Route Address            : 3FF5::147
RPF Route Prefix Length      : 64
RPF Route Metric Preference  : 20
RPF Route Metric             : 3

DGS-3620-28SC:admin#
```

To show the detailed information on a downstream interface of the multicast routing entries (*, G), specify the group address and the interface name.

```
DGS-3620-28SC:admin# show pim6 mroute star_g group FF13::100 ipif n10
Command: show pim6 mroute star_g group FF13::100 ipif n10

Group Address             : FF1E::100
Interface Name            : n10
Uptime                    : 150 sec
Have Local Membership     : True
Join Prune State          : Join
Prune Pending Timer       : 0 sec
Join Expiry Timer         : 10 sec
Assert State              : NoInfo
Assert Timer              : 0 sec
Assert Winner Address      : -
Assert Winner Metric Pref : 0
Assert Winner Metric      : 0

DGS-3620-28SC:admin#
```

# Chapter 75 Policy Route Commands

**create policy_route name** <policyroute_name 32>

**delete policy_route name** <policyroute_name 32>

**config policy_route name** <policyroute_name 32> acl profile_id <value 1-6> access_id <value 1-256> nexthop <ipaddr> state [enable | disable]

**show policy_route**

## 75-1 create policy_route name

### Description

This command is used to create a policy route and define the rule's name.

### Format

**create policy_route name <policyroute_name 32>**

### Parameters

**<policyroute_name 32>** - The policy route name. The maximum length is 32 characters.

### Restrictions

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

### Example

To create a policy route named "danilo":

```
DGS-3620-28SC:admin#create policy_route name danilo
Command: create policy_route name danilo

Success.

DGS-3620-28SC:admin#
```

## 75-2 delete policy_route name

### Description

This command is used to delete a policy route.

### Format

**delete policy_route name <policyroute_name 32>**

### Parameters

**<policyroute_name 32>** - The policy route name. The maximum length is 32 characters.

### Restrictions

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

### Example

To delete an IP route entry in the switch’s IP routing table named “duhon”:

```
DGS-3620-28SC:admin#delete policy_route name duhon
Command: delete policy_route name duhon

Success.

DGS-3620-28SC:admin#
```

## 75-3 config policy_route name

### Description

This command allows users to configure the different fields for a policy route entry. Users can set the state of a policy route to enable or disable.

- The user must create an ACL rule. If the ACL rule does not exist, the system will display an error message.
- If the ACL rule action is drop, these packets will not forward and the policy route will not be implemented.
- When a packet passes from the policy route, its TTL will decrease by 1.
- If a user deletes an ACL rule that is linked to a policy rule, the system will display an error message.

### Format

**config policy_route name <policyroute_name 32> acl profile_id <value 1-6> access_id <value 1-256> nexthop <ipaddr> state [enable | disable]**

### Parameters

**<policyroute_name 32>** - The policy route name. The maximum length is 32 characters.

**acl profile_id** - The ACL profile ID.
    **<value 1-6>**- Specifies the value between 1 and 6.

**access_id** - The ACL access ID.
    **<value 1-256>** - Specifies the value between 1 and 256.

**nexthop** - The next hop IP address.
    **<ipaddr>** - Specifies the IP address.

**state** - Activate or deactivate this rule.
    **enable** - Activate this rule.
    **disable** - Deactivate this rule.

### Restrictions

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

### Example

To configure all packets which match ACL rule profile ID=1 and access ID=1, and then route to 20.1.1.100:

```
DGS-3620-28SC:admin#config policy_route name danillo acl profile_id 1 access_id
1 nexthop 20.1.1.100 state enable
Command: config policy_route name danillo acl profile_id 1 access_id 1 nexthop
20.1.1.100 state enable

Success.

DGS-3620-28SC:admin#
```

## 75-4 show policy_route

### Description

This command is used to display the switch’s current policy route rules.

### Format

**show policy_route**

### Parameters

None.

### Restrictions

None.

### Example

To display the switch’s current policy route rules:

```
DGS-3620-28SC:admin#show policy_route
Command: show policy_route

Policy Routing Table
---------------------

Name                             Profile ID  Access ID Next Hop          State
-------------------------------- ----------  --------- --------------- --------
rname                            1           1         192.168.69.1    Enabled

Total Entries: 1

DGS-3620-28SC:admin#
```

# Chapter 76 Port Security Commands

| |
|---|
| **config port_security ports** [<portlist> \| all] [{admin_state [enable \| disable] \| max_learning_addr <max_lock_no 0-3328> \| lock_address_mode [permanent \| deleteontimeout \| deleteonreset]}(1) \| {vlan [<vlan_name 32> \| vlanid <vidlist>] max_learning_addr [<max_lock_no 0-3328> \| no_limit]}(1)] |
| **config port_security system max_learning_addr** [<max_lock_no 1-3328> \| no_limit] |
| **config port_security vlan** [<vlan_name 32> \| vlanid <vidlist>] max_learning_addr [<max_lock_no 0-3328> \| no_limit] |
| **delete port_security_entry** [vlan <vlan_name 32> \| vlanid <vlanid 1-4094>] mac_address <macaddr> |
| **clear port_security_entry** {ports [<portlist> \| all] \| {[vlan <vlan_name 32> \| vlanid <vidlist>]}} |
| **show port_security_entry** {ports {<portlist>} {[vlan <vlan_name 32> \| vlanid <vidlist>]}} |
| **show port_security** {ports {<portlist>} {[vlan <vlan_name 32> \| vlanid <vidlist>]}} |
| **enable port_security trap_log** |
| **disable port_security trap_log** |

## 76-1 config port_security ports

### Description

This command is used to set the port’s state, maximum supported MAC address entries, the default entry type, and set the maximum port-security entries that can be learned with a specific VLAN on a specific port. There are four levels of limitations on the learned entry number, for the entire system, for a port, for a VLAN, and for specific VLAN on a port. If any limitation is exceeded, the new entry will be discarded.

### Format

**config port_security ports [<portlist> | all] [{admin_state [enable | disable] | max_learning_addr <max_lock_no 0-3328> | lock_address_mode [permanent | deleteontimeout | deleteonreset]}(1) | {vlan [<vlan_name 32> | vlanid <vidlist>] max_learning_addr [<max_lock_no 0-3328> | no_limit]}(1)]**

### Parameters

| |
|---|
| **<portlist>** - Specify a range of ports to be configured. |
| **all** - Specify that all ports will be configured. |
| **admin_state** - Allow the port security to be enabled or disabled for the ports specified in the port list. The default setting is disabled.<br>**enable** - Enable port security for the ports specified in the port list.<br>**disable** - Disable port security for the ports specified in the port list. |
| **max_learning_addr** - Specify the maximum of MAC address entries that can be learned on this port. If the value is set to 0, it means that no user can get 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.<br>**<max_lock_no 0-3328>** - Specify the value between 0 and 3328. |
| **lock_address_mode** - Indicate locking address mode. The default mode is deleteonreset.<br>**permanent** - The address will never be deleted unless the user removes it manually or the |

VLAN of the entry is removed or the port are removed from the VLAN, or port security is disabled on the port where the address resides.
**deleteontimeout** - The locked addresses can be aged out after aging timer expires.
**deleteonreset** - This address will be removed if the switch is reset or reboots. The cases under which the permanent entries are deleted also apply to the deleteonreset entries

**vlan** - (Optional) Specify the VLAN to limit the address learning.
**<vlan_name 32>** - Specify the name of the VLAN. The maximum length is 32 characters.
**vlanid** - Specify a list of VLANs by VLAN ID to limit the address learning.
**<vidlist>** - Specify a list of VLAN ID.

**max_learning_addr** - (Optional) Specify the maximum of MAC address entries that can be learned on this port. If the value is set to 0, it means that no user can get authorized by the port security function on this port. If the setting is smaller than the number of current learned entries on the port, the command will be rejected. The default value is 32.
**<max_lock_no 0-3328>** - Specify the value between 0 and 3328.
**no_limit** - Specify no limitation on the number of entries.

### Restrictions

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

### Example

To configure port security:

```
DGS-3620-28SC: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-3620-28SC:admin#
```

To configure a port security setting:

```
DGS-3620-28SC:admin#config port_security ports 1 vlan vlanid 1
max_learning_addr 16
Command: config port_security ports 1 vlan vlanid 1 max_learning_addr 16

Success.

DGS-3620-28SC:admin#
```

## 76-2 config port_security system max_learning_addr

### Description

This command is used to set the maximum number of MAC address 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 specific VLAN on a port. If any limitation is exceeded, the new entry will be discarded. The setting for system level max learned users must be greater than the total of the max learned users allowed on all ports.

### Format

**config port_security system max_learning_addr [<max_lock_no 1-3328> | no_limit]**

### Parameters

**<max_lock_no 1-3328>** - Specify the maximum number of MAC address 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.

**no_limit** - By default, the number above is set to no limit.

### Restrictions

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

### Example

To configure the maximum number of port security entries to 256:

```
DGS-3620-28SC:admin# config port_security system max_learning_addr 256
Command: config port_security system max_learning_addr 256

Success.

DGS-3620-28SC:admin#
```

## 76-3 config port_security vlan

### Description

This command sets the maximum number of MAC address entries that can be learned on a specific VLAN. There are four levels of limitations on the learned entry number, for the entire system, for a port, for a VLAN, and for specific VLAN on a port. If any limitation is exceeded, the new entry will be discarded.

### Format

**config port_security vlan [<vlan_name 32> | vlanid <vidlist>] max_learning_addr [<max_lock_no 0-3328> | no_limit]**

### Parameters

**<vlan_name 32> -** Specify the VLAN by name. The maximum length is 32 characters.

**vlanid** - Specify a list of VLANs by VLAN ID.
**<vidlist>** - Specify the VLAN ID.

**max_learning_addr** - Specify the maximum number of MAC address entries that can be learned with this VLAN. If this parameter is set to 0, it means that no user can get authorization on this VLAN. If the setting is smaller than the number of current learned entries on the VLAN, the command will be rejected.
**<max_lock_no 0-3328>** - Specify the value between 0 and 3328.
**no_limit -** Specify the default value is no limit.

### Restrictions

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

### Example

To configure the maximum number of entries that can be learned at 64:

```
DGS-3620-28SC:admin#config port_security vlan vlanid 1 max_learning_addr 64
Command: config port_security vlan vlanid 1 max_learning_addr 64

Success.

DGS-3620-28SC:admin#
```

## 76-4 delete port_security_entry

### Description

This command is used to delete a port security entry by VLAN, VLAN ID, and MAC address.

### Format

**delete port_security_entry [vlan <vlan_name 32> | vlanid <vlanid 1-4094>] mac_address <macaddr>**

### Parameters

| |
|---|
| **vlan** - Specify the VLAN by name.<br>**<vlan_name 32>** - Specify the VLAN name. The maximum length is 32 characters. |
| **vlanid** - Specify a list of VLANs by VLAN ID.<br>**<vlanid 1-4094>** - Specify the VLAN ID. This value must be between 1 and 4094. |
| **mac_address** - Specify the MAC address of the entry.<br>**<macaddr>** - Specify the MAC address of the entry. |

### Restrictions

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

### Example

To delete the port security entry with a MAC address of 00-01-30-10-2c-c7 on the default VLAN:

```
DGS-3620-28SC:admin#delete port_security_entry vlan default mac_address 00-01-
30-10-2C-C7
Command: delete port_security_entry vlan default mac_address 00-01-30-10-2C-C7

Success.

DGS-3620-28SC:admin#
```

## 76-5 clear port_security_entry

### Description

This command is used to clear the MAC entries learned from the specified port(s) or VLAN(s) for the port security function.

### Format

**clear port_security_entry {ports [<portlist> | all] | {[vlan <vlan_name 32> | vlanid <vidlist>]}}**

### Parameters

**ports** - (Optional) The port-security entries learned on the specified port will be cleared.
    **<portlist>** - Specify a range of ports to be configured.
    **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>** - Specify the VLAN name. The maximum length is 32 characters.

**vlanid** - (Optional) Specify a list of VLANs by VLAN ID.
    **<vidlist>** - Specify a list of the VLAN IDs.

### Restrictions

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

### Example

To clear port security entry for port 6:

```
DGS-3620-28SC:admin#clear port_security_entry port 6
Command: clear port_security_entry port 6

Success.

DGS-3620-28SC:admin#
```

## 76-6 show port_security_entry

### Description

This command is used to display a port security entry.

### Format

**show port_security_entry {ports {<portlist>} {[vlan <vlan_name 32> | vlanid <vidlist>]}}**

### Parameters

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

**vlan** - (Optional) Specify a VLAN to display its entry.
    **<vlan_name 32>** - Specify the VLAN name. The maximum length is 32 characters.

**vlanid** - (Optional) Specify a VLAN list to display its entry.
    **<vidlist>** - Specify a list of the VLAN IDs.

### Restrictions

None.

### Example

To display a port security entry:

```
DGS-3620-28SC: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 Entry Number: 1

DGS-3620-28SC:admin#
```

## 76-7 show port_security

### Description

This command is used to display the port security related information of the switch ports including the port security admin state, the maximum number of learning addresses, and the lock mode.

### Format

**show port_security {ports {<portlist>} {[vlan <vlan_name 32> | vlanid <vidlist>]}}**

### Parameters

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

**vlan** - (Optional) Specify a VLAN to display its configuration.
  **<vlan_name 32>** - Specify the VLAN name. The maximum length is 32 characters.

**vlanid** - (Optional) Specify a VLAN list to display the configuration.
  **<vidlist>** - Specify a list of the VLAN IDs.

### Restrictions

None.

### Example

To display the global configuration of port security:

```
DGS-3620-28SC:admin# show port_security
Command: show port_security

Port Security Trap/Log          : Disabled
```

```
System Maximum Address          : 512

 VLAN Configuration (Only VLANs with limitation are displayed)
 VID   VLAN Name                        Max. Learning Addr.
 ----  --------------------------------  -------------------
 1     default                          64
 2     TstVLAN                          8

DGS-3620-28SC:admin#
```

To display the port security information of switch ports 1 to 6:

```
DGS-3620-28SC:admin#show port_security ports 1-6
Command: show port_security ports 1-6

Port   State    Lock Address Mode   Max. Learning Addr.
-----  -------  ------------------  -----------------
1      Disabled DeleteOnReset       32
2      Disabled DeleteOnReset       32
3      Disabled DeleteOnReset       32
4      Disabled DeleteOnReset       32
5      Disabled DeleteOnReset       32
6      Disabled DeleteOnReset       32

DGS-3620-28SC:admin#
```

## 76-8 enable port_security trap_log

### Description

This command is used to enable port security traps/logs. When this command is enabled, if there's a new MAC that violates the pre-defined port security configuration, a trap will be sent out with the MAC and port information and the relevant information will be logged.

### Format

**enable port_security trap_log**

### Parameters

None.

### Restrictions

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

### Example

To enable a port security trap:

```
DGS-3620-28SC:admin#enable port_security trap_log
Command: enable port_security trap_log
```

```
Success.

DGS-3620-28SC:admin#
```

## 76-9 disable port_security trap_log

### Description

This command is used to disable a port security trap/log. If the port security trap is disabled, no trap will be sent out for MAC violations, and no log will be recorded.

### Format

**disable port_security trap_log**

### Parameters

None.

### Restrictions

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

### Example

To prevent a port security trap from being sent from the switch:

```
DGS-3620-28SC:admin#disable port_security trap_log
Command: disable port_security trap_log

Success.

DGS-3620-28SC:admin#
```

# Chapter 77 Power over Ethernet (PoE) Commands

| |
|---|
| **config poe ports** [all \| <portlist>] {state [enable \| disable] \| [time_range <range_name 32> \| clear_time_range] \| priority [critical \| high \| low] \| power_limit [class_0 \| class_1 \| class_2 \| class_3 \| user_define <value 1000-35000>]} |
| **config poe system** {units [<unitlist> \| all]} {power_limit <value 37-760> \| power_disconnect_method [deny_next_port \| deny_low_priority_port] \| legacy_pd [enable \| disable]} |
| **show poe ports** {<portlist>} |
| **show poe system** {units <unitlist>} |

## 77-1 config poe ports

### Description

This command is used to configure the PoE port settings.

**Note:** This command is only available to Switches in the DGS-3620 Series that support Power over Ethernet.

### Format

**config poe ports [all | <portlist>] {state [enable | disable] | [time_range <range_name 32> | clear_time_range] | priority [critical | high | low] | power_limit [class_0 | class_1 | class_2 | class_3 | user_define <value 1000-35000>]}**

### Parameters

| |
|---|
| **ports** - Specifies the list of port used for this configuration.<br>**all** - Specifies that all the ports will be used for this configuration.<br>**<portlist>** - Enter the list of ports, used for this configuration, here. |
| **state** - (Optional) Specifies whether power will be supplied to the powered device connected to this port or not.<br>**enable** - Specifies that PoE will be enabled of the specifies port(s).<br>**disable** - Specifies that PoE will be disabled of the specifies port(s). |
| **time_range** - (Optional) Specifies the time range that applies to the port of the PoE. If the time range is configured, the power can only be supplied during the period specified by the time range.<br>**<range_name 32>** - Enter the the time range name used here. This name can be up to 32 characters long.<br>**clear_time_range** - Specifies that the time range will be removed. |
| **priority** - (Optional) Port priority determines the priority the system attempts to supply the power to the port. There are three levels of priority that can be selected, critical, high, and low. When multiple ports happen to have the same level of priority, the port ID will be used to determine the priority. The lower port ID has higher priority. The setting of priority will affect the ordering of supplying power. Whether the disconnect method is set to deny low priority port, priority of port will be used by the system to manage the power supply to the ports.<br>**critical** - Specifies that the priority value will be set to critical.<br>**high** - Specifies that the priority value will be set to high.<br>**low** - Specifies that the priority value will be set to low. |

**power_limit** - (Optional) Specifies the per-port power limit. If a port exceeds its power limit, it will be shut down. Based on the industry standard, 802.3af, there are 5 kinds of PD classes, class 0, class 1, class 2, and class 3. The power consumption ranges for them are 0.44~12.95W, 0.44~3.84W, 3.84~6.49W, 6.49~12.95W, and 12.95~29.5W, respectively. The five pre-defined settings are for the users' convenience: The following is the power limit applied to the port for these four classes. For each class, the power limit is a little more than the power consumption range for the class. This takes the factor of the power loss on cable into account.
**class_0** - Specifies that the power limit will be set to 15400mW.
**class_1** - Specifies that the power limit will be set to 4000mW.
**class_2** - Specifies that the power limit will be set to 7000mW.
**class_3** - Specifies that the power limit will be set to 15400mW.
**user_define** - Specifies the user defined power limit value here.
**<value 1000-35000>** - Enter the user defined port limit value used here. This value must be between 1000 and 35000mW. Other than the four pre-defined settings, the users can directly specify any value that the chip supports. Normally, the minimum setting is 1000mW, and the maximum setting is 15400mW for 802.3af and greater or equal to 35000mW for 802.3at.

### Restrictions

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

### Example

To configure the PoE port:

```
DGS-3620-28PC:admin# config poe ports 1:1-1:4 state enable priority critical
power_limit class_1
Command: config poe ports 1:1-1:4 state enable priority critical power_limit
class_1

Success.

DGS-3620-28PC:admin#
```

## 77-2 config poe system

### Description

This command is used to configure the parameters for the PoE system-wise function

**Note:** This command is only available to Switches in the DGS-3620 Series that support Power over Ethernet.

### Format

**config poe system {units [<unitlist> | all]} {power_limit <value 37-760> | power_disconnect_method [deny_next_port | deny_low_priority_port] | legacy_pd [enable | disable]}**

### Parameters

**units** - (Optional) Specifies the unit list that will be configured.
**<unitlist>** - Enter the unit list, used for this configuration, here.
**all** - Specifies that all the units will be used for this configuration.

**power_limit** - (Optional) Specifies the power budget of the PoE system.
**<value 37-760>** - Enter the power budger limit value here. This value must be between 37 and 760.

**power_disconnect_method** - (Optional) Specifies the disconnection method that will be used when the power budget is running out. When the system attempts to supply power to a new port, if the power budget is insufficient to do this, the PoE controller will initiate a port disconnection procedure to prevent overloading the power supply. The controller uses one of the following two ways to perform the disconnection procedure.
**deny_next_port** - Specifies the port with the maximum port number will be denied regardless of its priority. If the disconnect method is set to deny the next port, the power provision will not utilize the system's maximum power. There is a 19W safety margin. That is, when the system has only 19W remaining, this power cannot be utilized.
**deny_low_priority_port** - If there are ports that supplied power, that have a priority lower than the new port, the port with the lowest priority will be disconnected. This process will stop until enough power is released for the new port. Note that if the disconnect method is set to deny low priority port, then the power provision can utilize the system's maximum power.

**legacy_pd** - (Optional) Specifies the legacy PDs detection status.
**enable** - Specifies that the legacy PDs detection status will be enabled.
**disable** - Specifies that the legacy PDs detection status will be disabled and can't detect the legacy PDs signal.

### Restrictions

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

### Example

To configure the PoE system-wise setting:

```
DGS-3620-28SC:admin#config poe system power_limit 250 power_disconnect_method
deny_low_priority_port
Command: config poe system power_limit 250 power_disconnect_method
deny_low_priority_port


Success.


DGS-3620-28SC:admin#
```

## 77-3 show poe ports

### Description

This command is used to display the settings and actual values of the PoE port.

**Note:** This command is only available to Switches in the DGS-3620 Series that support Power over Ethernet.

### Format

**show poe ports {<portlist>}**

### Parameters

**ports** - (Optional) Specifies the list of ports to be displayed here.
**<portlist>** - Enter the list of ports, used for the display, here.

If no parameter is specified, the system will display the status for all the ports.

### Restrictions

None.

### Example

To display PoE port configurations on port 1 to 6:

```
DGS-3620-28PC:admin# show poe ports 1:1-1:6
Command: show poe ports 1:1-1:6

Port   State     Priority  Power Limit(mW)     Time Range
       Class     Power(mW) Voltage(decivolt)   Current(mA)
       Status
===============================================================================
1:1    Enabled   Critical  4000 (Class 1)
       0         0         0                   0
       OFF  : Interim state during line detection
1:2    Enabled   Critical  4000 (Class 1)
       0         0         0                   0
       OFF  : Interim state during line detection
1:3    Enabled   Critical  4000 (Class 1)
       0         0         0                   0
       OFF  : Interim state during line detection
1:4    Enabled   Critical  4000 (Class 1)
       0         0         0                   0
       OFF  : Interim state during line detection
1:5    Enabled   Low       7000 (User-defined)
       0         0         0                   0
       OFF  : Interim state during line detection
1:6    Enabled   Low       7000 (User-defined)
       0         0         0                   0
       OFF  : Interim state during line detection

DGS-3620-28PC:admin#
```

## 77-4 show poe system

### Description

This command is used to display the settings and actual values of the whole PoE system.

**Note:** This command is only available to Switches in the DGS-3620 Series that support Power over Ethernet.

### Format

**show poe system {units <unitlist>}**

## Parameters

**units** - (Optional) Specifies the unit list, that will be displayed, here.
**<unitlist>** - Enter the unit list, used for this display, here.

If no parameter is specified, the system will display the status of all the supported PoE units in the system.

## Restrictions

None.

## Example

To display the PoE system:

```
DGS-3620-28PC:admin# show poe system units 1
Command: show poe system units 1

Unit: 1 PoE System Information
---------------------------------------------------
Power Limit                : 760(Watts)
Power Consumption          : 0(Watts)
Power Remained             : 371(Watts)
Power Disconnection Method : Deny Next Port
Detection Legacy PD        : Disabled

If Power Disconnection Method is set to deny next port, then the system can not
utilize out of its maximum power capacity. The maximum unused watt is 19W.

DGS-3620-28PC:admin#
```

# Chapter 78 Power Saving Commands

|  |
|---|
| **config power_saving** {state [enable \| disable] \| length_detection [enable \| disable]} |
| **show power_saving** |

## 78-1 config power_saving

### Description

This command is used to configure the power saving for the system. By default, the power saving mode is enabled and the length detection mode is disabled. The power saving length detection function applies to the Gigabit ports with copper media.

The power is saved by the following mechanisms. When the port has no link partner, the port automatically turns off and wakes up once a second to send a single link pulse. When the port is turned off, a simple receive energy-detect circuit is continuously monitoring energy on the cable. At the moment when energy is detected, the port turns on fully per IEEE specification requirements. The power saving function is performed while no link is detected and it will not affect the port capabilities while it is link up.

When the port is link up, for shorter cable, the power consumption can 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 cable length and still maintain error free applications from both sides of the link. This mechanism will only be supported when the hardware supports the cable diagnostics function.

### Format

**config power_saving {state [enable | disable] | length_detection [enable | disable]}**

### Parameters

|  |
|---|
| **state** - (Optional) Configure the power saving state to enable or disable. The default value is enable.<br>**enable** - Enable the power saving feature.<br>**disable** - Disable the power saving feature. |
| **length_detection** - Configure the length detection state to enable or disable. The default value is disable.<br>**enable** - Enable the length detection feature.<br>**disable** - Disable the length detection feature. |

### Restrictions

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

### Example

To configure power saving:

```
DGS-3620-28SC:admin# config power_saving state enable
Command: config power_saving state enable

Success

DGS-3620-28SC:admin#
```

## 78-2 show power_saving

### Description

This command is used to display power saving information.

### Format

**show power_saving**

### Parameters

None.

### Restrictions

None.

### Example

To display power saving information:

```
DGS-3620-28SC:admin#show power_saving
Command: show power_saving

Power Saving State: Enabled

Length Detection State: Enabled

DGS-3620-28SC:admin#
```

# Chapter 79 Precision Time Protocol (PTP) Commands

| |
|---|
| **enable ptp** |
| **disable ptp** |
| **config ptp mode** [boundary \| p2p_transparent \| e2e_transparent] |
| **config ptp transport protocol** [ethernet \| udp] |
| **config ptp clock domain_number** <value 0-127> {unit <unit_id 1-12>} {domain_name <string 1-32>} |
| **config ptp boundary** {priority1 <value 0-255> \| priority2 <value 0-255>}(1) |
| **config ptp ports** [<portlist> \| all] state [enable \| disable] |
| **config ptp boundary ports** [<portlist> \| all] {announce [interval <sec 1-16> \| timeout <value 2-10>] \| sync_interval [half_second \| <sec 1-2>] \| delay_req_interval <value 0-5> \| pdelay_req_interval <sec 1-32> \| delay_mechanism [e2e \| p2p]}(1) |
| **config ptp p2p_transparent ports** [<portlist> \| all] pdelay_req_interval <sec 1-32> |
| **show ptp** |
| **show ptp clock** |
| **show ptp clock parent** |
| **show ptp ports** [<portlist> \| all] |
| **show ptp boundary** {ports [<portlist> \| all]} |
| **show ptp p2p_transparent ports** [<portlist> \| all] |
| **show ptp foreign_master_records ports** [<portlist> \| all] |

## 79-1 enable ptp

### Description

This command is used to enable the PTP function globally. The device will enter the P2P-transparent clock mode when the PTP global state is enabled. The PTP function can only work when both the global PTP state and the per port PTP state are enabled.

### Format

**enable ptp**

### Parameters

None.

### Restrictions

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

### Example

To enable the PTP function globally:

```
DGS-3620-28SC:admin# enable ptp
Command: enable ptp

Success.

DGS-3620-28SC:admin#
```

## 79-2 disable ptp

### Description

This command is used to disable the PTP function globally. When the PTP function is disabled, all switch ports will forward the PTP packets according to the multicast filtering configuration.

### Format

**disable ptp**

### Parameters

None.

### Restrictions

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

### Example

To disable the PTP function globally:

```
DGS-3620-28SC:admin# disable ptp
Command: disable ptp

Success.

DGS-3620-28SC:admin#
```

## 79-3 config ptp mode

### Description

This command is used to configure the PTP device type of the switch. The switch supports three PTP device types, which the user can set globally.

A Boundry Clock:

- Has multiple Precision Time Protocol (PTP) ports in a domain and maintains the timescale used in the domain.
- Can serve as the time source and can synchronize with another clock.
- Device type can choose to use the delay request-response mechanism or the peer delay mechanism to measure the propagation delay between the PTP ports.

A clock that provides Precision Time Protocol (PTP) event transit time information also provides corrections for the propagation delay of the link. The link, in this case, is connected to the port that is receiving the PTP event messages. Ports on peer-to-peer transparent clocks use the peer delay mechanism to calculate the propagation delay between PTP ports.

An End-to-End Transparent Clock supports the use of an end-to-end delay measurement mechanism between the slave clock and the master clock. Ports on end-to-end transparent clocks are independent of propagation delay mechanisms.

### Format

**config ptp mode [boundary | p2p_transparent | e2e_transparent]**

### Parameters

**boundary** - Specifies the Switch as a Boundary Clock.

**p2p_transparent** - Specifies the Switch as a Peer-to-Peer Transparent Clock.

**e2e_transparent** - Specifies the Switch as an End-to-End Transparent Clock.

### Restrictions

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

### Example

To specify the switch as a peer-to-peer transparent clock:

```
DGS-3620-28SC:admin# config ptp mode p2p_transparent
Command: config ptp mode p2p_transparent

Success.

DGS-3620-28SC:admin#
```

## 79-4 config ptp transport protocol

### Description

This command is used to specify the transport protocol that will be used for the communication path.

### Format

**config ptp transport protocol [ethernet | udp]**

### Parameters

**ethernet** - Specifies the transport protocol of PTP as IEEE802.3 Ethernet.

**udp** - Specifies the transport protocol of PTP as UDP over IPv4.

### Restrictions

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

### Example

To specify the transport protocol of PTP as IEEE802.3 Ethernet frames:

```
DGS-3620-28SC:admin# config ptp transport protocol ethernet
Command: config ptp transport protocol ethernet

Success.

DGS-3620-28SC:admin#
```

## 79-5 config ptp clock domain_number

### Description

This command is used to configure the PTP clock common attribute of the domain number. The domain number is used to identify the PTP domain that the PTP clock is working on. If the domain number of the received PTP message is not identical to the domain number of the local device, the PTP message shall be forwarded according to the multicast filtering configuration.

### Format

**config ptp clock domain_number <value 0-127> {unit <unit_id 1-12>} {domain_name <string 1-32>}**

### Parameters

**domain_number** - Specifies the domain attribute of the local clock. All PTP messages, data sets, state machines, and all other PTP entities are always associated with a particular domain number.
**<value 0-127>** - Enter the domain number used here. This value must be between 0 and 127. The default value is 0.

**unit** - (Optional) specifies the domain number for a specified unit. If not specified, the domain configurations applies to the local unit. If the unit is not present, the configuration is ignored.
**<unit_id 1-12>** - Enter the unit ID used here. This value must be between 1 and 12.

**domain_name** - (Optional) Specifies the domain name for a specified domain number.
**<string 1-32>** - Enter the domain name used here. This name can be up to 32 characters long.

### Restrictions

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

### Example

To configure the domain number of the PTP clock as 1 and assign a domain name of internal_domain on the local unit, when the stacking mode is disabled:

```
DGS-3620-28SC:admin# config ptp clock domain_number 1 domain_name
internal_domain
Command: config ptp clock domain_number 1 domain_name internal_domain

Success.

DGS-3620-28SC:admin#
```

To configure the domain number of the PTP clock as 1 and assign a domain name of internal_domain for the unit 1, when the stacking mode is enabled.

```
DGS-3620-28SC:admin#config ptp clock domain_number 1 unit 1 domain_name
internal_domain
Command: config ptp clock domain_number 1 unit 1 domain_name internal_domain

Success.

DGS-3620-28SC:admin#
```

## 79-6 config ptp boundary

### Description

This command is used to configure the PTP boundary clock attributes and requires at least one parameter to execute.

### Format

**config ptp boundary {priority1 <value 0-255> | priority2 <value 0-255>}(1)**

### Parameters

**priority1** - (Optional) Specifies that the priority 1 attribute is used in the execution of the best master clock algorithm. Lower values take precedence.
**<value 0-255>** - Enter the priority 1 value used here. This value must be between 0 and 255.

**priority2** - (Optional) Specifies that the priority 2 attribute is used in the execution of the best master clock algorithm. Lower values take precedence. In the event that the operation of the BMC algorithm fails to order the clocks based on the values of priority1, the clock's class, and the clock's accuracy; the priority2 attribute will allow the creation of lower values compared to the other devices.
**<value 0-255>** - Enter the priority 2 value used here. This value must be between 0 and 255.

### Restrictions

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

### Example

To configure the priority1 value of the boundary clock as 127:

```
DGS-3620-28SC:admin# config ptp boundary priority1 127
Command: config ptp boundary priority1 127

Success.

DGS-3620-28SC:admin#
```

## 79-7 config ptp ports

### Description

This command is used to configure the per port state of the PTP clock.

PTP port active state should meet the following three conditions:

- The global PTP state is enabled.
- The port PTP state is enabled.
- The port is not blocked, if the stp state is enabled.

### Format

**config ptp ports [<portlist> | all] state [enable | disable]**

### Parameters

**ports** - Specifies the list of port used for this configuration.
**<portlist>** - Enter the list of port used for this configuration here.
**all** - Specifies that all the ports will be used for this configuration.

**state** - Specifies the port state of the PTP clock function.
**enable** - Specifies that the port state of the PTP clock function will be enabled.
**disable** - Specifies that the port state of the PTP clock function will be disabled.

### Restrictions

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

### Example

To enable PTP on ports 1:1-1:4:

```
DGS-3620-28SC:admin# config ptp ports 1:1-1:4 state enable
Command: config ptp ports 1:1-1:4 state enable

Success.

DGS-3620-28SC:admin#
```

## 79-8 config ptp boundary ports

### Description

This command is used to configure the attributes of the PTP boundary clock. The configuration takes effect when the PTP device is a boundary type.

### Format

**config ptp boundary ports [<portlist> | all] {announce [interval <sec 1-16> | timeout <value 2-10>] | sync_interval [half_second | <sec 1-2>] | delay_req_interval <value 0-5> | pdelay_req_interval <sec 1-32> | delay_mechanism [e2e | p2p]}(1)**

## Parameters

**ports** - Specifies the list of port used for this configuration.
**<portlist>** - Enter the list of port used for this configuration here.
**all** - Specifies that all the ports will be used for this configuration.

**announce** - (Optional) Specifies that the announce options will be configured.
**interval** - Specifies the mean time interval between successive announce messages. In line with the IEEE 1588 protocol, the value of the announce interval is represented as the logarithm to the base 2 of this time measured in seconds. If the input is not allowed, then the input is automatically adjusted to allow the bigger and closest value. The value of the announce interval should be uniform throughout a domain. If the announce interval of one port changes, the announce interval of all the ports must be changed automatically to be consistent.
**<sec 1-16> -** Enter the interval value used here. This value must be between 1 and 16 seconds.
**timeout -** Specifies the announce interval number that has to pass without receiving an Announce message before the occurrence of the ANNOUNCE_RECEIPT_TIMEOUT_EXPIRES event. This value multiplied by the announce interval value is equal to the interval time of the announce receipt timeout. The value of the interval time of the announce receipt timeout should be uniform throughout a domain. If the value of one port is changed, the value of all ports must be changed automatically to be consistent.
**<value 2-10>** - Enter the timeout value used here. This value must be between 2 and 10 seconds.

**sync_interval** - (Optional) Specifies the mean time interval between successive Sync messages.
**half_second** - Specifies that the syncronization interval will be set to half a second.
**<sec 1-2>** - Enter the syncronization interval value used here. This value must be between 1 and 2.

**delay_req_interval** - (Optional) Specifies the permitted mean time interval between successive delay request messages which are sent by a slave to a specific port on the master. This mean time interval value is determined and advertised by a master.
**<value 0-5>** - Enter the delay required interval value used here. This value must be between 0 and 5.

**pdelay_req_interval** - (Optional) Specifies the permitted mean time interval between successive pdelay_request messages.
**<sec 1-32>** - Enter the permitted mean time interval value used here. This value must be between 1 and 32 seconds.

**delay_mechanism** - (Optional) Specifies the mechanism for measuring the propagation delay time of an event message.
**e2e** - E2E indicates that the port is configured to use the delay request-response mechanism.
**p2p** - P2P indicates that the port is configured to use the peer delay mechanism.

## Restrictions

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

## Example

To configure the announce interval attribute of ports 1-4 to 3 seconds:

```
DGS-3620-28SC:admin# config ptp boundary ports 1:1-1:4 announce interval 3
Command: config ptp boundary ports 1:1-1:4 announce interval 3

The announce interval is automatically adjusted to 4.

Success.

DGS-3620-28SC:admin#
```

To configure the announce timeout attribute of ports 1-4 to 4 seconds, which is about 4*Announce interval:

```
DGS-3620-28SC:admin# config ptp boundary ports 1:1-1:4 announce timeout 4
Command: config ptp boundary ports 1:1-1:4 announce timeout 4

Success.

DGS-3620-28SC:admin#
```

To configure the sync_interval attribute of the all the PTP ports to 2 seconds:

```
DGS-3620-28SC:admin# config ptp boundary ports all sync_interval 2
Command: config ptp boundary ports all sync_interval 2

Success.

DGS-3620-28SC:admin#
```

If the sync_interval is 0.5 seconds, then the delay_req_interval attribute of the all PTP ports is configured as 0.

```
DGS-3620-28SC:admin# config ptp boundary ports all delay_req_interval 0
Command: config ptp boundary ports all delay_req_interval 0

Success.

DGS-3620-28SC:admin#
```

To configure the pdelay_req_interval attribute of the all PTP ports as 5 seconds:

```
DGS-3620-28SC:admin# config ptp boundary ports all pdelay_req_interval 5
Command: config ptp boundary ports all pdelay_req_interval 5

The pdelay_req interval is automatically adjusted to 8.

Success.

DGS-3620-28SC:admin#
```

To configure the delay_mechanism attribute of the all the PTP ports as P2P:

```
DGS-3620-28SC:admin# config ptp boundary ports all delay_mechanism p2p
Command: config ptp boundary ports all delay_mechanism p2p

Success.

DGS-3620-28SC:admin#
```

## 79-9 config ptp p2p_transparent ports

### Description

This command is used to configure the pdelay_request message attribute for the message interval of the P2P transparent clock.

### Format

**config ptp p2p_transparent ports [<portlist> | all] pdelay_req_interval <sec 1-32>**

### Parameters

| |
|---|
| **ports** - Specifies the list of port used for this configuration.<br>**<portlist>** - Enter the list of port used for this configuration here.<br>**all** - Specifies that all the ports will be used for this configuration. |
| **pdelay_req_interval** - Specifies the permitted mean time interval between successive messages.<br>**<sec 1-32>** - Enter the permitted mean time interval value used here. This value must be between 1 and 32. |

### Restrictions

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

### Example

To configure the pdelay_req_interval attribute of all the PTP ports to 4 seconds:

```
DGS-3620-28SC:admin# config ptp p2p_transparent ports all pdelay_req_interval 4
Command: config ptp p2p_transparent ports all pdelay_req_interval 4

Success.

DGS-3620-28SC:admin#
```

## 79-10 show ptp

### Description

This command is used to display the configured attributes of PTP on the switch.

### Format

**show ptp**

### Parameters

None.

### Restrictions

None.

### Example

To show the global PTP configuration:

```
DGS-3620-28SC:admin# show ptp
Command: show ptp

PTP State Setting                : Enabled
PTP Mode Setting                 :  Boundary Clock
PTP Transport Protocol Setting   :  UDP
PTP Clock Domain Number Setting  :  0
PTP Clock Domain Name Setting    :  Internal Domain

DGS-3620-28SC:admin#
```

## 79-11 show ptp clock

### Description

This command is used to display the active attributes of the PTP clock.

### Format

**show ptp clock**

### Parameters

None.

### Restrictions

None.

### Example

To show the active attributes of the boundary clock:

```
DGS-3620-28SC:admin# show ptp clock
Command: show ptp clock

PTP State                    : Enabled
PTP Clock Mode               :  Boundary Clock
PTP Transport Protocol       :  UDP
PTP Clock Domain Number      :  1
PTP Clock Domain Name        :  internal_domain
PTP Clock Identity           :  ACDE48FFFE6789AB
PTP Priority 1               :  128
PTP Priority 2               :  128
PTP Clock Class              :  187
PTP Steps Removed            :  2
PTP Last Offset              :  +130ns
PTP Mean Path Delay          :  1 second
PTP Enabled Ports            : 1:1-1:4, 2:1-2:4

DGS-3620-28SC:admin#
```

To show the properties of the Peer-to-Peer transparent clock:

```
DGS-3620-28SC:admin# show ptp clock
Command: show ptp clock

PTP State                      : Enabled
PTP Clock Mode                 : Peer-to-Peer Transparent Clock
PTP Transport Protocol         : UDP
PTP Clock Domain Number        : 1
PTP Clock Domain Name          : internal_domain
PTP Clock Delay Mechanism      :  P2P
PTP Clock Identity             :  ACDE48FFFE6789AC
PTP Enabled Ports              : 1:1-1:4, 2:1-2:4

DGS-3620-28SC:admin#
```

To show the properties of the boundary clock of all stacking devices, when the stacking mode is enabled:

```
DGS-3620-28SC:admin# show ptp clock
Command: show ptp clock

Box ID: 1

PTP State                    : Enabled
PTP Clock Mode               :  Boundary Clock
PTP Transport Protocol       :  UDP
PTP Clock Domain Number      :  1
PTP Clock Domain Name        :  internal_domain
PTP Clock Identity           :  ACDE4823456789AB
PTP Priority 1               :  128
PTP Priority 2               :  128
PTP Clock Class              :  187
PTP Steps Removed          :  2
PTP Last Offset            :  +110 ns
PTP Mean Path Delay        :  120 second
PTP Enabled Ports          : 1:1-1:4

Box ID: 2

PTP State                  : Enabled
PTP Clock Mode             :  Boundary Clock
PTP Transport Protocol     :  UDP
PTP Clock Domain Number    :  1
PTP Clock Domain Name      :  internal_domain
PTP Clock Identity         :  ACDE482345678910
PTP Priority 1             :  128
PTP Priority 2             :  128
PTP Clock Class            :  187
PTP Steps Removed          :  3
PTP Last Offset            :  +130ns
PTP Mean Path Delay        :  140 second
PTP Enabled Ports          : 2:1-2:4

DGS-3620-28SC:admin#
```

## 79-12 show ptp clock parent

### Description

This command is used to display the active attributes of the PTP parent clock.

### Format

**show ptp clock parent**

### Parameters

None.

### Restrictions

None.

### Example

To show the active attributes of the boundary clock parent:

```
DGS-3620-28SC:admin# show ptp clock parent
Command: show ptp clock parent

PTP Parent Port Identity         :  ACDE48FFFE6789AB
PTP Parent Port Number           :  3
PTP Grandmaster Identity         :  ACDE48FFFE9789AD
PTP Grandmaster Clock Class      :  13
PTP Grandmaster Clock Accuracy   :  100ns
PTP Grandmaster Priority 1       :  120
PTP Grandmaster Priority 2       :  127

DGS-3620-28SC:admin#
```

The display of the active attributes of the boundary clock parent when the synchronization does not complete:

```
DGS-3620-28SC:admin# show ptp clock parent
Command: show ptp clock parent

The boundary clock has not completed synchronization.

DGS-3620-28SC:admin#
```

The display of the active attributes of the boundary clock parent when the boundary clock is the grandmaster clock:

```
DGS-3620-28SC:admin# show ptp clock parent
Command: show ptp clock parent

The grandmaster clock does not have this attribute.

DGS-3620-28SC:admin#
```

To show the parent and grandmaster properties of the transparent clock:

```
DGS-3620-28SC:admin# show ptp clock parent
Command: show ptp clock parent

The transparent clock does not have this attribute.

DGS-3620-28SC:admin#
```

To show the active attributes of the boundary clock parent of all stacking devices, when the stacking mode is enabled.

```
DGS-3620-28SC:admin# show ptp clock parent
Command: show ptp clock parent

Box ID: 1

PTP Parent Port Identity         :  ACDE4823456789AB
PTP Parent Port Number           :  3
PTP Grandmaster Identity         :  ACDE4823659789AD
PTP Grandmaster Clock Class      :  13
PTP Grandmaster Clock Accuracy   :  100ns
PTP Grandmaster Priority 1       :  120
PTP Grandmaster Priority 2       :  127

Box ID: 2

PTP Parent Port Identity         :  ACDE482345678910
PTP Parent Port Number           :  5
PTP Grandmaster Identity         :  ACDE4823659789AD
PTP Grandmaster Clock Class      :  13
PTP Grandmaster Clock Accuracy   :  100ns
PTP Grandmaster Priority 1       :  120
PTP Grandmaster Priority 2       :  127

DGS-3620-28SC:admin#
```

## 79-13 show ptp ports

### Description

This command is used to display the active attributes of the special PTP ports on the switch.

### Format

**show ptp ports [<portlist> | all]**

### Parameters

**ports** - Specifies the list of port used for this display.
**<portlist>** - Enter the list of port used for this display here.
**all** - Specifies that all the ports will be used for this display.

### Restrictions

None.

### Example

To show the active attributes for special ports 1:1-1:4 of the boundary clock:

```
DGS-3620-28SC:admin# show ptp ports 1:1-1:4
Command: show ptp ports 1:1-1:4

The active attributes:

DM  : Delay Mechanism
AI  : Announce Interval
ART : Announce Receipt Timeout
SI  : Synchronization Interval
DRIM: Delay_Request Interval-Master
DRIS: Delay_Request Interval-Slave
PDRI: Pdelay_Request Interval
PMPD: Peer Mean Path Delay

Port    Role     DM    AI    ART   SI    DRIM   DRIS  PDRI  PMPD   State
1:1     Master   P2P   2     8     1      1       2      4     1      Enabled
1:2     Slave    E2E   1     8     0.5    2       8      8     0      Enabled
1:3     Master   P2P   2     8     1      8       4      8     1      Enabled
1:4     Master   P2P   2     8     1      32      16    16     0      Enabled

DGS-3620-28SC:admin#
```

To show the active attributes for special ports 1:1-1:4 of the p2p-transparent clock:

```
DGS-3620-28SC:admin# show ptp ports 1:1-1:4
Command: show ptp ports 1:1-1:4

The active attributes:

PDRI : Pdelay_Request Interval
PMPD : Peer Mean Path Delay

Port      PDRI    PMPD    State
1:1        4       1       Enabled
1:2        8       0       Disabled
1:3        8       1       Enabled
1:4        16      1       Enabled

DGS-3620-28SC:admin#
```

## 79-14 show ptp boundary

### Description

This command is used to display the configured attributes of the boundary clock or the configured attributes of the boundary clock’s special ports.

### Format

**show ptp boundary {ports [<portlist> | all]}**

### Parameters

**ports** – (Optional) Specifies the list of port used for this display.
 **<portlist>** - Enter the list of port used for this display here.
 **all** - Specifies that all the ports will be used for this display.

### Restrictions

None.

### Example

To show the configured attributes of the boundary clock:

```
DGS-3620-28SC:admin# show ptp boundary
Command: show ptp boundary

PTP Priority1 Setting           :  128
PTP Priority2 Setting           :  127

DGS-3620-28SC:admin#
```

To show the configured attributes of special ports 1:1-1:4 of the boundary clock:

```
DGS-3620-28SC:admin# show ptp boundary ports 1:1-1:4
Command: show ptp boundary ports 1:1-1:4

The attribute configurations of the ports of boundary:

DM   : Delay Mechanism
AI   : Announce Interval
CART : The Coefficient of Announce Receipt Timeout
SI   : Synchronization Interval
EDRI : The Exponent of Delay_Request Interval
PDRI : Pdelay_Request Interval

Port     DM     AI   CART    SI   EDRI    PDRI      State
1:1      P2P    2      3      1     1       8       Enabled
1:2      E2E    1      2      0.5   0      16       Enabled
1:3      P2P    2      5      1     2       8       Enabled
1:4      P2P    2      6      1     4       4       Enabled

DGS-3620-28SC:admin#
```

## 79-15 show ptp p2p_transparent ports

### Description

This command is used to display the configured attributes of the P2P transparent clock’s special ports.

### Format

**show ptp p2p_transparent ports [<portlist> | all]**

### Parameters

**ports** - Specifies the list of port used for this display.
**<portlist>** - Enter the list of port used for this display here.
**all** - Specifies that all the ports will be used for this display.

### Restrictions

None.

### Example

To show the configured attributes of special ports 1:1-1:4 of the p2p_transparent clock:

```
DGS-3620-28SC:admin# show ptp p2p_transparent ports 1:1-1:4
Command: show ptp p2p_transparent ports 1:1-1:4

The attribute configuration of the p2p_transparent ports:

PDRI : Pdelay_Request Interval

Port     PDRI         State
1:1       8           Enabled
1:2       16          Enabled
1:3       8           Enabled
1:4       4           Disabled

DGS-3620-28SC:admin#
```

## 79-16 show ptp foreign_master_records ports

### Description

This command is used to display the current foreign master data set records of the boundary clock’s special ports.

### Format

**show ptp foreign_master_records ports [<portlist> | all]**

### Parameters

**ports** - Specifies the list of port used for this display.
**<portlist>** - Enter the list of port used for this display here.
**all** - Specifies that all the ports will be used for this display.

### Restrictions

None.

### Example

To show the current records of the foreign master data set for special ports 1:1-1:3 of the boundary clock:

```
DGS-3620-28SC:admin#show ptp foreign_master_records ports all
Command: show ptp foreign_master_records ports all


 FM Port Identity         : The clock identity of the Foreign Master Port
 FM Port Number           : The port number of the Foreign Master Port
 FM Announce Messages     : The numbers of Foreign Master announce messages

Port     FM Port Identity    FM Port Number    FM Announce Messages
1:1      001655fffe200000    1:7               4
2:1      001655fffe200000    1:8               4

DGS-3620-28SC:admin#
```

# Chapter 80 Protocol VLAN Commands

**create dot1v_protocol_group** group_id <id> group_name <name 32>

**config dot1v_protocol_group** [group_id <id> | group_name <name 32>] [add protocol [ethernet_2 | ieee802.3_snap | ieee802.3_llc] <protocol_value> | delete protocol [ethernet_2 | ieee802.3_snap | ieee802.3_llc] <protocol_value>]

**delete dot1v_protocol_group** [group_id <id> | group_name <name 32>| all]

**show dot1v_protocol_group** {group_id <id> | group_name <name 32>}

**config port dot1v ports** [<portlist> | all] [add protocol_group [group_id <id> | group_name <name 32>] [vlan <vlan_name 32> | vlanid <id>] {priority <value 0-7>} | delete protocol_group [group_id <id> | all]]

**show port dot1v** {ports <portlist>}

## 80-1 create dot1v_protocol_group

### Description

This command is used to create a protocol group for the protocol VLAN function.

### Format

**create dot1v_protocol_group group_id <id> group_name <name 32>**

### Parameters

**group_id** - Specify the ID of the protocol group which is used to identify a set of protocols.
**<id>** - The ID range is between 1 and 16.

**group_name** - Specify the name of the protocol group.
**<name 32>** - Specify the name of the protocol group. The maximum length is 32 characters.

### Restrictions

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

### Example

To create a protocol group:

```
DGS-3620-28SC:admin#create dot1v_protocol_group group_id 4 group_name
General_Group
Command: create dot1v_protocol_group group_id 4 group_name General_Group


Success.
DGS-3620-28SC:admin#
```

## 80-2 config dot1v_protocol_group

### Description

This command is used to add a protocol to a protocol group. The selection of a protocol can be a pre-defined protocol type or a user defined protocol.

### Format

**config dot1v_protocol_group [group_id <id> | group_name <name 32>] [add protocol [ethernet_2 | ieee802.3_snap | ieee802.3_llc] <protocol_value> | delete protocol [ethernet_2 | ieee802.3_snap | ieee802.3_llc] <protocol_value>]**

### Parameters

| |
|---|
| **group_id** - Specify the ID of the protocol group which is used to identify a set of protocols.<br>**<id>** - The ID range is between 1 and 16. |
| **group_name** - Specify the name of the protocol group.<br>**<name 32> -** Specify the name of the protocol group. The maximum length is 32 characters. |
| **add protocol** - Specify the protocol to be added. Depending on the frame type, the octet string will have one of the following values below. The form of the input is 0x0 to 0xffff.<br>**ethernet_2** - This is a 16-bit (2-octet) hex value. Example: IPv4 is 800, IPv6 is 86dd, ARP is 806, etc.<br>**ieee802.3_snap** - This is a 16-bit (2-octet) hex value. Example: IPv4 is 800, IPv6 is 86dd, ARP is 806, etc.<br>**ieee802.3_llc** - This is the 2-octet IEEE 802.2 Link Service Access Point (LSAP) pair: first octet for Destination Service Access Point (DSAP) and second octet for Source. |
| **<protocol_value>** - Specify the protocol value used to identify a protocol of the frame type. The form of the input is 0x0 to 0xffff. Depending on the frame type, the octet string will have one of the following values: For Ethernet II, this is a 16-bit (2-octet) hex value. For example, IPv4 is 800, IPv6 is 86dd, ARP is 806, etc. For IEEE802.3 SNAP, this is this is a 16-bit (2-octet) hex value. For IEEE802.3 LLC, this is the 2-octet IEEE 802.2 Link Service Access Point (LSAP) pair. The first octet is for Destination Service Access Point (DSAP) and the second octet is for Source. |
| **delete protocol** - Specify the protocol to be deleted. Depending on the frame type, the octet string will have one of the following values below. The form of the input is 0x0 to 0xffff.<br>**ethernet_2** - This is a 16-bit (2-octet) hex value. Example: IPv4 is 800, IPv6 is 86dd, ARP is 806, etc.<br>**ieee802.3_snap** - This is a 16-bit (2-octet) hex value. Example: IPv4 is 800, IPv6 is 86dd, ARP is 806, etc.<br>**ieee802.3_llc** - This is the 2-octet IEEE 802.2 Link Service Access Point (LSAP) pair: first octet for Destination Service Access Point (DSAP) and second octet for Source. |
| **<protocol_value>** - Specify the protocol value used to identify a protocol of the frame type. The form of the input is 0x0 to 0xffff. Depending on the frame type, the octet string will have one of the following values: For Ethernet II, this is a 16-bit (2-octet) hex value. For example, IPv4 is 800, IPv6 is 86dd, ARP is 806, etc. For IEEE802.3 SNAP, this is this is a 16-bit (2-octet) hex value. For IEEE802.3 LLC, this is the 2-octet IEEE 802.2 Link Service Access Point (LSAP) pair. The first octet is for Destination Service Access Point (DSAP) and the second octet is for Source. |

### Restrictions

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

### Example

To add a protocol IPv6 to protocol group 4:

```
DGS-3620-28SC:admin# config dot1v_protocol_group group_id 4 add protocol
ethernet_2 86dd
Command: config dot1v_protocol_group group_id 4 add protocol ethernet_2 86dd

Success.
DGS-3620-28SC:admin#
```

To delete a protocol IPv6 from protocol group ID 4:

```
DGS-3620-28SC:admin# config dot1v_protocol_group_group_id 4 delete protocol
ethernet_2 86dd
Command: config dot1v_protocol_group group_id 4 delete protocol ethernet_2 86dd

Success.
DGS-3620-28SC:admin#
```

## 80-3 delete dot1v_protocol_group

### Description

This command is used to delete a protocol group.

### Format

**delete dot1v_protocol_group [group_id <id> | group_name <name 32> | all]**

### Parameters

| |
|---|
| **group_id** - Specify the group ID to be deleted.<br>**<id>** - Specify the group ID to be deleted. |
| **group_name** - Specify the name of the protocol group to be deleted.<br>**<name 32>** - Specify the name of the protocol group to be deleted. The maximum length is 32 characters. |
| **all** - Specify to delete all protocol groups. |

### Restrictions

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

### Example

To delete protocol group ID 4:

```
DGS-3620-28SC:admin# delete dot1v_protocol_group group_id 4
Command: delete dot1v_protocol_group group_id 4

Success.
DGS-3620-28SC:admin#
```

## 80-4 show dot1v_protocol_group

### Description

This command is used to display the protocols defined in protocol groups.

### Format

**show dot1v_protocol_group {group_id <id> | group_name <name 32>}**

### Parameters

| |
|---|
| **group_id** - (Optional) Specify the group ID to be displayed.<br>**<id>** - Specify the group ID to be displayed. |
| **group_name** - (Optional) Specify the name of the protocol group.<br>**<name 32>** - Specify the name of the protocol group. The maximum length is 32 characters. |

**Note:** If no parameter is specified, all configured protocol groups will be displayed

### Restrictions

None.

### Example

To display protocol group ID 4:

```
DGS-3620-28SC:admin# show dot1v_protocol_group group_id 4
Command: show dot1v_protocol_group group_id 4

Protocol        Protocol             Frame Type             Protocol
Group ID       Group Name                                     Value
---------     ---------------      ------------        ------------
4            General Group         EthernetII             86dd

Total Entries: 1

DGS-3620-28SC:admin#
```

## 80-5 config port dot1v ports

### Description

This command is used to assign the VLAN for untagged packets ingress from the portlist 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 <id>| group_name <name 32>] [vlan <vlan_name 32> | vlanid <id>] {priority <value 0-7>} | delete protocol_group [group_id <id> | all]]**

### Parameters

**<portlist>** - Specify a range of ports to apply this command.

**all** - Specify all ports.

**add protocol_group** - Specify to add a protocol group.
**group_id** - Specify the group ID of the protocol group.
**<id>**- Specify the group ID of the protocol group.
**group_name** - Specify the name of the protocol group.
**<name 32>** - Specify the name of the protocol group. The maximum length is 32 characters.

**vlan** - Specify the VLAN that is to be associated with this protocol group on this port.
**<vlan_name 32>** - Specify the VLAN that is to be associated with this protocol group on this port. The maximum length is 32 characters.

**vlanid** - Specify the VLAN ID.
**<id>** - Specify the VLAN ID.

**priority** - Specify the priority to be associated with the packet which has been classified to the specified VLAN by the protocol.
**<value 0-7>** - Specify a value between 0 and 7.

**delete protocol_group** - Specify to delete a protocol group.
**group_id** – Specify the group ID to be deleted.
**<id>** - Specify the group ID.
**all** – Specify all groups.

### Restrictions

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

### Example

To configure the group ID 4 on port 3 to be associated with VLAN 2:

```
DGS-3620-28SC:admin# config port dot1v ports 3 add protocol_group group_id 4
vlan VLAN2
Command: config port dot1v ports 3 add protocol_group group_id 4 vlan VLAN2


Success.
DGS-3620-28SC:admin#
```

## 80-6 show port dot1v

### Description

This command is used to display the VLAN to be associated with untagged packets 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>** - Specify a range of ports to be displayed.

**Note:** If no parameter is specified, information for all ports will be displayed.

### Restrictions

None.

### Example

To display the protocol VLAN information for ports 1 to 2:

```
DGS-3620-28SC:admin# show port dot1v ports 1-2
Command: show port dot1v ports 1-2

Port: 1
 Protocol Group ID     VLAN Name                           Protocol Priority
 -------------------   ---------------------------------   -----------------
 1                     default                             -

 Port: 2
 Protocol Group ID     VLAN Name                           Protocol Priority
 -------------------   ---------------------------------   -----------------
 1                     default                             1

Total Entries  :  2

DGS-3620-28SC:admin#
```

# Chapter 81 QoS Commands

| |
|---|
| **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 0-7> {{min_rate [no_limit \| <value 64-10240000>]} max_rate [no_limit \| <value 64-10240000>]}(1) |
| **show per_queue bandwidth_control** {<portlist>} |
| **config scheduling** {ports [<portlist> \| all]} <class_id 0-7> [strict \| weight <value 1-127>] |
| **config scheduling_mechanism** {ports [<portlist> \| all]} [strict \| wrr] |
| **show scheduling** {<portlist>} |
| **show scheduling_mechanism** {<portlist>} |
| **config 802.1p user_priority** {ports [<portlist> \| all]} <priority 0-7> <class_id 0-7> |
| **show 802.1p user_priority** {<portlist>} |
| **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 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>] |
| **show dscp map** { <portlist> } [dscp_priority \| dscp_dscp] {dscp <dscp_list>} |

## 81-1 config bandwidth_control

### Description

This command is used to set the maximum limit for port bandwidth.

### Format

**config bandwidth_control [<portlist> | all] {rx_rate [no_limit | <value 64-10240000>] | tx_rate [no_limit | <value 64-10240000>]}(1)**

### Parameters

| |
|---|
| **<portlist>** - Specify a range of ports to be configured.<br>**all** - Specify all ports. |
| **rx_rate** - (Optional) Specify the limitation of receive data rate.<br>**no_limit** - Specify to indicate there is no limit on port rx bandwidth.<br>**<value 64-10240000>** - Specify an integer value from 64 to 10240000 to set a maximum limit in Kbits/sec. The specified bandwidth limit may be equaled but not exceeded. This exact logical limit or token value is hardware determined. Note: 1 Kbit = 1000 bits, 1 Gigabit = 1000*1000 Kbits. Actual rate = (inputted rate/ 64) * 64. |
| **tx_rate** - (Optional) Specify the limitation of transmit data rate.<br>**no_limit** - Specify to indicate there is no limit on port tx bandwidth.<br>**<value 64-10240000>** - Specify an integer value from 64 to 10240000 to set a maximum limit in Kbits/sec. The specified bandwidth limit may be equaled but not exceeded. This exact logical limit or token value is hardware determined. Actual rate = (inputted rate/ 64) * 64. |

### Restrictions

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

### Example

To configure port bandwidth:

```
DGS-3620-28SC:admin#config bandwidth_control 1-10 tx_rate 1024
Command: config bandwidth_control 1-10 tx_rate 1024

Success.

DGS-3620-28SC:admin#
```

## 81-2 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 the RADIUS server has assigned the bandwidth, then the RADIUS-assigned bandwidth will be the effective bandwidth.

### Format

**show bandwidth_control {<portlist>}**

### Parameters

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

**Note:** If no parameter is specified, the system will display all port bandwidth configurations.

### Restrictions

None.

### Example

To display the port bandwidth control table for ports 1 to 2:

```
DGS-3620-28SC:admin#show bandwidth_control 1-2
Command: show bandwidth_control 1-2

Bandwidth Control Table

Port   RX Rate      TX Rate       Effective RX        Effective TX
      (Kbit/sec)    (Kbit/sec)    (Kbit/sec)          (Kbit/sec)
----  ----------    ----------    ----------------    ----------------
```

```
 1    No Limit      No Limit      No Limit            No Limit
 2    No Limit      No Limit      No Limit            No Limit

DGS-3620-28SC:admin#
```

## 81-3 config per_queue bandwidth_control

### Description

This command is used to set the bandwidth control for each specific egress queue on specified ports. The maximum rate limits the bandwidth. When specified, packets transmitted from the queue will not exceed the specified limit even if extra bandwidth is available. The specification of maximum rate is effective regardless of whether the queue is operating in strict or Shaped Deficit Weighted Round Robin (SDWRR) mode.

### 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>** - Specify a range of ports to be configured.
**all** - Specify to set all ports in the system. If no parameter is specified, the system will set all the ports.

**<cos_id_list 0-7>** - Specify a list of priority queues. The priority queue number ranges from 0 to 7.

**min_rate** - Specify that one of the parameters below will be applied to the minimum rate that the class specified above will be allowed to transmit packets at.
**no_limit** - Indicates there is no limit on egress queue of specified port bandwidth.
**<value 64-10240000>** - Specify an integer value from 64 to 10240000 to set a minimum limit in Kbits/sec. The specified bandwidth limit may be equaled but not exceeded. The exact logical limit or token value is hardware determined. Note: 1 Kbit = 1000 bits, 1 Gigabit = 1000*1000 Kbits. Actual rate = (inputted rate/ 64) * 64.

**max_rate** - Specify one of the parameters below will be applied to the maximum rate that the class specified above will be allowed to transmit packets at.
**no_limit** - Indicates there is no limit on egress queue of specified port bandwidth.
**<value 64-10240000>** - Specify an integer value from 64 to 10240000 to set a maximum limit in Kbits/sec. The specified bandwidth limit may be equaled but not exceeded. The exact logical limit or token value is hardware determined. Note: 1 Kbit = 1000 bits, 1 Gigabit = 1000*1000 Kbits. Actual rate = (inputted rate/ 64) * 64.

### Restrictions

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

### Example

To configure the maximum rate to be 100 on queue 1 for ports 1 to 10:

```
DGS-3620-28SC:admin#config per_queue bandwidth_control ports 1-10 1 max_rate
100
Command: config per_queue bandwidth_control ports 1-10 1 max_rate 100

```

```
 Granularity: TX: 64. Actual Rate: MAX: 64.

Success.

DGS-3620-28SC:admin#
```

## 81-4 show per_queue bandwidth_control

### Description

This command is used to display the bandwidth control setting of per egress queue for each port.

### Format

**show per_queue bandwidth_control {<portlist>}**

### Parameters

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

### Restrictions

None

### Example

To display the port bandwidth control table for port 1:

```
DGS-3620-28SC:admin#show per_queue bandwidth_control 1
Command: show per_queue bandwidth_control 1

Queue Bandwidth Control Table On Port: 1

Queue     Min Rate(Kbit/sec)     Max Rate(Kbit/sec)
0         No Limit               No Limit
1         No Limit               No Limit
2         64                     1024
3         64                     No Limit
4         No Limit               No Limit
5         No Limit               No Limit
6         No Limit               No Limit
7         No Limit               No Limit

DGS-3620-28SC:admin#
```

## 81-5 config scheduling

### Description

This command is used to configure the traffic scheduling mechanism for each CoS queue.

### Format

**config scheduling {ports [<portlist> | all]} <class_id 0-7> [strict | weight <value 1-127>]**

### Parameters

**ports** - (Optional) Specifies the range of ports to be configured.
**<portlist>** - Enter the list of ports here.
**all** - Specifies that all the ports will be used.

**<class_id 0-7>** - Specifies the 8 hardware priority queues that the config scheduling command will apply to. The eight hardware priority queues are identified by a number from 0 to 7 with the 0 queue being the lowest priority.

**strict** - Specifies that the queue will operate in strict mode.

**weight** - Specifies the weight value for weighted round robin. The queue will operate in WRR mode if the port mode is WRR. It will operate in strict mode if the port mode is strict.
**<value 1-127>** - Enter the weight value here. This value must be between 1 and 127.

### Restrictions

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

### Example

To configure the traffic scheduling on CoS queue 0 with a maximum packet value of 10:

```
DGS-3620-28SC:admin#config scheduling 0 weight 10
Command: config scheduling 0 weight 10

Success.

DGS-3620-28SC:admin#
```

To configure the traffic scheduling on CoS queue 1, with a weight value of 25, on port 1:10:

```
DGS-3620-28SC:admin# config scheduling ports 1:10 1 weight 25
Command: config scheduling ports 1:10 1 weight 25

Success.

DGS-3620-28SC:admin#
```

## 81-6 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) Specifies the range of ports to be configured.
  **<portlist>** - Enter the list of ports here.
  **all** - Specifies that all the ports will be used.

**strict** - Specifies that all the queues will operate in strict mode.

**wrr** - Specifies that each queue will operate based on their weight settings.

### Restrictions

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

### Example

To configure the traffic scheduling mechanism for each CoS queue:

```
DGS-3620-28SC:admin# config scheduling_mechanism strict
Command: config scheduling_mechanism strict

Success.

DGS-3620-28SC:admin#
```

To configure the traffic scheduling mechanism for the CoS queue on port 1:1:

```
DGS-3620-28SC:admin# config scheduling_mechanism ports 1:1 strict
Command: config scheduling_mechanism ports 1:1 strict

Success.

DGS-3620-28SC:admin#
```

## 81-7 show scheduling

### Description

This command is used to display the current traffic scheduling parameters.

### Format

**show scheduling {<portlist>}**

### Parameters

**<portlist>** - (Optional) Specifies the range of ports to be displayed.

### Restrictions

None.

### Example

To display the traffic scheduling parameters for each CoS queue:

```
DGS-3620-28SC:admin#show scheduling
Command: show scheduling

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

QOS Output Scheduling On Port: 2
Class ID  Weight
--------  ------
Class-0   1
Class-1   2
Class-2   3
Class-3   4
Class-4   5
Class-5   6
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

To display the traffic scheduling parameters for each CoS queue on port 1:1.

```
DGS-3620-28SC: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-3620-28SC:admin#
```

## 81-8 show scheduling_mechanism

### Description

This command is used to display the traffic scheduling mechanism.

## Format

**show scheduling_mechanism {<portlist>}**

## Parameters

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

## Restrictions

None.

## Example

To display the scheduling mechanism for all ports:

```
DGS-3620-28SC: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
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

To show the scheduling mechanism on ports 1-10:

```
DGS-3620-28SC:admin#show scheduling_mechanism 1-10
Command: show scheduling_mechanism 1-10

Port    Mode
-----   ------
1       Strict
2       Strict
3       Strict
4       Strict
5       Strict
6       Strict
7       Strict
8       Strict
9       Strict
10      Strict

DGS-3620-28SC:admin#
```

## 81-9 config 802.1p user_priority

### Description

This command is used to configure the way by which the switch will map an incoming packet, based on its 802.1p user priority, to one of the eight available hardware priority queues on the switch. The switch's default is to map the following incoming 802.1p user priority values to the eight hardware priority queues. The suggested mapping is shown in the following table. Users can change this mapping by specifying the 802.1p user priority to assign to the <class_id>.

| Priority in Frames | Priority Queue of ASIC | Remark |
|---|---|---|
| 0 | 2 | Mid-Low |
| 1 | 0 | Lowest |
| 2 | 1 | Lowest |
| 3 | 3 | Mid-Low |
| 4 | 4 | Mid-High |
| 5 | 5 | Mid-High |
| 6 | 6 | Highest |
| 7 | 7 | Highest |

### Format

**config 802.1p user_priority {ports [<portlist> | all]} <priority 0-7> <class_id 0-7>**

### Parameters

**ports** - (Optional) Specifies that port used for this configuration.
**portlist** - Specifies the range of ports to be configured.
**all** - Specifies that all the ports will be used for this configuration.

**<priority 0-7>** - Specify the 802.1p user priority to associate with the <class_id> (the number of the hardware queue).

**<class_id 0-7>** - Specify the number of the switch's hardware priority queue. The switch has eight hardware priority queues available. They are numbered between 0 (the lowest priority) and 7 (the highest priority).

### Restrictions

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

### Example

To configure an 802.1p user priority of 1 map to class ID of 3:

```
DGS-3620-28SC:admin#config 802.1p user_priority 1 3
Command: config 802.1p user_priority 1 3

Success.

DGS-3620-28SC:admin#
```

## 81-10 show 802.1p user_priority

### Description

This command is used to display 802.1p user priority.

### Format

**show 802.1p user_priority {<portlist>}**

### Parameters

**<portlist>** - (Optional) Specifies the range of ports to be configured.

### Restrictions

None.

### Example

To display the 802.1p user priority:

```
DGS-3620-28SC:admin#show 802.1p user_priority
Command: show 802.1p user_priority

 QoS Class of Traffic

 Port 1
     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>

 Port 2
     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-3620-28SC:admin#
```

## 81-11 config 802.1p default_priority

### Description

This command is used to specify default priority for untagged packets received on a port of the switch.

### Format

**config 802.1p default_priority [<portlist> | all ] <priority 0-7>**

### Parameters

| |
|---|
| **<portlist>** - Specify 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 beginning and end of the port list range are separated by a dash.<br>**all** - Specify that the command applies to all ports on the switch. |
| **<priority 0-7>** - Specify a priority value (0 to 7) to assign to untagged packets received by the switch or a range of ports on the switch. |

### Restrictions

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

### Example

To configure an 802.1p default priority settings of 5 on all Switch ports:

```
DGS-3620-28SC:admin#config 802.1p default_priority all 5
Command: config 802.1p default_priority all 5

Success.

DGS-3620-28SC:admin#
```

## 81-12 show 802.1p default_priority

### Description

This command is used to display the current default priority settings on the switch. The default priority can also be assigned by the RADIUS server through the authentication process. Authentication with the RADIUS server can be either per port or per user. For per port authentication, the priority assigned by the RADIUS server will be the default priority of the effective port. For per user authentication, the priority assigned by RADIUS will not be the effective port default priority, as the will priority associated with MAC address will be assigned. Note that only devices supporting MAC-based VLANs can provide per user authentication.

### Format

**show 802.1p default_priority {<portlist>}**

### Parameters

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

**Note:** If no parameter is specified, the system will display all ports with 802.1p default priority.

### Restrictions

None.

### Example

To display 802.1p default priority for ports 1 to 4:

```
DGS-3620-28SC:admin#show 802.1p default_priority 1-4
Command: show 802.1p default_priority 1-4

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

DGS-3620-28SC:admin#
```

## 81-13 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-3620-28SC:admin#enable hol_prevention
Command: enable hol_prevention

```

```
Success.

DGS-3620-28SC:admin#
```

## 81-14 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-3620-28SC:admin#disable hol_prevention
Command: disable hol_prevention

Success.

DGS-3620-28SC:admin#
```

## 81-15 show hol_prevention

### Description

This command is used to display the 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-3620-28SC:admin#show hol_prevention
Command: show hol_prevention

Device HOL Prevention State: Enabled

DGS-3620-28SC:admin#
```

## 81-16 config dscp trust

### Description

This command is used to enable or disable the DSCP trust state on specified ports.

### Format

**config dscp trust [<portlist>|all] state [enable | disable]**

### Parameters

| |
|---|
| **<portlist>** - Specifies a range of ports to be displayed. |
| **all** - Specifies that the command will apply to all ports on the switch. |
| **state** - Enables/disables DSCP trust. By default, DSCP trust is disabled. |

### Restrictions

Only Administrator and Operator level users can issue this command.

### Example

To enable DSCP trust on ports 1:1-1:8:

```
DGS-3620-28SC:admin#config dscp trust port 1:1-1:8 state enable
Command: config dscp trust port 1:1-1:8 state enable

Success.

DGS-3620-28SC:admin#
```

## 81-17 show dscp trust

### Description

This command is used to display the DSCP trust state.

### Format

**show dscp trust {<portlist>}**

### Parameters

**<portlist>** - A range of ports to display. If not specifying any ports, the DSCP trust status for all ports on the switch will be displayed.

### Restrictions

Only Administrator, Operator level users can issue this command.

### Example

To enable DSCP trust on ports 1:1-1:8:

```
DGS-3620-28SC:admin#show dscp_trust 1:1-1:8
Command: show dscp_trust 1:1-1:8

Port    DSCP-Trust
-----   -----------
1:1     Disabled
1:2     Disabled
1:3     Disabled
1:4     Disabled
1:5     Enabled
1:6     Enabled
1:7     Enabled
1:8     Enabled

DGS-3620-28SC:admin #
```

## 81-18 config dscp map

### Description

This command is used to configure the mapping of DSCP to a priority.

### Format

**config dscp map [<portlist> | all] [ dscp_priority <dscp_list> to <priority 0-7> | dscp_dscp <dscp_list> to <dscp 0-63>]**

### Parameters

**<portlist>** - A range of ports to display. If not specifying any ports, the DSCP trust status for all ports on the switch will be displayed.

**all** - Specifies that the command applies to all ports on the switch.

**dscp_priority** - Specifies a list of DSCP values to be mapped to a specific priority.
**<dscp_list>** - Enter the dscp list number here.
**<priority 0-7>** - Specifies the result priority of a mapping.

**dscp_dscp** - Specifies a list of DSCP values to be mapped to a specific DSCP.
**<dscp_list>** - Enter the dscp list number here.
**<dscp 0-63>** - Specifies the result DSCP of mapping.

### Restrictions

Only Administrator, Operator level users can issue this command.

### Example

In the case of a product supporting per-port DSCP mapping configuration, to configure the mapping of DSCP priority 1 to priority 1:

```
DGS-3620-28SC:admin#config dscp map 1:1-1:8 dscp_priority 1 to priority 1
Command: config dscp map 1:1-1:8 dscp_priority 1 to priority 1

Success.

DGS-3620-28SC:admin#
```

In the case of a product supporting global DSCP mapping configuration, to configure the global mapping of DSCP priority 1 to priority 1:

```
DGS-3620-28SC:admin#config dscp map dscp_priority 1 to priority 1
Command: config dscp map dscp_priority 1 to priority 1

Success.

DGS-3620-28SC:admin#
```

## 81-19 show dscp map

### Description

This command is used to display the DSCP map configuration parameters.

### Format

**show dscp map { <portlist> } [dscp_priority | dscp_dscp] {dscp <dscp_list>}**

### Parameters

**<portlist>** - The range of ports to display. If no parameter is specified, the DSCP mapping for all ports will be displayed. If the project only support global configuration, the global information will be displayed.

**dscp_priority** - Specifies the list of DSCP values to be mapped to a specific priority.

**dscp_dscp** - Specifies the list of DSCP values to be mapped to a specific DSCP.

**dscp** - This specifies the DSCP value that will be mapped.
**<dscp_list>** - Enter the dscp list number here.

### Restrictions

Only Administrator and Operator level users can issue this command.

### Example

In the case of a product supporting per port configuration.,To show the DSCP map configuration on port 1:1.

```
DGS-3620-28SC:admin#show dscp map 1 dscp_priority
Command: show dscp map 1 dscp_priority

DSCP to 802.1p Priority Mapping:

Port 1
DSCP 0-7 is mapped to 0
DSCP 8-15 is mapped to 1
DSCP 16-23 is mapped to 2
DSCP 24-31 is mapped to 3
DSCP 32-39 is mapped to 4
DSCP 40-47 is mapped to 5
DSCP 48-55 is mapped to 6
DSCP 56-63 is mapped to 7
```

In the case of a product only supporting global configuration. To show the DSCP map configuration:

```
DGS-3620-28SC: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-3620-28SC:admin#
```

# Chapter 82 Q-in-Q Command

**enable qinq**

**disable qinq**

**show qinq**

**config qinq ports** [<portlist> | all] {role [uni | nni] | missdrop [enable | disable] | outer_tpid <hex 0x1-0xffff> | use_inner_priority [enable | disable] | add_inner_tag [<hex 0x1-0xffff> | disable]}(1)

**config qinq inner_tpid** <hex 0x1-0xffff>

**show qinq inner_tpid**

**show qinq ports** {<portlist>}

**create vlan_translation ports** [<portlist> | all] [add cvid <vidlist> | replace cvid <vlanid 1-4094>] svid <vlanid 1-4094> {priority <priority 0-7>}

**delete vlan_translation ports** [<portlist> | all] {cvid <vidlist>}

**show vlan_translation** {[ports <portlist> | cvid <vidlist>]}

## 82-1 enable qinq

### Description

This command is used to enable Q-in-Q. When Q-in-Q 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 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. In Q-in-Q mode, GVRP protocol will employ the reserve address 01-80-C2-00-00-0D. The default setting of Q-in-Q is disabled.

### Format

**enable qinq**

### Parameters

None.

### Restrictions

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

### Example

To enable Q-in-Q:

```
DGS-3620-28SC:admin#enable qinq
Command: enable qinq

Success.

DGS-3620-28SC:admin#
```

## 82-2 disable qinq

### Description

This command is used to disable Q-in-Q. When Q-in-Q 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 Administrator, Operator and Power-User level users can issue this command.

### Example

To disable Q-in-Q:

```
DGS-3620-28SC:admin#disable qinq
Command: disable qinq

Success.

DGS-3620-28SC:admin#
```

## 82-3 show qinq

### Description

This command is used to display the global Q-in-Q status.

### Format

**show qinq**

### Parameters

None.

### Restrictions

None.

### Example

To display Q-in-Q:

```
DGS-3620-28SC:admin#show qinq
Command: show qinq

QinQ Status : Enabled

DGS-3620-28SC:admin#
```

## 82-4 config qinq ports

### Description

This command is used to configure Q-in-Q port parameters on this Switch.

### Format

**config qinq ports [<portlist> | all] {role [uni | nni] | missdrop [enable | disable] | outer_tpid <hex 0x1-0xffff> | use_inner_priority [enable | disable] | add_inner_tag [<hex 0x1-0xffff> | disable]}(1)**

### Parameters

**<portlist>** - Specify a range of ports to configure.

**all** - Specify to configure all ports.

**role** - Specify the port role in Q-in-Q mode.
  **uni** - The port is connecting to the customer network.
  **nni** - The port is connecting to the service provider network.

**missdrop** - Enable or disable the tagged packet drop that does not match any assignment rule in the Q-in-Q profile.
  **enable** - Enable miss drop of ports.
  **disable** - Disable miss drop of ports.

**outer_tpid** - Specify the outer-TPID of a port.
  **<hex 0x1-0xffff>** - Specify the outer-TPID of a port.

**use_inner_priority** - Specify whether to use the priority in the C-VLAN tag as the priority in the S-VLAN tag. By default, the setting is disabled.
  **enable** - Specifies that the use of the inner priority will be enabled.
  **disable** - Specifies that the use of the inner priority will be disabled.

**add_inner_tag** - Specify whether to add 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.
  **<hex 0x1-0xffff>** - Enter the inner tag value here.
  **disable** - Specifies that only the s-tag will be added for ingress untagged packets.

### Restrictions

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

### Example

To configure ports 1 to 4 as NNI ports and set the TPID to 0x88A8:

```
DGS-3620-28SC:admin#config qinq ports 1-4 role nni outer_tpid 0x88a8
Command: config qinq ports 1-4 role nni outer_tpid 0x88a8
```

```
Success.

DGS-3620-28SC:admin#
```

## 82-5 config qinq inner_tpid

### Description

The command is used to configure the inner TPID of the system. The inner TPID is used to decide if the ingress packet is c-tagged. Inner tag TPID is per system configurable. This command is used in the ‘per-system’ TPID configuration.

### Format

**config qinq inner_tpid <hex 0x1-0xffff>**

### Parameters

**<hex 0x1-0xffff>** - Enter the Inner-TPID of the system used here.

### Restrictions

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

### Example

To configure the inner TPID in the system to 0x9100:

```
DGS-3620-28SC:admin# config inner_tpid 0x9100
Command: config inner_tpid 0x9100

Success.

DGS-3620-28SC:admin#
```

## 82-6 show qinq inner_tpid

### Description

This command is used to display the inner TPID of the system.

### Format

**show qinq inner_tpid**

### Parameters

None.

### Restrictions

None.

### Example

To display the inner TPID of the system:

```
DGS-3620-28SC:admin#show qinq inner_tpid
Command: show qinq inner_tpid

 Inner TPID: 0x8100

DGS-3620-28SC:admin#
```

## 82-7 show qinq ports

### Description

This command is used to display the Q-in-Q configuration of ports.

### Format

**show qinq ports {<portlist>}**

### Parameters

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

**Note:** If no parameter specified, the system will display port information for all ports.

### Restrictions

None.

### Example

To display the Q-in-Q mode for ports 1 to 2:

```
DGS-3620-28SC:admin#show qinq ports  1-2
Command: show qinq ports 1-2



Port ID:    1
---------------------------------------------------------
  Role:                        NNI
  Miss Drop:                   Disabled
  Outer Tpid:                  0x8100
  Use Inner Priority:          Disabled
  Add Inner Tag:               Disabled

Port ID:    2
```

```
--------------------------------------------------------
  Role:                     NNI
  Miss Drop:                Disabled
  Outer Tpid:               0x8100
  Use Inner Priority:       Disabled
  Add Inner Tag:            Disabled

DGS-3620-28SC:admin#
```

## 82-8 create vlan_translation ports

### Description

This command is used to create translation relationships between C-VLAN and S-VLAN. This setting will not be effective when the Q-in-Q mode is disabled. This configuration is only effective for a UNI port. At the 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>** - Specify a range of ports on which the C-VLAN will be translated to S-VLAN.

**all** - Specify to configure all ports.

**add cvid** - Specify to add a S-tag before C-tag for incoming packets with a specific CVID.
**<vidlist>** - Specify the CVID (or list) to be matched for incoming packets.

**replace cvid** - Specify to replace the original C-tag to a new S-tag for incoming packets with a specific CVID.
**<vlanid 1-4094>** - Specify the CVID to be matched for incoming packets.

**svid** - Specify the SVID of the S-tag to be added or replaced to the packets.
**<vlanid 1-4094>** - Specify the SVID between 1 and 4094.

**priority** - (Optional) Specify a 802.1p priority of the S-Tag between 0 and 7. If the priority is NOT specified, 802.1p priority of S-Tag will be assigned by the priority in C-tag.
**<priority 0-7>** - Specify a 802.1p priority of the S-Tag between 0 and 7.

### Restrictions

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

### Example

To replace the C-tag by the S-tag with SVID 200 and priority in C-tag, if the incoming packet with CVID 20:

```
DGS-3620-28SC:admin#create vlan_translation ports 1 replace cvid 20 svid 200
Command: create vlan_translation ports 1 replace cvid 20 svid 200

 Success.
```

```
DGS-3620-28SC:admin#
```

To add S-tag with SVID 300 and 802.1p priority 5, if incoming packet with CVID 30:

```
DGS-3620-28SC:admin#create vlan_translation ports 1 add cvid 30 svid 300
priority 5
Command: create vlan_translation ports 1 add cvid 30 svid 300 priority 5

 Success.

DGS-3620-28SC:admin#
```

## 82-9 delete vlan_translation ports

### Description

This command is used to delete translation relationships between C-VLAN and S-VLAN.

### Format

**delete vlan_translation ports [<portlist> | all] {cvid <vidlist>}**

### Parameters

| |
|---|
| **<portlist>** - Specify the ports to be deleted. |
| **all** - Specify to delete all ports. |
| **cvid** - (Optional) Specify to delete the rules for the specified CVIDs. If the CVID is not specified, all rules configured for the port will be deleted.<br>**<vidlist>** - Specify a range of VLAN IDs. |

### Restrictions

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

### Example

To delete a VLAN translation rule on ports 1 to 4:

```
DGS-3620-28SC:admin#delete vlan_translation ports 1-4
Command: delete vlan_translation ports 1-4

Success.

DGS-3620-28SC:admin#
```

## 82-10 show vlan_translation

### Description

This command is used to display existing C-VLAN based VLAN translation rules.

## Format

**show vlan_translation {[ports <portlist> | cvid <vidlist>]}**

## Parameters

**ports** - Specify to display the C-VLAN based VLAN translation rules of the ports.
**<portlist>** - Specify a range of ports to be displayed.

**cvid** - Specify to display the rules for the specified CVIDs.
**<vidlist>** - Specify a range of VLAN IDs.

## Restrictions

None.

## Example

To display VLAN translation for ports 1 and 2:

```
DGS-3620-28SC:admin#show vlan_translation ports 1-2
Command: show vlan_translation ports 1-2

 Port   CVID   SVID  Action  Priority
-----  -----  ----- ------- --------
1      10     100    Add       4
1      20     100    Add       5
1      30     200    Add       6
2      10     100    Add       7
2      20     100    Add       1

 Total Entries: 5

DGS-3620-28SC:admin#
```

# Chapter 83 Routing Information Protocol (RIP) Command List

**enable rip**

**config rip** [ipif <ipif_name 12> | all] {authentication [enable <password 16> | disable] | tx_mode [disable | v1_only | v1_compatible | v2_only] | rx_mode [v1_only | v2_only | v1_or_v2 | disable] | state [enable | disable]}(1)

**config rip timers** {update <sec 5-65535> | timeout <sec 5-65535> | garbage_collection <sec 5-65535>} (1)

**disable rip**

**show rip** {ipif <ipif_name 12>}

## 83-1 enable rip

### Description

This command is used to enable RIP for the switch. The default setting is disabled.

### Format

**enable rip**

### Parameters

None.

### Restrictions

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

### Example

To enable RIP:

```
DGS-3620-28SC:admin# enable rip
Command: enable rip

Success.

DGS-3620-28SC:admin#
```

## 83-2 config rip

### Description

This command is used to configure the RIP settings for one or more IP interfaces.

### Format

**config rip [ipif <ipif_name 12> | all] {authentication [enable <password 16> | disable] | tx_mode [disable | v1_only | v1_compatible | v2_only] | rx_mode [v1_only | v2_only | v1_or_v2 | disable] | state [enable | disable]}(1)**

### Parameters

**ipif_name** - Specifies the IP interface name used for this configuration.
**<ipif_name 12>** - Enter the IP interface name used here. This name can be up to 12 characters long.
**all** - Specifies that all the IP interfaces will be used in this configuration.

**authentication** - (Optional) Specifies to set the state of authentication.
**enable** - Specifies that the authentication state will be enabled.
**<password 16>** - When the authentication state is enabled, enter the password used here. This value can be up to 16 characters long.
**disable** - Specifies that the authentication state will be disabled.

**tx_mode** - (Optional) Specifies the RIP transmission mode.
**disable** - Specifies to prevent the transmission of RIP packets.
**v1_only** - Specifies that only RIP version 1 format packets will be transmitted.
**v1_compatible** - Specifies to transmit RIP version 2 format packets to the broadcast address.
**v2_only** - Specifies that only RIP version 2 format packets will be transmitted.

**rx_mode** - (Optional) Specifies the RIP receive mode.
**v1_only** - Specifies to receive RIP version 1 format packets.
**v2_only** - Specifies to receive RIP version 2 format packets.
**v1_or_v2** - Specifies to receive both v1 and v2 packet.
**disable** - Specifies that the receiving of RIP packets will be prevented.

**state** - (Optional) Specifies that the RIP state will be enabled or disabled. If the state is disabled, then RIP packets will not be either transmitted or received by the interface. The network configured on this interface will not be in the RIP database.
**enable** - Specifeies that the RIP state will be enabled.
**disable** - Specifeies that the RIP state will be disabled.

### Restrictions

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

### Example

To change the RIP receive mode for the IP interface System:

```
DGS-3620-28SC:admin# config rip ipif System rx_mode v1_only
Command: config rip ipif System rx_mode v1_only

Success.

DGS-3620-28SC:admin#
```

## 83-3 config rip timers

### Description

This command is used to configure RIP timers.

### Format

**config rip timers {update <sec 5-65535> | timeout <sec 5-65535> | garbage_collection <sec 5-65535>} (1)**

### Parameters

**update** - (Optional) Specifies the value of the rate at which RIP updates are sent.
**<sec 5-65535>** - Enter the update value used here. This value must be between 5 and 65535 seconds.

**timeout** - (Optional) Specifies the value of the time after which a RIP route is declared to be invalid.
**<sec 5-65535>** - Enter the timeout value used here. This value must be between 5 and 65535 seconds.

**garbage_collection** - (Optional) Specifies the value of the time for which a RIP route will be kept before it is removed from routing table.
**<sec 5-65535>** - Enter the garbage collection value used here. This value must be between 5 and 65535 seconds.

### Restrictions

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

### Example

To configure the RIP timers:

```
DGS-3620-28SC:admin# config rip timers update 60 timeout 360 garbage_collection
240
Command: config rip timers update 60 timeout 360 garbage_collection 240

Success.

DGS-3620-28SC:admin#
```

## 83-4 disable rip

### Description

This command is used to disable RIP for the switch.

### Format

**disable rip**

### Parameters

None.

### Restrictions

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

### Example

To disable RIP:

```
DGS-3620-28SC:admin# disable rip
Command: disable rip

Success.

DGS-3620-28SC:admin#
```

## 83-5 show rip

### Description

This command is used to display the RIP configuration for one or all the IP interfaces.

### Format

**show rip {ipif <ipif_name 12>}**

### Parameters

| |
|---|
| **ipif** - (Optional) Specifies the IP interface name used for this configuration.<br>**<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 RIP configuration and statistics for all the IP interface. |

### Restrictions

None.

### Example

To display RIP configuration and statistics for all IP interface.

```
DGS-3620-28SC:admin#show rip
Command: show rip

RIP Global State            : Enabled
Update Time                 : 120 seconds
Timeout Time                : 300 seconds
Garbage Collection Time     : 150 seconds

RIP Interface Settings

Interface     IP Address         TX Mode    RX Mode       Authen-    State
                                                          tication
------------- ------------------ ---------- ------------- ---------- -----
System        2.2.2.2/8          V1 Comp.   V1 or V2      Enabled    Disabled
n40           40.0.0.2/16        V1 Comp.   V1 or V2      Enabled    Enabled
n90           90.0.0.2/16        V1 Comp.   V1 or V2      Enabled    Enabled
n100          100.0.0.2/16       V1 Comp.   V1 or V2      Enabled    Enabled

Total Entries : 4

DGS-3620-28SC:admin#
```

# Chapter 84 RIPng Commands

**enable ripng**

**disable ripng**

**show ripng** {ipif <ipif_name 12>}

**config ripng** {method [no_horizon | split_horizon | poison_reverse] | update <sec 5-65535> | expire <sec 1-65535> | garbage_collection <sec 1-65535>} (1)

**config ripng ipif** [<ipif_name 12> | all] {state [enable | disable] | metric <value 1-15>} (1)

## 84-1 enable ripng

### Description

This command is used to enable RIPng globally for the Switch.

### Format

**enable ripng**

### Parameters

None.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

To enable RIPng globally:

```
DGS-3620-28SC:admin# enable ripng
Command: enable ripng

Success.

DGS-3620-28SC:admin#
```

## 84-2 disable ripng

### Description

This command is used to disable RIPng globally for the Switch.

### Format

**disable ripng**

### Parameters

None.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

To disable RIPng globally:

```
DGS-3620-28SC:admin# disable ripng
Command: disable ripng

Success.

DGS-3620-28SC:admin#
```

## 84-3 show ripng

### Description

This command is used to display the RIPng state on all or specified interfaces.

### Format

**show ripng {ipif <ipif_name 12>}**

### Parameters

**ipif** - (Optional) Specifies the RIPng IP interface name to be displayed.

**<ipif_name 12>** - Enter the RIPng IP interface name to be displayed here. This name can be up to 12 characters long.

### Restrictions

None. (EI Mode Only Command)

### Example

To display RIPng configurations:

```
DGS-3620-28SC:admin#show ripng
Command: show ripng

 Global State:          Disabled
 Method:                Split Horizon
 Update Time:           30 seconds
 Expire Time:           180 seconds
 Garbage Collection Time:               120 seconds

 Interface              State                   Metric
-----------------------------------------------------

Total Entries : 0

DGS-3620-28SC:admin#
```

## 84-4 config ripng

### Description

This command is used to configure the RIPng algorithm and timer.

### Format

**config ripng {method [no_horizon | split_horizon | poison_reverse] | update <sec 5-65535> | expire <sec 1-65535> | garbage_collection <sec 1-65535>} (1)**

### Parameters

**method** - (Optional) Specifies the method used.
- **no_horizon** - Specifies to configure not use any horizon.
- **split_horizon** - Specifies to configure use a basic split horizon.
- **poison_reverse** - Specifies to configure to use a split horizon with poison reverse.

**update** - (Optional) Specifies the value of the update timer.
- **<sec 5-65535>** - Enter the update timer value used here. This value must be between 5 and 65535 seconds.

**expire** - (Optional) Specifies the interval when the update expires.
- **<sec 1-65535>** - Enter the expire value used here. This value must be between 1 and 65535 seconds.

**garbage_collection** - (Optional) Specifies the value of the garbage-collection timer.
- **<sec 1-65535>** - Enter the garbage-collection timer value used here. This value must be between 1 and 65535 seconds.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

To configure the RIPng method as poison reverse:

```
DGS-3620-28SC:admin# config ripng method poison_reverse
Command: config ripng method poison_reverse

Success.

DGS-3620-28SC:admin#
```

## 84-5 config ripng ipif

### Description

This command is used to specify the RIPng state and metric value for one or all interfaces

### Format

**config ripng ipif [<ipif_name 12> | all] {state [enable | disable] | metric <value 1-15>} (1)**

### Parameters

**ipif** - Specifies the RIPng IP interface name to be configured.
**<ipif_name 12>** - Enter the RIPng IP interface name to be configured here. This name can be up to 12 characters long.
**all** - Specifies that all the RIPng IP interfaces will be used.

**state** - (Optional) Specifies the RIPng state of the specifies IP interface.
**enable** - Specifies that the RIPng state on the specified interface will be enabled.
**disable** - Specifies that the RIPng state on the specified interface will be disabled.

**metric** - (Optional) Specifies the cost value of an interface. The RIPng route that was learned from the interface will add this value as a new route metric.
**<value 1-15>** - Enter the metric value used here. This value must be between 1 and 15. The default value is 1.

### Restrictions

Only Administrator, Operator and Power-User level users can issue this command. (EI Mode Only Command)

### Example

To enable the RIPng interface state:

```
DGS-3620-28SC:admin# config ripng ipif System state enable
Command: config ripng ipif System state enable

Success.

DGS-3620-28SC:admin#
```

# Chapter 85 RSPAN Commands

**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>]}

## 85-1 enable rspan

### Description

This command is used to enable RSPAN globally.

### Format

**enable rspan**

### Parameters

None.

### Restrictions

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

### Example

To enable RSPAN globally:

```
DGS-3620-28SC:admin#enable rspan
Command: enable rspan

Success.

DGS-3620-28SC:admin#
```

## 85-2 disable rspan

### Description

This command is used to disable RSPAN globally.

### Format

**disable rspan**

### Parameters

None.

### Restrictions

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

### Example

To disable the RSPAN globally:

```
DGS-3620-28SC:admin#disable rspan
Command: disable rspan

Success.

DGS-3620-28SC:admin#
```

## 85-3 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>** - Specify the VLAN name.

**vlan_id** - Create the RSPAN VLAN by VLAN ID.
**<vlanid 1-4094>** - Specify the VLAN ID between 1 and 4094.

### Restrictions

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

### Example

To create an RSPAN VLAN entry by VLAN name “v2”:

```
DGS-3620-28SC:admin#create rspan vlan vlan_name v2
Command: create rspan vlan vlan_name v2

Success.

DGS-3620-28SC:admin#
```

To create an RSPAN VLAN entry by VLAN ID “3”:

```
DGS-3620-28SC:admin#create rspan vlan vlan_id 3
Command: create rspan vlan vlan_id 3

Success.

DGS-3620-28SC:admin#
```

## 85-4 delete rspan vlan

### Description

This command is used to delete an RSPAN VLAN.

### 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>** - Specify the VLAN name.

**vlan_id** - Specify the RSPAN VLAN by VLAN ID.
**<vlanid 1-4094>** - Specify the VLAN ID between 1 and 4094.

### Restrictions

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

### Example

To delete an RSPAN VLAN entry by VLAN name “v2”:

```
DGS-3620-28SC:admin#delete rspan vlan vlan_name v2
Command: delete rspan vlan vlan_name v2

Success.

DGS-3620-28SC:admin#
```

To delete an RSPAN VLAN entry by VLAN ID “3”:

```
DGS-3620-28SC:admin#delete rspan vlan vlan_id 3
Command: delete rspan vlan vlan_id 3

Success.

DGS-3620-28SC:admin#
```

## 85-5 config rspan vlan

### Description

This command is used by the source switch to configure the source setting for the RSPAN VLAN. The redirect command 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.

### 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>** - Specify the VLAN name.
**vlan_id** - Specify the RSPAN VLAN by VLAN ID.
**<vlanid 1-4094>** - Specify 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>** - Specify 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.
**mirror_group_id** - The mirror group identify that specify which mirror session used for RSPAN source function. If the mirror group is not specified when configuring the mirror ports, the mirror group 1 will be the default group.
**<value 1-4>** - Enter the mirror group ID value here. This value must be between 1 and 4.
**add** - (Optional) Specify to add source ports.
**delete** - (Optional) Specify to delete source ports.

**ports** - (Optional) Specify source port list to add to or delete from the RSPAN source.
**<portlist>** - Specify a range of ports to be configured.
**rx** - (Optional) Specify to only monitor ingress packets.
**tx** - (Optional) Specify to only monitor egress packets.
**both** - (Optional) Specify to monitor both ingress and egress packets.

### Restrictions

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

### Example

To configure an RSPAN source entry without source target port:

```
DGS-3620-28SC:admin#config rspan vlan vlan_name vlan2 source add ports 2-5 rx
Command: config rspan vlan vlan_name vlan2 source add ports 2-5 rx

Success.

DGS-3620-28SC:admin#
```

To configure an RSPAN source entry for per flow RSPAN, without any source ports:

```
DGS-3620-28SC:admin#config rspan vlan vlan_id 2 source
Command: config rspan vlan vlan_id 2 source

Success.

DGS-3620-28SC:admin#
```

To configure RSPAN redirect for “VLAN 2” to ports 18 and 19:

```
DGS-3620-28SC:admin#config rspan vlan vlan_name vlan2 redirect add ports 18-19
Command: config rspan vlan vlan_name vlan2 redirect add ports 18-19

Success.

DGS-3620-28SC:admin#
```

## 85-6 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** - Specify the RSPAN VLAN by VLAN name.<br>**<vlan_name>** - Specify the VLAN name. |
| **vlan_id** - Specify the RSPAN VLAN by VLAN ID.<br>**<vlanid 1-4094>** - Specify the VLAN ID between 1 and 4094. |

### Restrictions

None.

### Example

To display specific RSPAN settings:

```
DGS-3620-28SC:admin# show rspan vlan_id 63
Command: show rspan vlan_id 63
```

```
RSPAN  : Enabled

RSPAN VLAN ID : 63
-------------------
Mirror Group ID  : 1
Target Port       : 1:1
Source Ports
RX          : 1:2-1:5
TX          : 1:2-1:5
Redirect Ports   : 1:9-1:12

Total RSPAN VLAN : 1
DGS-3620-28SC:admin#
```

To display all RSPAN settings:

```
DGS-3620-28SC:admin# show rspan
Command: show rspan

RSPAN: Enabled

RSPAN VLAN ID: 1
--------------------
Mirror Group ID  : 1
Target Port       : 1:1
Source Ports
                    RX:
                    TX:

RSPAN VLAN ID: 2
--------------------
Redirect Ports        : 1:6-1:10

RSPAN VLAN ID: 3
----------------------
Redirect Ports        : 1:6-1:10

Total RSPAN VLAN :3
DGS-3620-28SC:admin#
```

# Chapter 86 Safeguard Engine Commands

| |
|---|
| **config safeguard_engine** {state [enable \| disable] \| utilization {rising <value 20-100> \| falling <value 20-100>} (1)\| trap_log [enable \| disable] \| mode [strict \| fuzzy]} (1) |
| **show safeguard_engine** |

## 86-1 config safeguard_engine

### Description

This command is used to configure the safeguard engine for the system.

### Format

**config safeguard_engine {state [enable | disable] | utilization {rising <value 20-100> | falling <value 20-100>} (1)| trap_log [enable | disable] | mode [strict | fuzzy]} (1)**

### Parameters

| |
|---|
| **state** - (Optional) Configure the safeguard engine state to enable or disable.<br>**enable** - Configure the safeguard engine state to enable.<br>**disable** - Configure the safeguard engine state to disable. |
| **utilization** - (Optional) Configure the safeguard engine threshold.<br>**rising** - (Optional) Configure the utilization rising threshold. The range is between 20%-100%. If the CPU utilization is over the rising threshold, the switch enters exhausted mode.<br>**<value 20-100>** - Configure the utilization rising threshold. The range is between 20%-100%.<br>**falling** - (Optional) Configure the utilization falling threshold. The range is between 20%-100%. If the CPU utilization is lower than the falling threshold, the switch enters normal mode.<br>**<value 20-100>** - Configure the utilization falling threshold. The range is between 20%-100%. If the CPU utilization is lower than the falling threshold, the switch enters normal mode. |
| **trap_log** - (Optional) Configure the state of the safeguard engine related to the trap/log mechanism to enable or disable.<br>**enable** - If set to enable, trap and log will be active while the safeguard engine current mode is changed.<br>**disable** - If set to disable, the current mode change will not trigger trap and log events. |
| **mode** - (Optional) Determines the controlling method of broadcast traffic. There are two modes, strict and fuzzy.<br>**strict** - In strict, the switch will stop receiving all 'ARP not to me' packets (the protocol address of the target in the ARP packet is the Switch itself). That means no matter what reasons cause the high CPU utilization (may not be caused by ARP storm), the Switch reluctantly processes any 'ARP not to me' packets in exhausted mode.<br>**fuzzy** - In fuzzy mode, the switch will adjust the bandwidth dynamically depending on some reasonable algorithm. |

### Restrictions

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

### Example

To configure the safeguard engine:

```
DGS-3620-28SC: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-3620-28SC:admin#
```

## 86-2 show safeguard_engine

### Description

This command is used to display safeguard engine information.

### Format

**show safeguard_engine**

### Parameters

None.

### Restrictions

None.

### Example

To display safeguard engine information:

```
DGS-3620-28SC: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-3620-28SC:admin#
```

**Note:** The safeguard engine current status has two modes: exhausted and normal mode.

# Chapter 87 sFlow Commands

| |
|---|
| **enable sflow** |
| **disable sflow** |
| **show sflow** |
| **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>} |
| **config sflow flow_sampler ports** [<portlist> \| all] {rate <value 0-65535> \| tx_rate <value 0-65535> \| maxheadersize <value 18-256>}(1) |
| **delete sflow flow_sampler ports** [<portlist> \| all] |
| **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>} |
| **delete sflow analyzer_server** <value 1-4> |
| **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) |
| **show sflow analyzer_server** |
| **create sflow counter_poller ports** [<portlist> \| all] analyzer_server_id <value 1-4> {interval [disable \| <sec 20-120>]} |
| **config sflow counter_poller ports** [<portlist> \| all] interval [disable \| <sec 20-120>] |
| **delete sflow counter_poller ports** [<portlist> \| all] |
| **show sflow counter_poller** |
| **show sflow flow_sampler** |

## 87-1 enable sflow

### Description

This command is used to enable the sFlow function.

### Format

**enable sflow**

### Parameters

None.

### Restrictions

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

### Example

To enable the sFlow function:

```
DGS-3620-28SC:admin#enable sflow
Command: enable sflow
```

```

Success.

DGS-3620-28SC:admin#
```

## 87-2 disable sflow

### Description

This command is used to disable the sFlow function.

### Format

**disable sflow**

### Parameters

None.

### Restrictions

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

### Example

To disable the sFlow function:

```
DGS-3620-28SC:admin#disable sflow
Command: disable sflow

Success.

DGS-3620-28SC:admin#
```

## 87-3 show sflow

### Description

This command is used to display sFlow information.

### Format

**show sflow**

### Parameters

None.

### Restrictions

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

### Example

To display the sFlow information:

```
DGS-3620-28SC:admin#show sflow
Command: show sflow

 sFlow Version  : V5
 sFlow Address  : 10.90.90.90
 sFlow AddressV6: FE80::201:2FF:FE03:400
 sFlow State    : Enabled

DGS-3620-28SC:admin#
```

## 87-4 create sflow flow_sampler ports

### Description

This command is used to create the sFlow flow sampler.

### 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>** - Specify the list of ports to be configured.

**all** - Specify to configure all ports.

**analyzer_server_id** - Specify the ID of an analyzer server where the packet will be forwarded.
**<value 1-4>** - Specify the ID of an analyzer server where the packet will be forwarded.

**rate** - (Optional) Specify the sampling rate for packet sampling.
**<value 0-65535>** - Specify the sampling rate for packet sampling. The configured rate value multiplied by 256 is the actual rate. For example, if the rate is 20, the actual rate 5120. One packet will be sampled from every 5120 packets. If set to 0, the sampler is disabled. If the rate is not specified, its default value is 0.

**tx_rate** – Specifies the transmit rate.
**<value 0-65535>** - Enter the transmit rate used here. This value must be between 0 and 65535.

**maxheadersize** - (Optional) Specify the maximum number of leading bytes in the packet which has been sampled that will be encapsulated and forwarded to the server.
**<value 18-256>** - Specify 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.

### Restrictions

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

### Example

To create the sFlow flow sampler:

```
DGS-3620-28SC:admin#create sflow flow_sampler ports 1 analyzer_server_id 1 rate
```

```
200 maxheadersize 120
Command: create sflow flow_sampler ports 1 analyzer_server_id 1 rate 200
maxheadersize 120

Success.

DGS-3620-28SC:admin#
```

## 87-5 config sflow flow_sampler ports

### Description

This command is used to configure the sFlow flow sampler parameters.

### Format

**config sflow flow_sampler ports [<portlist> | all] {rate <value 0-65535> | tx_rate <value 0-65535> | maxheadersize <value 18-256>}(1)**

### Parameters

**<portlist>** - Specify the list of ports to be configured.

**all** - Specify to configure all ports.

**rate** - Specify the sampling rate for packet sampling.
**<value 0-65535>** - Specify the sampling rate for packet sampling. The configured rate value multiplied by 256 is the actual rate. For example, if the rate is 20, the actual rate 5120. One packet will be sampled from every 5120 packets. If set to 0, the sampler is disabled. If the rate is not specified, its default value is 0.

**tx_rate** – Specifies the transmit rate.
**<value 0-65535>** - Enter the transmit rate used here. This value must be between 0 and 65535.

**maxheadersize** - Specify the maximum number of leading bytes in the packet which has been sampled that will be encapsulated and forwarded to the server.
**<value 18-256>** - Specify 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.

### Restrictions

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

### Example

To configure the sFlow flow sampler parameters:

```
DGS-3620-28SC:admin#config sflow flow_sampler ports all rate 1
Command: config sflow flow_sampler ports all rate 1

Success.

DGS-3620-28SC:admin#
```

## 87-6 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>** - Specify the list of ports to be deleted.

**all** - Specify to delete all ports.

### Restrictions

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

### Example

To delete the sFlow flow sampler for ports 1 to 3:

```
DGS-3620-28SC:admin#delete sflow flow_sampler ports 1-3
Command: delete sflow flow_sampler ports 1-3

Success.

DGS-3620-28SC:admin#
```

## 87-7 create sflow analyzer_server

### Description

This command is used to create the sFlow flow sampler ports.

### 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>** - Specify a value between 1 and 4.

**owner** - Specify the entity making use of this sflow analyzer server. When owner is set or modified, the timeout value will become 400 automatically.

**<name 16>** - Specify the entity making use of this sflow analyzer server. When owner is set or modified, the timeout value will become 400 automatically.

**timeout** - (Optional) Specify the length of time 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. If not specified, its default value is 400. If it is specified as infinite, the server will never time out.

**<sec 1-2000000>** - Specify the time out value, in seconds, between 1 and 2000000.
**infinite** - Specify to never time out.

**collectoraddress** - (Optional) Specify the IP address of the analyzer server.
**<ipaddr>** - Specify the IP address of the analyzer server. If not specified, the address will be 0.0.0.0, which means that the entry will be inactive.
**<ipv6addr>** - Specify the IPv6 address of the analyzer server.

**collectorport** - (Optional) Specify the destination UDP port for sending the sFlow datagrams.
**<udp_port_number 1-65535>** - Specify the destination UDP port for sending the sFlow datagrams. If not specified, the default value is 6343.

**maxdatagramsize** - (Optional) Specify the maximum number of data bytes that can be packed in a single sample datagram.
**<value 300-1400>** - Specify the maximum number of data bytes that can be packed in a single sample datagram. If not specified, the default value is 1400.

### Restrictions

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

### Example

To create an sFlow analyzer server named “monitor”:

```
DGS-3620-28SC:admin#create sflow analyzer_server 1 owner monitor
Command: create sflow analyzer_server 1 owner monitor

Success.

DGS-3620-28SC:admin#
```

## 87-8 delete sflow analyzer_server

### Description

This command is used to delete the sFlow analyzer server.

### Format

**delete sflow analyzer_server <value 1-4>**

### Parameters

**<value 1-4>** - Specify a value between 1 and 4.

### Restrictions

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

### Example

To delete the sFlow analyzer server 1:

```
DGS-3620-28SC:admin#delete sflow analyzer_server 1
Command: delete sflow analyzer_server 1

```

```
Success.

DGS-3620-28SC:admin#
```

## 87-9 config sflow analyzer_server

### Description

This command is used to configure the sFlow analyzer server information. More than one collector with the same IP address can be specified 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 analyser server ID used here. This value must be between 1 and 4. The switch supports 4 different analyser servers at the same time. Each sampler or poller can select a server ID (1, 2, 3, or 4) to send the samples.

**timeout** - (Optional) Specify 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. If it is specified as infinite, the server will never be timeout.
**<sec 1-2000000>** - Specify the time out value, in seconds, between 1 and 2000000.
**infinite** - Specify to never time out.

**collectoraddress** - (Optional) Specify the IP address of the server.
**<ipaddr>** - Specify the IP address of the server. If set to 0, sFlow packets will not be sent to this server.
**<ipv6addr>** - Specifies the IPv6 used.

**collectorport** - (Optional) Specify the destination port for sending sflow datagrams.
**<udp_port_number 1-65535>** - Specify the destination port for sending sflow datagrams. The number is between 1 and 65535.

**maxdatagramsize** - (Optional) Specify the maximum number of data bytes that can be packed in a single sample datagram.
**<value 300-1400>** - Specify the maximum number of data bytes that can be packed in a single sample datagram. The values is between 300 and 1400.

### Restrictions

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

### Example

To configure the sFlow analyzer server information:

```
DGS-3620-28SC:admin#config sflow analyzer_server 1 collectoraddress 10.90.90.9
Command: config sflow analyzer_server 1 collectoraddress 10.90.90.9

Success.

DGS-3620-28SC:admin#
```

## 87-10 show sflow analyzer_server

### Description

This command is used to display sFlow analyzer server information.

### Format

**show sflow analyzer_server**

### Parameters

None.

### Restrictions

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

### Example

To display sFlow analyzer server information:

```
DGS-3620-28SC:admin#show sflow analyzer_server
Command: show sflow analyzer_server

 sFlow Analyzer_server Information
 ------------------------------
 Server ID             : 1
 Owner                 : admin
 Timeout               : 400
 Current Countdown Time: 400
 Collector Address     :
 Collector Port        : 6343
 Max Datagram Size     : 1400

Total Entries: 1

DGS-3620-28SC:admin#
```

## 87-11 create sflow counter_poller ports

### Description

This command is used to create the sFlow counter poller. With the poller function, the statistics counter information with respect to a port will be forwarded to the server at the configured interval. These counters are RFC 2233 counters.

### Format

**create sflow counter_poller ports [<portlist> | all] analyzer_server_id <value 1-4> {interval [disable | <sec 20-120>]}**

### Parameters

**<portlist>** - Specify the ports to be configured.

**all** - Specify to configure all ports.

**analyzer_server_id** - Specify the ID of an analyzer server where the packet will be forwarded.
**<value 1-4>** - Specify the ID of an analyzer server where the packet will be forwarded.

**interval** - (Optional) Specify the maximum number of seconds between successive statistic counters information. If set to disable, the counter-poller is disabled. If the interval is not specified, its default value is disable.
**disable** - Specify to disable the interval.
**<sec 20-120>** - Specify the interval, in seconds, between 20 and 120.

### Restrictions

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

### Example

To create the sFlow counter poller:

```
DGS-3620-28SC:admin#create sflow counter_poller ports 1 analyzer_server_id 1
Command: create sflow counter_poller ports 1 analyzer_server_id 1

Success.

DGS-3620-28SC:admin#
```

## 87-12 config sflow counter_poller ports

### Description

This command is used to configure the sflow counter poller parameters. If a user wants to change the analyzer server ID, they need to delete the counter poller and create a new one.

### Format

**config sflow counter_poller ports [<portlist> | all] interval [disable | <sec 20-120>]**

### Parameters

**<portlist>** - Specify the ports to be configured.

**all** - Specify to configure all ports.

**interval** - Specify the maximum number of seconds between successive samples of the counters. If set to disabled, the counter sample is disabled.
**disable** - Specify to disable the interval.
**<sec 20-120>** - Specify the interval, in seconds, between 20 and 120.

### Restrictions

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

### Example

To configure the sFlow counter poller parameters interval to 50 for port 1:

```
DGS-3620-28SC:admin#config sflow counter_poller ports 1 interval 50
Command: config sflow counter_poller ports 1 interval 50

Success.

DGS-3620-28SC:admin#
```

## 87-13 delete sflow counter_poller ports

### Description

This command is used to delete the sFlow counter poller.

### Format

**delete sflow counter_poller ports [<portlist> | all]**

### Parameters

| |
|---|
| **<portlist>** - Specify the ports to be deleted. |
| **all** - Specify to delete all ports. |

### Restrictions

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

### Example

To delete the sFlow counter poller for port 1:

```
DGS-3620-28SC:admin#delete sflow counter_poller ports 1
Command: delete sflow counter_poller ports 1

Success.

DGS-3620-28SC:admin#
```

## 87-14 show sflow counter_poller

### Description

This command is used to display sFlow counter poller information for the ports that have been created.

### Format

**show sflow counter_poller**

### Parameters

None.

### Restrictions

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

### Example

To display sFlow counter poller information for the ports that have been created:

```
DGS-3620-28SC:admin#show sflow counter_poller
Command: show sflow counter_poller

 Port   Analyzer Server ID   Polling Interval (sec)
 ----   ------------------   -----------------------
 1      1                    50

Total Entries: 1

DGS-3620-28SC:admin#
```

## 87-15 show sflow flow_sampler

### Description

This command is used to display sFlow sampler information for the ports that have been created.

### Format

**show sflow flow_sampler**

### Parameters

None.

### Restrictions

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

### Example

To display sFlow sampler information for the ports that have been created:

```
DGS-3620-28SC: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
 ------  ---------  ----------  ----------  -------  -------  -----------
 1:15    1          10          10          10       10       18
 1:21    1          10          10          10       10       18

Total Entries: 1

DGS-3620-28SC:admin#
```

# Chapter 88 Single IP Management Commands

| |
|---|
| **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]} |

## 88-1 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 Administrator-level users can issue this command.

### Example

To enable single IP management:

```
DGS-3620-28SC:admin#enable sim
Command: enable sim

Success.

DGS-3620-28SC:admin#
```

## 88-2 disable sim

### Description

This command is used to configure the single IP management on the switch as disabled.

### Format

**disable sim**

### Parameters

None.

### Restrictions

Only Administrator-level users can issue this command.

### Example

To disable single IP management:

```
DGS-3620-28SC:admin#disable sim
Command: disable sim

Success.

DGS-3620-28SC:admin#
```

## 88-3 show sim

### Description

This command is used to display the information of the specific sorts of devices including of self, candidate, member, group, and neighbor.

### 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) Specify the candidate devices. The ID is from 1 to 100.

**members** - (Optional) Specify the member devices.
  **<member_id 1-32>** - (Optional) Specify the member devices. The ID is from 1 to 32.

**group** – (Optional) Specify other group devices.
  **commander_mac** - Specify the commander MAC address.
    **<macaddr>** - Specify the commander MAC address.

**neighbor** - (Optional) Specify other neighbor devices.

### Restrictions

None.

### Example

To show the self information in detail:

```
DGS-3620-28SC:admin#show sim
Command: show sim

SIM Version        : VER-1.61
Firmware Version   : 1.00.034
Device Name        :
MAC Address        : 00-01-02-03-04-00
Capabilities       : L3
Platform           : DGS-3620-28SC-DC L3 Switch
SIM State          : Disabled
Role State         : Candidate
Discovery Interval : 30 sec
Hold Time          : 100 sec

DGS-3620-28SC:admin#
```

To show the candidate information in summary:

```
DGS-3620-28SC:admin#show sim candidate
Command: show sim candidates

ID  MAC Address       Platform /               Hold  Firmware Device Name
Capability               Time  Version
--- ----------------- ------------------------ ----- --------- ----------------
-------------
 1  00-01-02-03-04-00 DGS-3620-28SC-DC L3 Switch  40   2.00.009
aaaaaaaaaaaaaaaabbbbbbbbbbbb

bbb
 2  00-55-55-00-55-00 DGS-3620-28SC-DC L3 Switch 140   2.00.009 default master

Total Entries: 2

DGS-3620-28SC:admin#
```

To show the member information in summary:

```
DGS-3620-28SC:admin#show sim member
Command: show sim member

ID  MAC Address       Platform /               Hold  Firmware Device Name
Capability               Time  Version
--- ----------------- ------------------------ ----- --------- ----------------
 1  00-01-02-03-04-00 DGS-3620-28SC-DC L3 Switch  40
2.00.009aaaaaaaaaaaaaa009aaaaaaaaaaaaaa
                                                          aabbbbbbbbbbbbbbb
 2  00-55-55-00-55-00 DGS-3620-28SC-DC L3 Switch  140 2.00.009 default master

Total Entries: 2

DGS-3620-28SC:admin#
```

To show other groups information in summary:

```
DGS-3620-28SC: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-3620-28SC-DC L3 Switch   40   2.00.009
aaaaaaaaaaaaaaaabbbbbbbbbbbb

bbb
 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-3620-28SC-DC L3 Switch  40   2.00.009
aaaaaaaaaaaaaaaabbbbbbbbbbbb

bbb
 2  00-55-55-00-55-00

'*' means commander switch.

DGS-3620-28SC:admin#
```

To show an SIM neighbor table:

```
DGS-3620-28SC: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-3620-28SC:admin#
```

## 88-4 reconfig

### Description

This command is used to re-Telnet to a member.

### Format

**reconfig [member_id <value 1-32> | exit]**

### Parameters

**member_id** - Specify the serial number of a member.
    **<value 1-32>** - Specify the serial number of a member. The value is between 1 and 32.

**exit** - Specify to terminate command switch access.

### Restrictions

Only Administrator-level users can issue this command.

### Example

To re-Telnet to a member:

```
DGS-3620-28SC:admin#reconfig member_id 1
Command: reconfig member_id 1

DGS-3620-28SC:admin#
                        DGS-3620-28SC Gigabit Ethernet Switch
                             Command Line Interface

                            Firmware: Build 2.00.015
           Copyright(C) 2012 D-Link Corporation. All rights reserved.

DGS-3620-28SC:admin#
```

## 88-5 config sim_group

### Description

This command is used to configure group information on the switch.

### 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>** - Specify to add a specific candidate to the group.
**<password>** - (Optional) Specify the password of a candidate, if necessary.

**delete** - Specify to remove a specific member from the group.
**<member_id 1-32>** - Specify to remove a specific member from the group. The ID is from 1 to 32.

### Restrictions

Only Administrator-level users can issue this command.

### Example

To add a member:

```
DGS-3620-28SC:admin#config sim_group add 2
Command: config sim_group add 2

Please wait for ACK !!!
SIM Config Success !!!

Success.

DGS-3620-28SC:admin#
```

To delete a member:

```
DGS-3620-28SC:admin#config sim_group delete 1
Command: config sim_group delete 1

Please wait for ACK !!!
SIM Config Success !!!

Success.

DGS-3620-28SC:admin#
```

## 88-6 config sim

### Description

This command is used to configure the role state and parameters of 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** - Transfer the role to commander.

**group_name** - (Optional) If commander, users can specify the name of the group.
**<groupname 64>** - If commander, users can specify the name of the group. The maximum length is 64 characters.

**candidate** - Transfer role to candidate.

**dp_interval** - Specify the time in seconds between discoveries.
**<sec 30-90>** - Specify the time in seconds between discoveries.

**hold_time** - Specify the time in seconds the device holds the discovery result.
**<sec 100-255>** - Specify the time in seconds the device holds the discovery result.

## Restrictions

Only Administrator-level users can issue this command.

## Example

To transfer to commander:

```
DGS-3620-28SC:admin#config sim commander
Command: config sim commander

Success.

DGS-3620-28SC:admin#
```

To transfer to candidate:

```
DGS-3620-28SC:admin#config sim candidate
Command: config sim candidate

Success.

DGS-3620-28SC:admin#
```

To update the name of  a group:

```
DGS-3620-28SC:admin#config sim commander group_name mygroup
Command: config sim commander group_name mygroup

Success.

DGS-3620-28SC:admin#
```

To change the time interval of discovery protocol:

```
DGS-3620-28SC:admin#config sim dp_interval 30
Command: config sim dp_interval 30

Success.

DGS-3620-28SC:admin#
```

To change the hold time of discovery protocol:

```
DGS-3620-28SC:admin#config sim hold_time 200
Command: config sim hold_time 200

Success.

DGS-3620-28SC:admin#
```

## 88-7 download sim_ms

### Description

This command is used to download firmware or configuration from a 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>** - Specify the IP address of the TFTP server.

**<path_filename>** - Specify 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>** - Specify a range of members which download this firmware or configuration.
**all** - Specify all members which download this firmware or configuration.

### Restrictions

Only Administrator-level users can issue this command.

### Example

To download firmware:

```
DGS-3620-28SC:admin#download sim_ms firmware_from_tftp 10.55.47.1
D:\dwl600x.tfp members 1-3
Commands: download sim_ms firmware_from_tftp 10.55.47.1 D:\dwl600x.tfp members
1-3


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  Fail
3   00-07-06-05-04-04  Fail
```

```
DGS-3620-28SC:admin#
```

To download configuration:

```
DGS-3620-28SC:admin#download sim_ms configuration_from_tftp 10.55.47.1
D:\test.txt members 1-3
Commands: download sim_ms configuration_from_tftp 10.55.47.1 D:\test.txt
members 1-3

This device is updating configuration.  Please wait several minutes...

Download Status :

ID   MAC Address        Result
---  -----------------  ----------------
1   00-01-02-03-04-00  Success
2   00-07-06-05-04-03  Fail
3   00-07-06-05-04-03  Fail

DGS-3620-28SC:admin#
```

## 88-8 upload sim_ms

### Description

This command is used to upload configuration or a log from indicated devices to a 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>** - Specify the IP address of the TFTP server.

**<path_filename>** - Specify the file path to store configuration or a log in the TFTP server.

**members** – (Optional) Specifiy the members which upload its configuration.
- **<mslist>** - Specifiy the members which upload its configuration.The value is from 1 to 32.
- **all** - Specify all members which upload its configuration.

### Restrictions

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

### Example

To upload a configuration:

```
DGS-3620-28SC:admin#upload sim_ms configuration_to_tftp 10.55.47.1
D:\configuration.txt members 1
Command: upload sim_ms configuration_to_tftp 10.55.47.1 D:\configuration.txt
members 1
```

```
This device is uploading configuration. Please wait several minutes...

Upload Status:

ID   MAC Address        Result
--   ----------------   -------
 1    00-01-02-03-04-00  Success

DGS-3620-28SC:admin#
```

# Chapter 89 SNMPv1/v2/v3 Commands

| |
|---|
| **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** <user_name 32> |
| **show snmp user** |
| **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 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] |
| **config snmp engineID** <snmp_engineID 10-64> |
| **show snmp engineID** |
| **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>}(1) |
| **delete snmp group** <groupname 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 v6host** {<ipv6addr>} |
| **show snmp host** {<ipaddr>} |
| **enable community_encryption** |
| **disable community_encryption** |
| **show community_encryption** |

## 89-1 create snmp user

### Description

This command is used to create a new user to an SNMP group originated by this command. Users can choose input authentication and privacy by password or by key.

### 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>** - Specify the name of the user on the host that connects to the agent. The range is 1 to 32 characters.

**<groupname 32>** - Specify the name of the group to which the user is associated. The range is 1 to 32 characters.

**encrypted** - (Optional) Specify whether the password appears in encrypted format.

**by_password auth** - Indicate the input password for authentication

**sha** - Specify the HMAC-SHA-96 authentication level between 8 and 20 characters.
**<auth_password 8-20>** - Specify the HMAC-SHA-96 authentication level between 8 and 20 characters.

**md5** – Specify the HMAC-MD5-96 authentication level between 8 and 16 characters.
**<auth_password 8-16>** - Specify the HMAC-MD5-96 authentication level between 8 and 16 characters.

**priv** - Indicate the input password for privacy. The options are none and DES.
**none** - Specify there will be no privacy string.
**des** - Specify a privacy string used by DES between 8 and 16 characters.
**<priv_password 8-16>** - Specify a privacy string used by DES between 8 and 16 characters.

**by_key auth** - Indicate the input key for authentication. The options are MD5 and SHA1.

**md5** - Specify an authentication key used by MD5. This is a hex string type of 32 characters.
**<auth_key 32-32>** - Specify an authentication key used by MD5. This is a hex string type of 32 characters.

**sha** - Specify an authentication key used by SHA1. This is a hex string type of 40 characters.
**<auth_key 40-40>** - Specify an authentication key used by SHA1. This is a hex string type of 40 characters.

**priv** - Indicate the input key for privacy. The options are none and DES.
**none** - Specify there will be no privacy key.
**des** - Specify a privacy key used by DES. This is a hex string type of 32 characters
**<priv_key 32-32>** - Specify a privacy key used by DES. This is a hex string type of 32 characters.

### Restrictions

Only Administrator-level users can issue this command.

### Example

To create a new user to an SNMP group originated by this command:

```
DGS-3620-28SC:admin#create snmp user dlink D-Link_group encrypted by_password
auth md5 12345678 priv des 12345678
Command: create snmp user dlink D-Link_group encrypted by_password auth md5
12345678 priv des 12345678


Success.


DGS-3620-28SC:admin#
```

## 89-2 delete snmp user

### Description

This command is used to remove a user from an SNMP group and deletes the associated group in the SNMP group.

### Format

**delete snmp user <user_name 32>**

### Parameters

**<user_name 32>** - Specify the name of the user on the host to be deleted. The range is 1 to 32 characters.

### Restrictions

Only Administrator-level users can issue this command.

### Example

To delete an SNMP user:

```
DGS-3620-28SC:admin#delete snmp user dlink
Command: delete snmp user dlink

Success.

DGS-3620-28SC:admin#
```

## 89-3 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 display SNMP user information:

```
DGS-3620-28SC:admin#show snmp user
Command: show snmp user

Username                    Group Name                    VerAuthPriv
---------------------------  ---------------------------  ------------
initial                     initial                       V3 NoneNone
```

```
Total Entries : 1

DGS-3620-28SC:admin#
```

## 89-4 show snmp groups

### Description

This command is used to display the names of groups on the switch, and the security model, level, and the status of the different views.

### Format

**show snmp groups**

### Parameters

None.

### Restrictions

None.

### Example

To display the names of the SNMP groups on the switch:

```
DGS-3620-28SC:admin#show snmp groups
Command: show snmp groups

Vacm Access Table Settings

Group    Name     : public
ReadView Name     : CommunityView
WriteView Name    :
Notify View Name : CommunityView
Security Model    : SNMPv1
Security Level    : NoAuthNoPriv

Group    Name     : public
ReadView Name     : CommunityView
WriteView Name    :
Notify View Name : CommunityView
Security Model    : SNMPv2
Security Level    : NoAuthNoPriv

Group    Name     : private
ReadView Name     : CommunityView
WriteView Name    : CommunityView
Notify View Name : CommunityView
Security Model    : SNMPv2
Security Level    : NoAuthNoPriv
```

```

Total Entries: 3

DGS-3620-28SC:admin#
```

## 89-5 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>** - Specify the view name to be created.

**<oid>** - Specify the object-identified tree (the MIB tree).

**view_type** - Specify the access type of of the MIB tree in this view.

**included** - Specify to include this view.

**excluded** - Specify to exclude this view.

### Restrictions

Only Administrator-level users can issue this command.

### Example

To assign views to community strings to limit which MIB objects an SNMP manager can access:

```
DGS-3620-28SC:admin#create snmp view dlinkview 1.3.6 view_type included
Command: create snmp view dlinkview 1.3.6 view_type included

Success.

DGS-3620-28SC:admin#
```

## 89-6 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>** - Specify the view name of the user who will be deleted.

**all** - Specify to view all records.

**<oid> -** Specify the object-identified tree (the MIB tree).

### Restrictions

Only Administrator-level users can issue this command.

### Example

To remove a view record:

```
DGS-3620-28SC:admin#delete snmp view dlinkview all
Command: delete snmp view dlinkview all

Success.

DGS-3620-28SC:admin#
```

## 89-7 show snmp view

### Description

This command is used to display SNMP view records.

### Format

**show snmp view {<view_name 32>}**

### Parameters

**<view_name 32> -** (Optional) Specify the view name of the user to be displayed.

### Restrictions

None.

### Example

To display SNMP view records:

```
DGS-3620-28SC:admin#show snmp view
Command: show snmp view

Vacm View Table Settings
View Name             Subtree                    View Type
--------------------  -------------------------  ----------
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: 8

DGS-3620-28SC:admin#
```

## 89-8 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: 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>** - Specify the community string. The maximum string length is 32 characters.

**view** - Specify the view name of the MIB. The maximum length is 32 characters.
**<view_name 32>** - Specify the view name of the MIB. The maximum length is 32 characters.

**read_only** - Specify read-only permission.

**read_write** - Specify read and write permission.

### Restrictions

Only Administrator-level users can issue this command.

### Example

To create an SNMP community string:

```
DGS-3620-28SC:admin#create snmp community dlink view CommunityView read_write
Command: create snmp community dlink view CommunityView read_write

Success.

DGS-3620-28SC:admin#
```

## 89-9 delete snmp community

### Description

This command is used to remove a specific community string.

### Format

**delete snmp community <community_string 32>**

### Parameters

**<community_string 32>** - Specify the community string that will be deleted.

### Restrictions

Only Administrator-level users can issue this command.

### Example

To delete an SNMP community:

```
DGS-3620-28SC:admin#delete snmp community dlink
Command: delete snmp community dlink

Success.

DGS-3620-28SC:admin#
```

## 89-10 show snmp community

### Description

This command is used to display community string configurations.

### Format

**show snmp community {<community_string 32>}**

### Parameters

**<community_string 32> -** (Optional) Specify the community string to be displayed.

**Note:** If a community string is not specified, all community string information will be displayed.

### Restrictions

None.

### Example

To display the current community string configurations:

```
DGS-3620-28SC: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-3620-28SC:admin#
```

## 89-11 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** - Specifies that the user, using the community string, will have read only access to the switch's SNMP agent.

**read_write** - Specifies that the user, using the community string, will have read/write access to the switch's SNMP agent.

### Restrictions

Only Administrator level users can issue this command.

### Example

To create an SNMP community string called "community123" with the "read_only" security method:

```
DGS-3620-28SC: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-3620-28SC:admin#
```

## 89-12 config snmp engineID

### Description

This command is used to configure an identifier for the SNMP engine on the switch. Associated with each SNMP entity is a unique engine ID.

### Format

**config snmp engineID <snmp_engineID 10-64>**

### Parameters

**<snmp_engineID 10-64>** - Specify the identify for the SNMP engine on the switch.

### Restrictions

Only Administrator-level users can issue this command.

### Example

To configure an identifier for the SNMP engine on the switch:

```
DGS-3620-28SC:admin#config snmp engineID 1023457890
Command: config snmp engineID 1023457890

Success.

DGS-3620-28SC:admin#
```

## 89-13 show snmp engineID

### Description

This command is used to display the identification of the SNMP engine on the switch.

### Format

**show snmp engineID**

### Parameters

None.

### Restrictions

None.

### Example

To display the identification of an SNMP engine:

```
DGS-3620-28SC:admin#show snmp engineID
Command: show snmp engineID

SNMP Engine ID : 1023457890

DGS-3620-28SC:admin#
```

## 89-14 create snmp group

### Description

This command is used to create a new SNMP group.

### 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>}(1)**

### Parameters

**<groupname 32>** - Specify the name of the group.

**v1** - Specify the least secure of the possible security models.

**v2c** - Specify the second least secure of the possible security models.

**v3** - Specify the most secure of the possible security models. Specifies authentication of a packet.

**noauth_nopriv** - Specify to neither support packet authentication nor encrypting.

**auth_nopriv** - Specify to support packet authentication.

**auth_priv** - Specify to support packet authentication and encrypting.

**read_view** - Specify the view name between 1 and 32 characters.
**<view_name 32>** - Specify the view name between 1 and 32 characters.

**write_view** - Specify the view name between 1 and 32 characters.
**<view_name 32>** - Specify the view name between 1 and 32 characters.

**notify_view** - Specify the view name between 1 and 32 characters.
**<view_name 32>** - Specify the view name between 1 and 32 characters.

### Restrictions

Only Administrator-level users can issue this command.

### Example

To create a new SNMP group:

```
DGS-3620-28SC:admin#create snmp group D-Link_group v3 auth_priv read_view
CommunityViewwrite_view CommunityView notify_view CommunityView
Command: create snmp group D-Link_group v3 auth_priv read_view CommunityView
write_view CommunityView notify_view CommunityView


Success.

DGS-3620-28SC:admin#
```

## 89-15 delete snmp group

### Description

This command is used to remove an SNMP group.

### Format

**delete snmp group <groupname 32>**

### Parameters

**<groupname 32>** - Specify the name of the group that will be deleted.

### Restrictions

Only Administrator-level users can issue this command.

### Example

To remove an SNMP group:

```
DGS-3620-28SC:admin#delete snmp group D_Link_group
Command: delete snmp group D_Link_group

Success.

DGS-3620-28SC:admin#
```

## 89-16 create snmp

### Description

This command is used to create a recipient of an SNMP operation.

### Format

**create snmp [host <ipaddr> | v6host <ipv6addr>] [v1 | v2c | v3 [noauth_nopriv | auth_nopriv | auth_priv] ] <auth_string 32>**

### Parameters

**host** - Specify the IP address of the recipient for which the traps are targeted.
**<ipaddr>** - Specify the IP address of the recipient for which the traps are targeted.

**v6host** - Specify the v6host IP address to which the trap packet will be sent.
**<ipv6addr>** - Specify the v6host IP address to which the trap packet will be sent.

**v1** - Specify the least secure of the possible security models.

**v2c** - Specify the second least secure of the possible security models.

**v3** - Specify the most secure of the possible security models.

**noauth_nopriv** - Specify to neither support packet authentication nor encrypting.

**auth_nopriv** - Specify to support packet authentication.

**auth_priv** - Specify to support packet authentication and encrypting.

**<auth_string 32>** - Specify the authentication string. If 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 v3

| |
|---|
| is specified, the auth_string presents the user name, and it must be one of the entries in the user table. |

### Restrictions

Only Administrator level users can issue this command.

### Example

To create a recipient of an SNMP operation:

```
DGS-3620-28SC:admin#create snmp host 10.48.74.100 v3 noauth_nopriv initial
Command: create snmp host 10.48.74.100 v3 noauth_nopriv initial

Success.

DGS-3620-28SC:admin#
```

## 89-17 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** - Specify the IP address of the SNMP host recipient to be deleted.<br>**<ipaddr>** - Specify the IP address of the SNMP host recipient to be deleted. |
| **v6host** - Specify the IPv6 address of the SNMP host recipient to be deleted.<br>**<ipv6addr>** - Specify the IPv6 address of the SNMP host recipient to be deleted. |

### Restrictions

Only Administrator-level users can issue this command.

### Example

To delete a recipient of an SNMP trap operation:

```
DGS-3620-28SC:admin#delete snmp host 10.48.74.100
Command: delete snmp host 10.48.74.100

Success.

DGS-3620-28SC:admin#
```

## 89-18 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) Specify the IP address of the recipient for which the traps are targeted. |

**Note:** If no parameter is specified, all SNMP hosts will be displayed.

### Restrictions

None.

### Example

To display the receipient for which the traps are targeted:

```
DGS-3620-28SC:admin# show snmp host
Command: show snmp host

SNMP Host Table
Host IP Address  SNMP Version     Community Name / SNMPv3 User Name
---------------  ---------------  ---------------------------------
10.48.76.100     V3 noauthnopriv  initial
10.51.17.1       V2c              public

Total Entries : 2

DGS-3620-28SC:admin#
```

## 89-19 show snmp v6host

### Description

This command is used to display the recipient for which the traps are targeted.

### Format

**show snmp v6host {<ipv6addr>}**

### Parameters

| |
|---|
| **<ipv6addr>** - (Optional) Specify the v6host IP address. |

**Note:** If no parameter is specified, all SNMP IPv6 hosts will be displayed.

### Restrictions

None.

### Example

To display the recipient for which the traps are targeted:

```
DGS-3620-28SC:admin# show snmp v6host
Command: show snmp v6host

SNMP Host Table
-------------------------------------------------------------------
Host IPv6 Address: FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
SNMP Version     : V3 na/np
Community Name/SNMPv3 User Name: 12345678901234567890

Host IPv6 Address: FEC0:1A49:2AA:FF:FE34:CA8F
SNMP Version     : V3 a/np
Community Name/SNMPv3 User Name: abcdefghijk

Total Entries : 2

DGS-3620-28SC:admin#
```

## 89-20 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 Administrator level users can issue this command.

### Example

To enable the encryption state on an SNMP community string:

```
DGS-3620-28SC:admin# enable community_encryption
Command: enable community_encryption
```

```
Success.

DGS-3620-28SC:admin#
```

When creating an SNMP community string after the encryption state has been enabled, the community string will be displayed as an encrypted string (six "*"), otherwise displayed as plaintext, for example:

```
DGS-3620-28SC:admin# show snmp community
Command: show snmp community

SNMP Community Table
Community Name         View Name              Access Right
---------------------  ---------------------  ------------
******                 CommunityView          read_write
******                 CommunityView          read_only
private                CommunityView          read_write
public                 CommunityView          read_only

Total Entries : 4

DGS-3620-28SC:admin#
```

## 89-21 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 Administrator level users can issue this command.

### Example

To disable the encryption state on the SNMP community string:

```
DGS-3620-28SC:admin# disable community_encryption
Command: disable community_encryption

Success.

DGS-3620-28SC:admin#
```

## 89-22 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-3620-28SC:admin# show community_encryption
Command: show community_encryption

SNMP Community Encryption State : Enabled

DGS-3620-28SC:admin#
```

# Chapter 90 Spanning Tree Protocol (STP) commands

| |
|---|
| **show stp** |
| **show stp instance** {<value 0-64>} |
| **show stp ports** {<portlist>} |
| **show stp mst_config_id** |
| **create stp instance_id** <value 1-64> |
| **delete stp instance_id** <value 1-64> |
| **config stp instance_id** <value 1-64> [add_vlan \| remove_vlan] <vidlist> |
| **config stp mst_config_id** {revision_level <int 0-65535> \| name <string>} (1) |
| **enable stp** |
| **disable stp** |
| **config stp version** [mstp \| rstp \| stp] |
| **config stp priority** <value 0-61440> instance_id <value 0-64> |
| **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]}(1) |
| **config stp ports** <portlist> {externalCost [auto \| <value 1-200000000>] \| hellotime <value 1-2> \| migrate [yes \| no] \| edge [true \| false \| auto] \| p2p [true \| false \| auto] \| state [enable \| disable] \| restricted_role [true \| false] \| restricted_tcn [true \| false] \| fbpdu [enable \| disable]} (1) |
| **config stp mst_ports** <portlist> instance_id <value 0-64> {internalCost [auto \| <value 1-200000000>] \| priority <value 0-240>}(1) |

## 90-1 show stp

### Description

This command is used to display the bridge parameters global settings.

### Format

**show stp**

### Parameters

None.

### Restrictions

None.

### Example

To display STP:

```
DGS-3620-28SC:admin#show stp
Command: show stp

STP Bridge Global Settings
-----------------------------
STP Status          : Enabled
STP Version         : MSTP
Max Age             : 20
Forward Delay       : 15
Max Hops            : 20
TX Hold Count       : 6
Forwarding BPDU     : Enabled
NNI BPDU Address    : dot1d

DGS-3620-28SC:admin#
```

## 90-2 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 instances will be shown.

### Format

**show stp instance {<value 0-64>}**

### Parameters

**<value 0-64>** - (Optional) Specify the MSTP instance ID. Instance 0 represents the default instance: CIST. This value must be between 0 and 64.

### Restrictions

None.

### Example

To display STP instances:

```
DGS-3620-28SC: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-3620-28SC:admin#
```

## 90-3 show stp ports

### Description

This command is used to display the switch’s current per-port STP configuration:

STP port configuration, STP port role (Disabled, Alternate, Backup, Root, Designated, NonStp), and

STP port status (Disabled, Discarding, Learning, Forwarding).

### Format

**show stp ports {<portlist>}**

### Parameters

| |
|---|
| **<portlist>** - (Optional) Specify a range of ports to be displayed. |

### Restrictions

None.

### Example

To show STP ports:

```
DGS-3620-28SC:admin#show stp ports
Command: show stp ports
```

```

MSTP Port Information
Port Index        : 1     ,  Hello Time       : 2 /2 ,  Port STP : enabled
External PathCost : Auto/200000   ,  Edge Port : No /No ,  P2P    : False/No
Port RestrictedRole : False,  Port RestrictedTCN : False
Port Forward BPDU : Enabled

MSTI   Designated Bridge   Internal PathCost  Prio  Status      Role
-----  ------------------  -----------------  ----  ----------  ----------
0      N/A                 200000             128   Disabled    Disabled
2      N/A                 200000             128   Disabled    Disabled

DGS-3620-28SC:admin#
```

## 90-4 show stp mst_config_id

### Description

This command is used to display the three elements of the MST configuration Identification, including Configuration Name, Revision Level, and the MST configuration Table. The default Configuration name is the MAC address of the bridge. If two bridges have the same three elements in **mst_config_id**, that means they are in the same MST region.

### Format

**show stp mst_config_id**

### Parameters

None.

### Restrictions

None.

### Example

Display the STP MST Config ID:

```
DGS-3620-28SC: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-3620-28SC:admin#
```

## 90-5 create stp instance_id

### Description

This command is used to create a new MST instance independent from the default Instance: CIST (Instance 0). After creating the MST instance, a user needs to configure the VLANs (using commands in 90-7), or the newly created MST instance will still be in a disabled state.

### Format

**create stp instance_id <value 1-64>**

### Parameters

**<value 1-64>** - Specify the MSTP instance ID. Instance 0 represents a default instance CIST. This value must be between 1 and 64.

### Restrictions

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

### Example

To create an MSTP instance:

```
DGS-3620-28SC:admin#create stp instance_id 2
Command: create stp instance_id 2

Warning:There is no VLAN mapping to this instance_id!
Success.

DGS-3620-28SC:admin#
```

## 90-6 delete stp instance_id

### Description

This command is used to delete the specified MST Instance. CIST (Instance 0) cannot be deleted and you can only delete one instance at a time.

### Format

**delete stp instance_id <value 1-64>**

### Parameters

**<value 1-64>** - Specify the MSTP instance ID. Instance 0 represents the default instance CIST. This value must be between 1 and 64.

### Restrictions

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

### Example

To delete an MSTP instance:

```
DGS-3620-28SC:admin#delete stp instance_id 2
Command: delete stp instance_id 2

Success.

DGS-3620-28SC:admin#
```

## 90-7 config stp instance_id

### Description

There are two different action types to deal with an MST instance. They are listed as follows:

1) add_vlan: To map specified VLAN lists to an existing MST instance.
2) remove_vlan: To delete specified VLAN lists from an existing MST instance.

### Format

**config stp instance_id <value 1-64> [add_vlan | remove_vlan] <vidlist>**

### Parameters

**<value 1-64>** - Specify the MSTP instance ID. Instance 0 represents a default instance CIST. The DUT supports 65 instances (0-64) at most.

**add_vlan** - Defined action type to configure an MST instance.

**remove_vlan** - Defined action type to configure an MST instance.

**<vidlist>** - Specify the newly added CLI Value Type. It is similar to **<portlist>** type, but the value range is 1 to 4094.

### Restrictions

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

### Example

To map a VLAN ID to an MSTP instance:

```
DGS-3620-28SC:admin#config stp instance_id 2 add_vlan 1
Command: config stp instance_id 2 add_vlan 1

Success.

DGS-3620-28SC:admin#
```

To remove a VLAN ID from an MSTP instance:

```
DGS-3620-28SC:admin#config stp instance_id 2 remove_vlan 2
Command: config stp instance_id 2 remove_vlan 2
```

```
Success.

DGS-3620-28SC:admin#
```

## 90-8 config stp mst_config_id

### Description

This command is used to configure a configuration name or revision level in the MST configuration identification. The default configuration name is the MAC address of the bridge.

### Format

**config stp mst_config_id {revision_level <int 0-65535> | name <string>} (1)**

### Parameters

**revision_level** - Specify the revision level.
  **<int 0-65535>** - Specify the revision level.

**name** - Specify the name given for a specified MST region.
  **<string>** - Specify the name given for a specified MST region.

### Restrictions

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

### Example

To change the name and revision level of the MST configuration identification:

```
DGS-3620-28SC:admin#config stp mst_config_id revision_level 1 name R&D_BlockG
Commands: config stp mst_config_id revision_level 1 name R&D_BlockG

Success.

DGS-3620-28SC:admin#
```

## 90-9 enable stp

### Description

Although it is possible to modify to allow a user to enable STP per instance, CIST should be enabled first before enabling other instances. When a user enables the CIST, all MSTIs will be enabled automatically if FORCE_VERSION is set to MSTP and there is at least one VLAN mapped to this instance.

### Format

**enable stp**

### Parameters

None.

### Restrictions

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

### Example

To enable STP:

```
DGS-3620-28SC:admin#enable stp
Command: enable stp

Success.

DGS-3620-28SC:admin#
```

## 90-10 disable stp

### Description

This command is used to disable STP functionality in every existing instance.

### Format

**disable stp**

### Parameters

None.

### Restrictions

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

### Example

To disable STP:

```
DGS-3620-28SC:admin#disable stp
Command: disable stp

Success.

DGS-3620-28SC:admin#
```

## 90-11 config stp version

### Description

This command is used to change STP version. If the version is configured as STP or RSTP, all currently running MSTIs should be disabled. If the version is configured as MSTP, the current chip design is enabled for all available MSTIs (assuming that CIST is enabled).

### Format

**config stp version [mstp | rstp | stp]**

### Parameters

| |
|---|
| **mstp** - Specify to use Multiple Spanning Tree Protocol. |
| **rstp** - Specify to use Rapid Spanning Tree Protocol. This is the default. |
| **stp** - Specify to use Spanning Tree Protocol. |

### Restrictions

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

### Example

To configure the STP version:

```
DGS-3620-28SC:admin#config stp version mstp
Command: config stp version mstp

Success.

DGS-3620-28SC:admin#
```

To configure the STP version with the same value of the old configuration:

```
DGS-3620-28SC:admin#config stp version mstp
Command: config stp version mstp

Configure value is the same with current value.
Success.

DGS-3620-28SC:admin#
```

## 90-12 config stp priority

### Description

One of the parameters used to select the Root Bridge.

### Format

**config stp priority <value 0-61440> instance_id <value 0-64>**

### Parameters

**<value 0-61440>** - Specify the bridge priority value, which must be divisible by 4096. The default value is 32768.

**instance_id** - Specify the identifier value, which is used to distinguish different STP instances.
- **<value 0-64>** - Specify the identifier value, which is used to distinguish different STP instances.

### Restrictions

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

### Example

To configure the STP instance ID:

```
DGS-3620-28SC:admin#config stp priority 61440 instance_id 0
Command: config stp priority 61440 instance_id 0

Success.

DGS-3620-28SC:admin#
```

## 90-13 config stp

### Description

This command is used to configure the bridge parameter 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]} (1)**

### Parameters

**maxage** - Specify to determine if a BPDU is valid.
- **<value 6-40>** - Specify to determine if a BPDU is valid. The default value is 20.

**maxhops** - Specify to restrict the forwarded times of one BPDU.
- **<value 6-40>** - Specify to restrict the forwarded times of one BPDU. The default value is 20.

**hellotime** - Specify the time interval for sending Configuration BPDUs by the Root Bridge. This parameter is for STP and RSTP version. MSTP version uses per-port hellotime parameter.
- **<value 1-2>** - Specify the time interval for sending Configuration BPDUs by the Root Bridge. This parameter is for STP and RSTP version. MSTP version uses per-port hellotime parameter. The default value is 2 seconds.

**forwarddelay** - Specify the maximum delay time for one BPDU to be transmitted by a bridge and received from another bridge.
- **<value 4-30>**- Specify the maximum delay time for one BPDU to be transmitted by a bridge and received from another bridge. The default value is 15.

**txholdcount** - Specify to restrict the numbers of BPDU transmitted in a time interval (per Hello Time).
- **<value 1-10>** - Specify to restrict the numbers of BPDU transmitted in a time interval (per Hello Time).

**fbpdu** - To decide if the Bridge will flood STP BPDU when STP functionality is disabled.

**enable** - Specify to enable FBPDU.
**disable** - Specify to disable FBPDU.

**nni_bpdu_addr** - Specify to determine the BPDU protocol address for STP in service provide site. It can use 802.1d STP address, 802.1ad service provider STP address.
**dot1d** - Specify to use an 802.1d STP address.
**dot1ad** - Specify to use an 802.1ad service provider STP address.

### Restrictions

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

### Example

To configure STP:

```
DGS-3620-28SC:admin# config stp maxage 25
Command: config stp maxage 25

Success.

DGS-3620-28SC:admin#
```

## 90-14 config stp ports

### Description

This command is used to configure all the parameters of ports, except for Internal Path Cost and Port Priority.

### Format

**config stp ports <portlist> {externalCost [auto | <value 1-200000000> ] | hellotime <value 1-2> | migrate [yes | no] | edge [true | false | auto] | p2p [true | false | auto] | state [enable | disable] | restricted_role [true | false] | restricted_tcn [true | false] | fbpdu [enable | disable ]}(1)**

### Parameters

**<portlist>** - Specify a range of ports.

**externalCost** - Specify the path cost between the MST regions from the transmitting Bridge to the CIST Root Bridge. It is only used at CIST level.
**auto** - Specify to automatically choose the path cost.
**<value 1-200000000>** - Specify a value between 1 and 200000000.

**hellotime** - This is a per-Bridge parameter in RSTP, but it becomes a per-Port parameter in MSTP.
**<value 1-2>** - This is a per-Bridge parameter in RSTP, but it becomes a per-Port parameter in MSTP. The default value is 2.

**migrate** - Operation of management in order to specify the port to send MSTP BPDU for a delay time.
**yes** - Specify for port to send MSTP BPDU for a delay time.
**no** - Specify for port not to send MSTP BPDU for a delay time.

**edge** - Decide if this port is connected to a LAN or a Bridged LAN. In **auto** mode, the bridge will delay for a period to become edge port if no bridge BPDU is received.
**true** - Specify a true edge connection.
**false** - Specify a false edge connection.

**auto** - The bridge will delay for a period to become edge port if no bridge BPDU is received.

**p2p** - Decide if this port is in Full-Duplex or Half-Duplex mode.
**true** - Specify full-duplex mode.
**false** - Specify half-duplex mode.
**auto** - The switch will automatically determine the P2P mode.

**state** - Decide if this port supports the STP functionality.
**enable** - Enable to support STP functionality.
**disable** - Disable STP functionality support.

**restricted_role** - Decide if this port is to be selected as Root Port or not. The default value is false.
**true** - Decide that this port is not to be selected as Root Port.
**false** - Decide that this port is to be selected as Root Port.

**restricted_tcn** - Decide if this port is to propagate a topology change or not. The default value is false.
**true** - Specify not to propagate a topology change.
**false** - Specify to propagate a topology change.

**fbpdu** - Decide if this port will flood STP BPDU when STP functionality is disabled.
**enable** - Enable port to flood STP BPDU when STP functionality is disabled.
**disable** - Disable port from flooding STP BPDU when STP functionality is disabled.

### Restrictions

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

### Example

To configure STP ports:

```
DGS-3620-28SC:admin# config stp ports 1 externalCost auto
Command: config stp ports 1 externalCost auto

Success.

DGS-3620-28SC:admin#
```

## 90-15 config stp mst_ports

### Description

Internal Path Cost and Port Priority of a Port in MSTI can be separately configured to different values from the configuration of CIST (instance ID = 0).

### Format

**config stp mst_ports <portlist> instance_id <value 0-64> {internalCost [auto | <value 1-200000000>] | priority <value 0-240>}(1)**

### Parameters

**<portlist>** - Specify a range of ports.

**instance_id** - Specify an instance ID.
**<value 0-64>** - Instance = 0 represents CIST, Instance from 1 to 64 represents MSTI 1 to MSTI 64.

**internalCost** - The Port Path Cost used in MSTP.
**auto** - Specify to automatically determine the internal cost.

**<value 1-200000000>** - Specify a value between 1 and 200000000.

**priority** - Specify the Port Priority.

**<value 0-240>** - Specify a value between 0 and 240.

### Restrictions

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

### Example

To configure STP MST ports:

```
DGS-3620-28SC:admin# config stp mst_ports 1 instance_id 0 internalCost auto
Command: config stp mst_ports 1 instance_id 0 internalCost auto

Success.

DGS-3620-28SC:admin#
```

# Chapter 91 SSH Commands

| |
|---|
| **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>}(1) |
| **enable ssh** |
| **disable ssh** |
| **show ssh server** |

## 91-1 config ssh algorithm

### Description

This command is used to configure the 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** - Specify an SSH server encryption algorithm.<br>**blowfish** - Specify an SSH server encryption algorithm.<br>**AES(128,192,256)** - Specify an SSH server encryption algorithm.<br>**arcfour** - Specify an SSH server encryption algorithm.<br>**cast128** - Specify an SSH server encryption algorithm.<br>**twofish (128,192,256)** - Specify an SSH server encryption algorithm.<br>**MD5** - Specify an SSH server data integrality algorithm.<br>**SHA1** - Specify an SSH server data integrality algorithm.<br>**DSA** - Specify an SSH server public key algorithm.<br>**RSA** - Specify an SSH server public key algorithm. |
| **enable** - Specify to enable the algorithm.<br>**disable** - Specify to disable the algorithm. |

### Restrictions

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

### Example

To enable an SSH server public key algorithm:

```
DGS-3620-28SC:admin#config ssh algorithm DSA enable
```

```
Command: config ssh algorithm DSA enable

Success.

DGS-3620-28SC:admin#
```

## 91-2 show ssh algorithm

### Description

This command is used to display the SSH authentication algorithm.

### Format

**show ssh algorithm**

### Parameters

None.

### Restrictions

None.

### Example

To show the SSH server algorithms:

```
DGS-3620-28SC: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-3620-28SC:admin#
```

## 91-3 config ssh authmode

### Description

This command is used to update the user authentication for SSH configuration.

### Format

**config ssh authmode [password | publickey | hostbased] [enable | disable]**

### Parameters

| |
|---|
| **password** - Specify the user authentication method.<br>**publickey** - Specify the user authentication method.<br>**hostbased** - Specify the user authentication method. |
| **enable** - Specify to enable the user authentication method.<br>**disable** - Specify to disable the user authentication method. |

### Restrictions

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

### Example

To configure the SSH user authentication method:

```
DGS-3620-28SC:admin#config ssh authmode publickey enable
Command: config ssh authmode publickey enable

Success.

DGS-3620-28SC:admin#
```

## 91-4 show ssh authmode

### Description

This command is used to display the user authentication methods.

### Format

**show ssh authmode**

### Parameters

None.

### Restrictions

None.

### Example

To display the SSH user authentication method:

```
DGS-3620-28SC:admin#show ssh authmode
Command: show ssh authmode

The SSH Authentication Method:
Password    : Enabled
Public Key  : Enabled
Host-based  : Enabled

DGS-3620-28SC:admin#
```

## 91-5 config ssh user

### Description

This command is used to update SSH user information.

### Format

**config ssh user <username 15> authmode [hostbased [hostname <domain_name 32> | hostname_IP <domain_name 32> [<ipaddr> | <ipv6addr>]] | password | publickey]**

### Parameters

| |
|---|
| **<username 15>** - Specify the user name. |
| **authmode** - Specify the authentication mode. |
| **hostbased** - Specify the user authentication method.<br>**hostname** - Specify the host domain name.<br>**<domain_name 32>** - Specify the host domain name. The hostname value can be up to 32 characters long.<br>**hostname_IP** - Specify the host domain name and IP address.<br>**<domain_name 32>** - Specify the host domain name. The hostname value can be up to 32 characters long.<br>**<ipaddr>** - Specify the host IPv4 address.<br>**<ipv6addr>** - Specifies the host IPv6 address. |
| **password** - Specify the user authentication method. |
| **publickey** - Specify the user authentication method. |

### Restrictions

Only Administrator-level users can issue this command.

**Note:** The user account must be created first.

### Example

To update user “danilo” in authentication mode:

```
DGS-3620-28SC:admin#config ssh user danilo authmode publickey
Command: config ssh user danilo authmode publickey

Success.

DGS-3620-28SC:admin#
```

## 91-6 show ssh user authmode

### Description

This command is used to display SSH user information.

### Format

**show ssh user authmode**

### Parameters

None.

### Restrictions

Only Administrator-level users can issue this command.

### Example

To show user information about SSH configuration:

```
DGS-3620-28SC:admin# show ssh user authmode
Command: show ssh user authmode

Current Accounts
User Name       Authentication         Host Name            Host IP
--------------  ---------------        ---------------      -------------
test              Public Key
alpha             Host-based           alpha-local          172.18.61.180
beta              Host-based           beta-local           3000::105

Total Entries : 3

DGS-3620-28SC:admin#
```

## 91-7 config ssh server

### Description

This command is used to configure 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>}(1)**

### Parameters

**maxsession** - Specify the SSH server maximum session at the same time.
**<int 1-8>** - Specify the SSH server maximum session at the same time. The maximum session value must be between 1 and 8. The default value is 8.

**contimeout** - Specify the SSH server connection timeout.
**<sec 30-600>** - Specify the SSH server connection timeout. The connection timeout value must be between 30 and 600 seconds. The default value is 120 seconds.

**authfail** - Specify the user maximum fail attempts.
**<int 2-20>** - Specify the user maximum fail attempts. The maximum authentication fail attempts must be between 2 and 20. The default value is 2.

**rekey** - (Optional) Specify the time to re-generate the session key.
**10min** - Specify 10 minutes to re-generate the session key.
**30min** - Specify 30 minutes to re-generate the session key.
**60min** - Specify 60 minutes to re-generate the session key.
**never** - Do not re-generate the session key.

**port** - Specify a TCP port number between 1 and 65535.
**<tcp_port_number 1-65535>** - Specify a TCP port number between 1 and 65535.

### Restrictions

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

### Example

To configure an SSH server maximum session of 3:

```
DGS-3620-28SC:admin#config ssh server maxsession 3
Command: config ssh server maxsession 3

Success.

DGS-3620-28SC:admin#
```

## 91-8 enable ssh

### Description

This command is used to enable SSH server services.

### Format

**enable ssh**

### Parameters

None.

### Restrictions

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

### Example

To enable SSH:

```
DGS-3620-28SC:admin#enable ssh
Command: enable ssh

Success.

DGS-3620-28SC:admin#
```

## 91-9 disable ssh

### Description

This command is used to disable SSH server services.

### Format

**disable ssh**

### Parameters

None.

### Restrictions

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

### Example

To disable SSH:

```
DGS-3620-28SC:admin#disable ssh
Command: disable ssh

Success.

DGS-3620-28SC:admin#
```

## 91-10 show ssh server

### Description

This command is used to display SSH server general information.

### Format

**show ssh server**

## Parameters

None.

## Restrictions

None.

## Example

To show SSH server:

```
DGS-3620-28SC:admin# show ssh server
Command: show ssh server

The SSH Server Configuration
Maximum Session                    : 3
Connection Timeout                 : 300
Authentication Fail Attempts       : 2
Rekey Timeout                      : 60min
TCP Port Number                    : 22

DGS-3620-28SC:admin#
```

# Chapter 92 SSL Commands

**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 }(1)}

**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 }(1)}

**show ssl** {certificate}

**show ssl cachetimeout**

**config ssl cachetimeout** <value 60-86400>

## 92-1 download ssl certificate

### Description

This command is used to download specified certificates to a device according to the desired key exchange algorithm. For RSA key exchange, a user must download an RSA type certificate and for DHS_DSS must use the DSA certificate for key exchange.

### Format

**download ssl certificate <ipaddr> certfilename <path_filename 64> keyfilename <path_filename 64>**

### Parameters

**<ipaddr>** - Specify the TFTP server IP address.

**certfilename** - Specify the desired certificate file name and the certificate file path in respect to the TFTP server root path. Input characters with a maximum of 64 octets.

**<path_filename 64>** - Specify the desired certificate file name and the certificate file path in respect to the TFTP server root path. Input characters with a maximum of 64 octets. The certificate file name can be up to 64 characters long.

**keyfilename** - Specify the private key file name which accompanies the certificate and the private key file path in respect to the TFTP server root path. Input characters with a maximum of 64 octets.

**<path_filename 64>** - Specify the private key file name which accompanies the certificate and the private key file path in respect to the TFTP server root path. Input characters with a maximum of 64 octets. The private key file name can be up to 64 characters long.

### Restrictions

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

### Example

To download a certificate from a TFTP server:

```
DGS-3620-28SC: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

Success.

DGS-3620-28SC:admin#
```

## 92-2 enable ssl

### Description

This command is used to enable the SSL status and its individual cipher suites. Using the **enable ssl** command will enable the SSL feature, which means SSLv3 and TLSv1. Each cipher suite must be enabled 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}(1)}**

### Parameters

**ciphersuite** - (Optional) This is used for configuring a cipher suite combination.

- **RSA_with_RC4_128_MD5** - Indicate an RSA key exchange with RC4 128 bits encryption and MD5 hash.
- **RSA_with_3DES_EDE_CBC_SHA** - Indicate an RSA key exchange with 3DES_EDE_CBC encryption and SHA hash.
- **DHE_DSS_with_3DES_EDE_CBC_SHA** - Indicate a DH key exchange with 3DES_EDE_CBC encryption and SHA hash.
- **RSA_EXPORT_with_RC4_40_MD5** - Indicate an RSA_EXPORT key exchange with RC4 40 bits encryption and MD5 hash.

### Restrictions

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

### Example

To enable the SSL ciphersuite for RSA_with_RC4_128_MD5:

```
DGS-3620-28SC:admin# enable ssl ciphersuite RSA_with_RC4_128_MD5
Command: enable ssl ciphersuite RSA_with_RC4_128_MD5

Success.

DGS-3620-28SC:admin#
```

To enable SSL:

```
DGS-3620-28SC:admin# enable ssl
Command: enable ssl

Note: Web will be disabled if SSL is enabled.
Success.
```

```

DGS-3620-28SC:admin#
```

## 92-3 disable ssl

### Description

This command is used to disable the SSL feature and supported ciphersuites.

### 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}(1)}**

### Parameters

**ciphersuite** - (Optional) This is used for configuring cipher suite combination.

- **RSA_with_RC4_128_MD5** - Indicate an RSA key exchange with RC4 128 bits encryption and MD5 hash.
- **RSA_with_3DES_EDE_CBC_SHA** - Indicate an RSA key exchange with 3DES_EDE_CBC encryption and SHA hash.
- **DHE_DSS_with_3DES_EDE_CBC_SHA** - Indicate a DH key exchange with 3DES_EDE_CBC encryption and SHA hash.
- **RSA_EXPORT_with_RC4_40_MD5** - Indicate an RSA_EXPORT key exchange with RC4 40 bits encryption and MD5 hash.

### Restrictions

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

### Example

To disable the SSL ciphersuite for RSA_with_RC4_128_MD5:

```
DGS-3620-28SC:admin# disable ssl ciphersuite RSA_with_RC4_128_MD5
Command: disable ssl ciphersuite RSA_with_RC4_128_MD5

Success.

DGS-3620-28SC:admin#
```

To disable the SSL feature:

```
DGS-3620-28SC:admin# disable ssl
Command: disable ssl

Success.

DGS-3620-28SC:admin#
```

## 92-4 show ssl

### Description

This command is used to display the current SSL status and supported ciphersuites.

### Format

**show ssl {certificate}**

### Parameters

**certificate** - (Optional) Specify the certificate type.

### Restrictions

None.

### Example

To display SSL:

```
DGS-3620-28SC:admin# show ssl
Commands: show ssl

SSL Status                                     Disabled

RSA_WITH_RC4_128_MD5                           Enabled
RSA_WITH_3DES_EDE_CBC_SHA                      Enabled
DHE_DSS_WITH_3DES_EDE_CBC_SHA                  Enabled
RSA_EXPORT_WITH_RC4_40_MD5                     Enabled

DGS-3620-28SC:admin#
```

To display the SSL certificate:

```
DGS-3620-28SC:admin#show ssl certificate
Command: show ssl certificate

Loaded with RSA Certificate!

DGS-3620-28SC:admin#
```

## 92-5 show ssl cachetimeout

### Description

This command is used to display the cache timeout value which is designed for a **dlktimer** library to remove the session ID after it has expired. In order to support the resume session feature, the SSL library keeps the session ID on the web server and invokes the **dlktimer** library to remove this session ID by the cache timeout value.

### Format

**show ssl cachetimeout**

### Parameters

None.

### Restrictions

None.

### Example

To show the SSL cache timeout:

```
DGS-3620-28SC:admin# show ssl cachetimeout
Commands: show ssl cachetimeout

Cache timeout is 600 second(s)

DGS-3620-28SC:admin#
```

## 92-6 config ssl cachetimeout

### Description

This command is used to configure the cache timeout value which is designed for the **dlktimer** library to remove the session ID after expiration. In order to support the resume session feature, the SSL library keeps the session ID on the web server, and invokes the **dlktimer** library to remove this session ID by the cache timeout value. The unit of argument's value is second and its boundary is between 60 (1 minute) and 86400 (24 hours). The default value is 600 seconds.

### Format

**config ssl cachetimeout <value 60-86400>**

### Parameters

**cachetimeout** - Specify the SSL cache timeout value attributes. The SSL cache timeout value must be between 60 and 86400 seconds. The default value is 600 seconds

**<value 60-86400>** - Specify the SSL cache timeout value attributes. The SSL cache timeout value must be between 60 and 86400 seconds. The default value is 600 seconds.

### Restrictions

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

### Example

To configure an SSL cache timeout value of 60:

```
DGS-3620-28SC:admin# config ssl cachetimeout 60
```

```
Commands: config ssl cachetimeout 60

Success.
DGS-3620-28SC:admin#
```

# Chapter 93 Stacking Commands

**config stacking_mode** [disable | enable]
**config stacking force_master_role state** [enable | disable]
**show stacking_mode**
**show stack_information**
**show stack_device**
**config box_id current_box_id** <value 1-12> new_box_id [auto | <value 1-12>]
**config box_priority current_box_id** <value 1-12> priority <value 1-63>

## 93-1 config stacking_mode

### Description

This command configures the state of stacking function. By default stacking mode is disabled. Administrators need to specifically configure the stacking mode to make the switch stackable. Stacking mode can be changed under standalone mode only!

### Format

**config stacking_mode [disable | enable]**

### Parameters

**enable** - Specifies that the Switch's stacking capability will be enabled.
**disable** - Specifies that the Switch's stacking capability will be disabled.

### Restrictions

Only Administrator-level users can issue this command.

### Example

To enable stacking mode:

```
DGS-3620-28SC:admin# config stacking_mode enable
Command: config stacking_mode enable

Change Box stacking_mode may cause devices work restart, still continue?(y/n)
y
Please wait, the switch is rebooting...
```

## 93-2 config stacking force_master_role state

### Description

This command is used to configure stacking force master role state. If 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** - Specifies that the Switch's Stacking Force Master Role state will be enabled.
**disable** - Specifies that the Switch's Stacking Force Master Role state will be disabled.

### Restrictions

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

### Example

To enable stacking force master role state:

```
DGS-3620-28SC:admin# config stacking force_master_role state enable
Command: config stacking force_master_role state enable

Success.

DGS-3620-28SC:admin#
```

## 93-3 show stacking_mode

### Description

This command displays 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-3620-28SC:admin# show stacking_mode
Command: show stacking_mode

Stacking mode  : Enabled

DGS-3620-28SC:admin#
```

## 93-4 show stack_information

### Description

This command displays stacking information.

### 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-3620-28SC:admin# show stack_information
Command: show stack_information

Stack topology status:
New device is detected, hot insert may happen after 7 seconds.

Topology     :Duplex_Chain
My Box ID    :3
Master ID    :3
Box Count    :1
Force Master Role: Enable

 Box User                     Prio-                  Prom       Runtime   H/W
 ID  Set  Type          Exist rity        MAC        Version    Version
Version
 --- ---- ------------- ----- ---- ------------------ ---------- --------- ----
----
 1    -   DGS-3620-28SC   No
 2    -   NOT_EXIST       No
 3   User DGS-3620-28SC  Exist  1   00-00-11-33-66-33  1.00.009  1.00.034 A1
 4    -   NOT_EXIST       No
 5    -   NOT_EXIST       No
 6    -   NOT_EXIST       No
 7    -   NOT_EXIST       No
 8    -   NOT_EXIST       No

DGS-3620-28SC:admin#
```

## 93-5 show stack_device

### Description

This command displays stack device information.

### Format

**show stack_device**

### Parameters

None.

### Restrictions

None.

### Example

To display the stack information:

```
DGS-3620-28SC:admin# show stack_device
Command: show stack_device

Box ID     Box Type        H/W Version   Serial Number
-------  ---------------   ------------  ----------------
1          DGS-3620-28SC   A1            D1234567890
2          DGS-3620-28SC   A1            D1234567891

DGS-3620-28SC:admin#
```

## 93-6 config box_id current_box_id

### Description

This command configures 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 1-12> new_box_id [auto | <value 1-12>]**

### Parameters

**<value 1-12>** - Enter the current box ID value used here. This value must be between 1 and 12.

**new_box_id** - Specifies the new ID assigned to the box.

- **auto** - Specifies that the box ID to be assigned automatically by the stack system. The new box ID will take effect after the next boot.
- **<value 1-12>** - Enter the new box ID used here. This value must be between 1 and 12.

### Restrictions

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

### Example

To configure box ID of box 1 to be auto:

```
DGS-3620-28SC: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-3620-28SC:admin#
```

## 93-7 config box_priority current_box_id

### Description

This command configures the priority of switch, which will determines which box becomes master. Lower number means higher priority. New priority will take effect after user reboot

### Format

**config box_priority current_box_id <value 1-12> priority <value 1-63>**

### Parameters

**<value 1-12>** - Enter the current box ID value used here. This value must be between 1 and 12.

**priority** - Specifies the priority assigned to the box, with lower number meaning higher priority.

- **<value 1-63>** - Enter the priority value used here. This value must be between 1 and 63.

### Restrictions

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

### Example

To configure box priority:

```
DGS-3620-28SC:admin# config box_priority current_box_id 1 priority 1
Command: config box_priority current_box_id 1 priority 1

Success.

DGS-3620-28SC:admin#
```

# Chapter 94 Static MAC-based VLAN Commands

**create mac_based_vlan mac_address** <macaddr> [vlan <vlan_name 32> | vlanid <vlanid 1-4094>] {priority <value 0-7>}

**delete mac_based_vlan** {mac_address <macaddr> [vlan <vlan_name 32>| vlanid <vlanid 1-4094>]}

**show mac_based_vlan** {mac_address <macaddr> | [vlan <vlan_name 32> | vlanid <vlanid 1-4094>]}

## 94-1 create mac_based_vlan mac_address

### Description

This command is used to create static MAC-based VLAN entries.

### Format

**create mac_based_vlan mac_address <macaddr> [vlan <vlan_name 32> | vlanid <vlanid 1-4094>] {priority <value 0-7>}**

### Parameters

**<macaddr>** - Specify the MAC address.

**vlan** - Specify the VLAN to be associated with the MAC address. The name must be an existing static VLAN name.
**<vlan_name 32>** - Specify the VLAN name. The maximum length is 32 characters.

**vlanid** - Specify the VLAN ID to be associated with the MAC address. The ID must be an existing static VLAN ID.
**<vlanid 1-4094>** - Specify the VLAN ID between 1 and 4094.

**priority** – (Optional) Specifies the priority that is assigned to untagged packets. If not specified, the priority is the default value 0.
**<value 0-7>** - Enter the priority value used here. This value must be between 0 and 7.

### Restrictions

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

### Example

To create a static MAC-based VLAN entry:

```
DGS-3620-28SC:admin#create mac_based_vlan mac_address 00-00-00-00-00-01 vlan
default
Command: create mac_based_vlan mac_address 00-00-00-00-00-01 vlan default
Success.

DGS-3620-28SC:admin#
```

## 94-2 delete mac_based_vlan

### Description

This command is used to delete static MAC-based VLAN entries.

### Format

**delete mac_based_vlan {mac_address <macaddr> [vlan <vlan_name 32>| vlanid <vlanid 1-4094>]}**

### Parameters

**mac_address** - (Optional) Specify the MAC address to be deleted.
  **<macaddr>** - Specify the MAC address to be deleted.

**vlan** - (Optional) Specify the VLAN associated with the MAC address.
  **<vlan_name 32>** - Specify the VLAN name. The maximum length is 32 characters.

**vlanid** - (Optional) Specify the VLAN ID associated with the MAC address.
  **<vlanid 1-4094>** - Specify the VLAN ID between 1 and 4094.

**Note:** If the MAC address and VLAN are not specified, all static entries associated with the port will be removed.

### Restrictions

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

### Example

To delete a static MAC-based VLAN entry:

```
DGS-3620-28SC:admin#delete mac_based_vlan mac_address 00-00-00-00-00-01 vlan
default
Command: delete mac_based_vlan mac mac_address 00-00-00-00-00-01 vlan default

Success.

DGS-3620-28SC:admin#
```

## 94-3 show mac_based_vlan

### Description

This command is used to display the MAC-based VLAN entries.

### Format

**show mac_based_vlan {mac_address <macaddr> | [vlan <vlan_name 32> | vlanid <vlanid 1-4094>]}**

### Parameters

**mac_address** - (Optional) Specify the MAC address to be displayed.
  **<macaddr>** - Specify the MAC address to be displayed.

**vlan** - (Optional) Specify the VLAN associated with the MAC address.
**<vlan_name 32>** - Specify the VLAN name. The maximum length is 32 characters.

**vlanid** - (Optional) Specify the VLAN ID associated with the MAC address.
**<vlanid 1-4094>** - Specify the VLAN ID 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 configuration. It is assigned to VLAN 400 by MAC-AC. Since MAC AC has higher priority than manual configuration, the manually configured entry will become inactive. To display the MAC-based VLAN entries:

```
DGS-3620-28SC: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      MAC_based Access Control
00-a2-44-17-32-98   400           Active      WAC

Total Entries : 4

DGS-3620-28SC:admin#
```

# Chapter 95 Static Multicast Route Commands

| |
|---|
| **create ipmroute** <network_address> rpf_address [<ipaddr> \| null] |
| **delete ipmroute** [<network_address> \| all] |
| **show ipmroute** {<network_address>} |

## 95-1 create ipmroute

### Description

This command is used to create an IP multicast static route configuration entry. Normally, when an IP multicast packet is received, the source IP address of the packet is used to do the RPF check. When the RPF network is configured for a network, if the source IP address of the received IP multicast packet matches this network, the RPF network will be used to do RPF check.

The IP multicast static route can be assigned to the RPF check path to the Switch in order to control the IP multicast routing path. It needs to work with a multicast route protocol such as PIM. It takes higher priority than unicast route information and multicast route information when the RPF checking is done. The RPF check rule will first check whether it matches an entry in the IP multicast static route table before continuing.

### Format

**create ipmroute <network_address> rpf_address [<ipaddr> | null]**

### Parameters

| |
|---|
| **<network_address>** - Specifies the source IP address of the received IP multicast packet matches this network, the RPF address is used to do RPF check. |
| **rpf_address** - Specifies the IP address, it means that if the source IP address of the received IP multicast packet match the network_address, rpf_address will be used to check whether packet receive from legal interface.<br>**<ipaddr>** - Enter the RPF IP address used here.<br>**null** - Specifies that if it is set to null, it means that if the source IP address in the received IP multicast packet match network_address, RPF check will always fail. |

### Restrictions

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

### Example

To create ip multicast static route entry:

```
DGS-3620-28SC:admin# create ipmroute 11.0.0.0/8 rpf_address 20.1.2.3
Command: create ipmroute 11.0.0.0/8 rpf_address 20.1.2.3

Success.

DGS-3620-28SC:admin#
```

## 95-2 delete ipmroute

### Description

This command is used to delete an IP multicast static route configuration entry.

### Format

**delete ipmroute [<network_address> | all]**

### Parameters

**<network_address>** - Enter the network address that will be deleted here.
**all** - Specifies that all the IP multicast static routes will be deleted.

### Restrictions

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

### Example

To delete ip multicast static route entry:

```
DGS-3620-28SC:admin# delete ipmroute 11.0.0.0/8
Command: delete ipmroute 11.0.0.0/8

Success.

DGS-3620-28SC:admin#
```

## 95-3 show ipmroute

### Description

This command is used to display the IP multicast static route configuration entry.

### Format

**show ipmroute {<network_address>}**

### Parameters

**<network_address>** - (Optional) Enter the network address used here. If the IP multicast packet received matches it, we will use the RPF address configured to do RPF checking.

If no parameter is specified, the system will display all static multicast route configurations.

## Restrictions

None.

## Example

To display ip multicast static route entry:

```
DGS-3620-28SC:admin# show ipmroute 11.0.0.0/8
Command: show ipmroute 11.0.0.0/8

Index    Source IP Address      RPF IP Address
-----    --------------------   ---------------------
1        11.0.0.0/8             20.1.2.3

Total Entries:1

DGS-3620-28SC:admin#
```

# Chapter 96 Subnet VLAN Commands

| |
|---|
| **create subnet_vlan** [network <network_address> \| ipv6network <ipv6networkaddr>] [vlan <vlan_name 32> \| vlanid <vlanid 1-4094>] {priority <value 0-7>} |
| **delete subnet_vlan** [network <network_address> \| ipv6network <ipv6networkaddr> \| vlan <vlan_name 32> \| vlanid <vidlist> \| all] |
| **show subnet_vlan** {[network <network_address> \| ipv6network <ipv6networkaddr> \| vlan <vlan_name 32> \| vlanid <vidlist>]} |
| **config vlan_precedence ports** <portlist> [mac_based_vlan \| subnet_vlan] |
| **show vlan_precedence ports** {<portlist>} |

## 96-1 create subnet_vlan

### Description

This command is used to create a subnet VLAN entry. A subnet VLAN entry is an IP subnet-based VLAN classification rule. If an untagged or priority-tagged IP packet is received on a port, its source IP address will be used to match the subnet VLAN entries. If the source IP is in the subnet of an entry, the packet will be classified to the VLAN defined for this subnet.

### Format

**create subnet_vlan [network <network_address> | ipv6network <ipv6networkaddr>] [vlan <vlan_name 32> | vlanid <vlanid 1-4094>] {priority <value 0-7>}**

### Parameters

**network** - Specify an IPv4 network address.
**<network_address>** - Specify an IPv4 network address. The format is ipaddress/prefix length.

**ipv6network** - Specify an IPv6 network address.
**<ipv6networkaddr>** - Specify an IPv6 network address. The format is ipaddress/prefix length. The prefix length of IPv6 network address shall not be greater than 64.

**vlan** - Specify a VLAN name to be associated with the subnet. The VLAN must be an existing static VLAN.
**<vlan_name 32>** - Specify a VLAN name. The maximum length is 32 characters.

**vlanid** - Specify the VLAN ID to be associated with the subnet. The VLAN must be an existing static VLAN.
**<vlanid 1-4094>** - Specify the VLAN ID between 1 and 4094.

**priority** - (Optional) Specify the priority to be associated with the subnet.
**<value 0-7>** - Specify the priority to be associated with the subnet. The range is 0 to 7.

### Restrictions

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

### Example

To create a subnet VLAN entry:

```
DGS-3620-28SC:admin#create subnet_vlan network 172.168.1.1/24 vlan v2 priority
2
Command: create subnet_vlan network 172.168.1.1/24 vlan v2 priority 2

Success.

DGS-3620-28SC:admin#
```

To create an IPv6 subnet VLAN entry:

```
DGS-3620-28SC:admin# create subnet_vlan ipv6network fe80:250:baff::0/64 vlan v2
priority 2
Command: create subnet_vlan ipv6network fe80:250:baff::0/64 vlan v2 priority 2

Success.

DGS-3620-28SC:admin#
```

## 96-2 delete subnet_vlan

### Description

This command is used to delete a subnet VLAN from the switch. Users can delete a subnet VLAN entry by IP subnet or VLAN, or delete all subnet VLAN entries.

### Format

**delete subnet_vlan [network <network_address> | ipv6network <ipv6networkaddr> | vlan <vlan_name 32> | vlanid <vidlist> | all]**

### Parameters

**network** - Specify an IPv4 network address.
  **<network_address>** - Specify an IPv4 network address. The format is ipaddress/prefix length.

**ipv6network** - Specify an IPv6 network address.
  **<ipv6networkaddr>** - Specify an IPv6 network address. The format is ipaddress/prefix length.

**vlan** - Specify to delete all subnet VLAN entries associated with this VLAN.
  **<vlan_name 32>** - Specify a VLAN name. The maximum length is 32 characters.

**vlanid** - Specify a list of VLANs by VLAN ID.
  **<vidlist>** - Specify the VLAN ID.

**all** - Specify to delete all subnet VLAN entries.

### Restrictions

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

### Example

To delete a subnet VLAN entry:

```
DGS-3620-28SC:admin#delete subnet_vlan network 172.168.1.1/24
Command: delete subnet_vlan network 172.168.1.1/24

Success.

DGS-3620-28SC:admin#
```

To delete all subnet VLAN entries:

```
DGS-3620-28SC:admin#delete subnet_vlan all
Command: delete subnet_vlan all

Success.

DGS-3620-28SC:admin#
```

## 96-3 show subnet_vlan

### Description

This command is used to display a subnet VLAN.

### Format

**show subnet_vlan {[network <network_address> | ipv6network <ipv6networkaddr> | vlan <vlan_name 32> | vlanid <vidlist>]}**

### Parameters

**network** - (Optional) Specify an IPv4 network address.
**<network_address>** - Specify an IPv4 network address. The format is ipaddress/prefix length.

**ipv6network** - (Optional) Specify an IPv6 network address.
**<ipv6networkaddr>** - Specify an IPv6 network address. The format is ipaddress/prefix length.

**vlan** - (Optional) Specify to display all subnet VLAN entries associated with this VLAN.
**<vlan_name 32>** - Specify a VLAN name. The maximum length is 32 characters.

**vlanid** - (Optional) Specify a list of VLANs by VLAN ID.
**<vidlist>** - Specify the VLAN ID.

**Note:** If no parameter is specified, all subnet VLAN information will be displayed.

### Restrictions

None.

### Example

To display a specified subnet VLAN entry:

```
DGS-3620-28SC:admin#show subnet_vlan network 172.168.1.1/24
Command: show subnet_vlan network 172.168.1.1/24

```

```
IP Address/Subnet Mask         VLAN      Priority
------------------------       -----    ----------
172.168.1.1/255.255.255.0      10          2

DGS-3620-28SC:admin#
```

To display a specied IPv6 subnet VLAN entry:

```
DGS-3620-28SC:admin# show subnet_vlan ipv6network fe80:250:baff::0/64
Command: show subnet_vlan ipv6network fe80:250:baff::0/64

IP Address/Subnet Mask         VLAN      Priority
------------------------       -----    ----------
fe80:250:baff::0/64            10          2

DGS-3620-28SC:admin#
```

To display all subnet VLAN entries:

```
DGS-3620-28SC:admin#show subnet_vlan
Command: show subnet_vlan

IP Address/Subnet Mask         VLAN      Priority
------------------------       -----    ----------
172.168.1.1/255.255.255.0       10          2
172.18.211.1/255.255.255.0      20          3
172.18.211.6/255.255.255.0      5           1
fe80:250:baff::0/64             10          2

Total Entries: 4

DGS-3620-28SC:admin#
```

## 96-4 config vlan_precedence ports

### Description

This command is used to configure vlan classification precedence on each port.

You can specify the order of MAC-based VLAN classification and subnet VLAN classification.

If a port’s VLAN classification is MAC-based precedence, MAC-based VLAN classification will process at first. If MAC-based VLAN classification fails, the subnet VLAN classification will be executed.

If a port’s VLAN classification is subnet VLAN precedence, the subnet VLAN classification will process at first. If subnet VLAN classification fails, the MAC-based VLAN classification will be executed.

### Format

**config vlan_precedence ports <portlist> [mac_based_vlan | subnet_vlan]**

### Parameters

**<portlist>** - Enter a list of ports used for this configuration here.

**mac_based_vlan** - Specifies that the MAC-based VLAN classification is precedence than subnet VLAN classification

**subnet_vlan** - Specifies that the subnet VLAN classification is precedence than MAC-based VLAN classification

### Restrictions

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

### Example

To configure subnet VLAN classification precedence on port 1:

```
DGS-3620-28SC:admin# config vlan_precedence ports 1 subnet_vlan
Command: config vlan_precedence ports 1 subnet_vlan

Success.

DGS-3620-28SC:admin#
```

## 96-5 show vlan_precedence ports

### Description

This command is used to display the VLAN classification precedence.

### Format

**show vlan_precedence ports {<portlist>}**

### Parameters

**<portlist>** - (Optional) Specifies the list of ports used for this display.

### Restrictions

None.

### Example

To display VLAN classification precedence on ports 1-5:

```
DGS-3620-28SC:admin#show vlan_precedence ports 1:1-1:5
Command: show vlan_precedence ports 1:1-1:5

Port      VLAN Precedence
----      -----------------
1         MAC-Based VLAN
2         Subnet VLAN
3         MAC-Based VLAN
4         MAC-Based VLAN
5         Subnet VLAN

DGS-3620-28SC:admin#
```

# Chapter 97 Super VLAN and Sub-VLAN Commands

| |
|---|
| **create super_vlan** [<vlan_name 32> \| vlanid <vlanid 1-4094>] {sub_vlan <vidlist>} |
| **config super_vlan** [<vlan_name 32> \| vlanid <vlanid 1-4094>] [add \| delete] sub_vlan <vidlist> |
| **delete super_vlan** [<vlan_name 32> \| vlanid <vlanid 1-4094>] |
| **config sub_vlan** [<vlan_name 32> \| vlanid <vlanid 1-4094>] [add \| delete] ip_range <ipaddr> to <ipaddr> |
| **show super_vlan** {[<vlan_name 32> \| vlanid <vlanid 1-4094>]} |
| **show sub_vlan** {[<vlan_name 32> \| vlanid <vidlist>]} |

## 97-1 create super_vlan

### Description

This command is used to create a super VLAN. The specified VLAN must be an 802.1Q VLAN. If the specified VLAN does not exist, the operation will fail.

✎ **Note:** A Layer 3 Routing Protocol, like VRRP, the Multicast Protocol, and the IPv6 Protocol cannot run on a super VLAN interface.

Super VLANs are used to aggregate multiple sub-VLANs in the same IP subnet.

A sub-VLAN is a Layer 2, separated broadcast domain. The super VLAN cannot have any physical member ports and hosts that resides within any sub-VLANs. Once an IP interface is bound to a super VLAN, the proxy ARP will be enabled automatically on the specified interface for the communication between its sub-VLANs. If an IP interface is bound to a super VLAN, it cannot be bound to any other VLANs.

A super VLAN cannot be a sub-VLAN of other super VLANs.

### Format

**create super_vlan [<vlan_name 32> | vlanid <vlanid 1-4094>] {sub_vlan <vidlist>}**

### Parameters

| |
|---|
| **<vlan_name 32>** - Enter the VLAN name used here. This name can be up to 32 characters long.<br>**vlanid** - Specifies the VLAN ID used.<br>**<vlanid 1-4094>** - Enter the VLAN ID used here. This value must be between 1 and 4094. |
| **sub_vlan** - (Optional) Specifies the sub-VLANs of the super VLAN. By default, a new created super VLAN has no sub-VLANs configured.<br>**<vidlist>** - Enter the VLAN ID of the sub-VLAN used here. This value must be between 1 and 4094. |

### Restrictions

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

### Example

To create super VLAN 10:

```
DGS-3620-28SC:admin# create super_vlan vlanid 10
Command: create super_vlan vlanid 10

Success.

DGS-3620-28SC:admin#
```

## 97-2 config super_vlan

### Description

This command is used to configure the sub-VLANs of a super VLAN. A sub-VLAN only can belong to one super VLAN and you cannot bind an IP interface on it. The maximum sub-VLAN number of a super VLAN is 80.

### Format

**config super_vlan [<vlan_name 32> | vlanid <vlanid 1-4094>] [add | delete] sub_vlan <vidlist>**

### Parameters

**<vlan_name 32>** - Enter the VLAN name used here. This name can be up to 32 characters long.
**vlanid** - Specifies the VLAN ID used.
    **<vlanid 1-4094>** - Enter the VLAN ID used here. This value must be between 1 and 4094.

**add** - Specifies the sub-VLAN ID list to add to the super VLAN. The sub-VLAN shall be an existent 802.1Q VLAN.
**delete** - Specifies the sub-VLAN ID list to delete from the super VLAN.

**sub_vlan** - Specifies the sub-VLANs of the super VLAN. By default, a new created super VLAN has no sub-VLANs configured.
    **<vidlist>** - Enter the VLAN ID of the sub-VLAN used here. This value must be between 1 and 4094.

### Restrictions

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

### Example

To add sub VLAN 2-4 into super VLAN 10:

```
DGS-3620-28SC:admin# config super_vlan 10 add sub_vlan 2-4
Command: config super_vlan 10 add sub_vlan 2-4

Success.

DGS-3620-28SC:admin#
```

## 97-3 delete super_vlan

### Description

This command is used to delete a super VLAN.

### Format

**delete super_vlan [<vlan_name 32> | vlanid <vlanid 1-4094>]**

### Parameters

**<vlan_name 32>** - Enter the VLAN name used here. This name can be up to 32 characters long.
**vlanid** - Specifies the VLAN ID used.
**<vlanid 1-4094>** - Enter the VLAN ID used here. This value must be between 1 and 4094.

### Restrictions

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

### Example

To delete the super VLAN by specify the VLAN ID 10:

```
DGS-3620-28SC:admin# delete super_vlan vlanid 10
Command: delete super_vlan vlanid 10

Success.

DGS-3620-28SC:admin#
```

## 97-4 config sub_vlan

### Description

This command is used to configure the IP range of the sub-VLAN.

A sub-VLAN can has one or more IP ranges. Configuring IP range of sub-VLAN can reduce the ARP traffic in the super VLAN. That is multiple IP (ranges) is allowed to map to one sub-VLAN. One IP can not map to multiple sub-VLANs, if one IP is mapped to multiple VLAN it may cause traffic forwarding to the wrong VLAN.

### Format

**config sub_vlan [<vlan_name 32> | vlanid <vlanid 1-4094>] [add | delete] ip_range <ipaddr> to <ipaddr>**

### Parameters

**<vlan_name 32>** - Enter the VLAN name used here. This name can be up to 32 characters long.
**vlanid** - Specifies the VLAN ID used.
**<vlanid 1-4094>** - Enter the VLAN ID used here. This value must be between 1 and 4094.

**add** - Specifies the IP range of the sub-VLAN that will be added.
**delete** - Specifies the IP range of the sub-VLAN that will be deleted.

**ip_range** - Specifies the IP range of the sub-VLAN that will be used.
**<ipaddr>** - Enter the starting IP address used here.
**to** - Specifies that the next IP address will be the ending IP address.
**<ipaddr>** - Enter the ending IP address used here.

### Restrictions

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

### Example

To configure IP range of sub VLAN 1 to 10.1.1.1-10.1.1.3:

```
DGS-3620-28SC:admin# config sub_vlan vlanid 1 add ip_range 10.1.1.1 to 10.1.1.3
Command: config sub_vlan vlanid 1 add ip_range 10.1.1.1 to 10.1.1.3

Success.

DGS-3620-28SC:admin#
```

## 97-5 show super_vlan

### Description

This command is used to display the super VLAN parameters.

### Format

**show super_vlan {[<vlan_name 32> | vlanid <vlanid 1-4094>]}**

### Parameters

**<vlan_name 32>** - (Optional) Enter the super VLAN name used here. This name can be up to 32 characters long.
**vlanid** - (Optional) Specifies the super VLAN ID used.
**<vlanid 1-4094>** - Enter the super VLAN ID used here. This value must be between 1 and 4094.

### Restrictions

None.

### Example

To show super VLAN:

```
DGS-3620-28SC:admin# show super_vlan
Command: show super_vlan

Super VID : 3
 VLAN Name : super3
 IP Subnet: 172.6.0.254/16
 Status   : Inactive
 Sub VID  : 200-204

Total Entries: 1

DGS-3620-28SC:admin#
```

## 97-6 show sub_vlan

### Description

This command is used to show sub-VLAN.

### Format

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

### Parameters

**<vlan_name 32>** - (Optional) Enter the sub-VLAN name used here. This name can be up to 32 characters long.

**vlanid** - (Optional) Specifies the sub-VLAN ID used.

**<vidlist>** - Enter the sub-VLAN ID used here. This value must be between 1 and 4094.

### Restrictions

None.

### Example

To show all sub-VLAN:

```
DGS-3620-28SC:admin# show sub_vlan
Command: show sub_vlan

Sub VID   Status      Super VID     IP Range
-------   -------    ----------    ------------------------
  1          Active     10          10.1.1.1-10.1.1.10
                                    10.1.2.1-10.1.2.20
  2          Active     10          10.1.3.0-10.1.3.100
  3          Inactive   10          10.1.4.0-10.1.4.255
  4          Active     20          10.1.5.0-10.1.5.255
  5          Inactive   20          10.1.6.0-10.1.6.255

Total Entries: 5

DGS-3620-28SC:admin#
```

# Chapter 98 Switch Port Commands

|  |
|---|
| **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]}] \| 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]}(1) |
| **show ports** {<portlist>} {[description \| err_disabled \| auto_negotiation \| details \| media_type]} |

## 98-1 config ports

### Description

This command is used to change switch 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]}] | 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]}(1)**

### Parameters

|  |
|---|
| **<portlist>** - Specify a range of ports to be configured.<br>**all** – Specify to set all ports in the system. |
| **medium_type** - (Optional) Specify the medium type when configuring ports that are combo ports.<br>**fiber** - Specify the fiber port.<br>**copper** - Specify the copper port. |
| **speed** - Set port speed for the specified ports.<br>**auto** - Set port speed to auto negotiation.<br>**capability_advertised** - Specifies that the capability will be advertised.<br>**10_half** - Set port speed to 10_half.<br>**10_full** - Set port speed to 10_full.<br>**100_half** - Set port speed to 100_half.<br>**100_full** - Set port speed to 100_full.<br>**1000_full** - Set port speed to 1000_full. When setting copper port speed to 1000_full, users should specify master and slave mode in pair for 1000-BASE TX, and leave the 1000_full without any master or slave setting for fiber.<br>**master** - (Optional) Set to master.<br>**slave** - (Optional) Set to slave. |
| **auto_negotiation** - Specifies that the auto-negotiation option will be configured.<br>**restart_an** - Specifies to restart the auto-negotiation process.<br>**remote_fault_advertised** - Specifies that the remote fault advertisement option will be configured.<br>**disable** - Specifies to disable remote fault advertisement. |

**offline** - Specifies 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** - Specifies 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** - Specifies 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** - Turn on or turn off flow control on one or more ports by setting flow_control to enable or disable. The default value is disable.

**enable** - Turn on flow control.

**disable** - Turn off flow control.

**learning** - Turn on or turn off MAC address learning on one or more ports. The default value is enable.

**enable** - Turn on MAC address learning.

**disable** - Turn off MAC address learning.

**state** - Enable or disable the state of the specified port. If the ports are in error-disabled status, configuring their state to enable will recover these ports from a disabled to an enabled state. The default value is enable.

**enable** - Enable the specified port(s).

**disable** - Disable the specified port(s).

**mdix** - Specify the type of cabling. The default value is auto.

**auto** - Select auto for auto sensing of the optimal type of cabling.

**normal** - Select normal for normal cabling. If set to normal state, the port is in MDI mode and can be connected to a PC NIC using a straight-through calbe or a port (in MDI mode) on another switch through a cross-over cable.

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

**description** - (Optional) Describe the port interface.

**<desc 1-32>** - Describe the port interface.

**clear_description** - (Optional) Deletes the present description of the port interface.

### Restrictions

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

### Example

To configure the speed of ports 1 to 3 to be 10 Mbps, with full duplex, learning enabled, state enabled, and flow control enabled:

```
DGS-3620-28SC:admin#config ports 1-3 speed 10_full state enable learning enable
flow_control enable
Command: config ports 1-3 speed 10_full state enable learning enable
flow_control enable

Success.

DGS-3620-28SC:admin#
```

## 98-2 show ports

### Description

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

## Format

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

## Parameters

**<portlist>** - (Optional) Specify 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) Specifies to display detailed auto-negotiation information.

**details** - (Optional) Specify to indicate if port detail information will be included in the display.

**media_type** - (Optional) Specify to display the current port media type. For FE ports, the media type should be 100BASE-T. For GE ports (the combo port), if the current active port is the fiber port, the media type is 1000BASE-X or 100BASE-X; if the current active port is the copper port, the media type is 1000BASE-T.

**Note:** If no parameter is specified, all ports will be displayed.

## Restrictions

None.

## Example

To display the configuration of ports 1 to 4:

```
DGS-3620-28SC:admin#show ports 1:1-1:4
Command: show ports 1:1-1:4

 Port      State/          Settings             Connection          Address
           MDIX      Speed/Duplex/FlowCtrl  Speed/Duplex/FlowCtrl   Learning
 -------  --------  ---------------------  ----------------------  ---------
 1:1      Enabled   Auto/Disabled          Link Down               Enabled
          Auto
 1:2      Enabled   Auto/Disabled          Link Down               Enabled
          Auto
 1:3      Enabled   Auto/Disabled          Link Down               Enabled
          Auto
 1:4      Enabled   Auto/Disabled          Link Down               Enabled
          Auto
CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

To display the description information of ports 1 to 4:

```
DGS-3620-28SC:admin# show ports 1-4 description
Command: show ports 1:1-1:4 description

 Port      State/          Settings             Connection          Address
           MDIX      Speed/Duplex/FlowCtrl  Speed/Duplex/FlowCtrl   Learning
 -------  --------  ---------------------  ----------------------  ---------
 1:1      Enabled   Auto/Disabled          Link Down               Enabled
```

```
          Auto
          Description:
 1:2      Enabled   Auto/Disabled          Link Down               Enabled
          Auto
          Description:
 1:3      Enabled   Auto/Disabled          Link Down               Enabled
          Auto
          Description:
 1:4      Enabled   Auto/Disabled          Link Down               Enabled
          Auto
          Description:
CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

**Note:** Connection status has the following situations: Link Down, Speed/Duplex/FlowCtrl (link up), and Err-Disabled.

To display port error-disabled information:

```
DGS-3620-28SC:admin# show ports err_disabled
Command: show ports err_disabled

Port    Port      Connection Status      Reason
        State
------  --------  ---------------------  ----------------
1       Enabled   Err-Disabled           Storm control
        Description: port1.
8       Enabled   Err-Disabled           Storm control
        Description: port8.

DGS-3620-28SC:admin#
```

# Chapter 99 System Severity Commands

**config system_severity** [trap | log | all] [emergency | alert | critical | error | warning | notice | information | debug | <level 0-7>]

**show system_severity**

## 99-1 config system_severity

### Description

This command is used to configure severity level control for the system.

### Format

**config system_severity [trap | log | all] [emergency | alert | critical | error | warning | notice | information | debug | <level 0-7>]**

### Parameters

**trap** - Configure severity level control for a trap.

**log** - Configure severity level control for a log.

**all** - Configure severity level control for a trap and a log.

**emergency** - Specify to configure the severity level for emergency messages.

**alert** - Specify to configure the severity level for alert messages.

**critical** - Specify to configure the severity level for critical messages.

**error** - Specify to configure the severity level for error messages.

**warning** - Specify to configure the severity level for warning messages.

**notice** - Specify to configure the severity level for notice messages.

**informational** - Specify to configure the severity level for informational messages.

**debug** - Specify to configure the severity level for debug messages.

**<level 0-7>** - Specify to configure a severity level between 0 and 7.

### Restrictions

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

### Example

To configure severity level control for information level for a trap:

```
DGS-3620-28SC:admin#config system_severity trap information
Command: config system_severity trap information
```

```
Success.

DGS-3620-28SC:admin#
```

## 99-2 show system_severity

### Description

This command is used to show the severity level control for a system.

### Format

**show system_severity**

### Parameters

None.

### Restrictions

None.

### Example

To show the severity level control for a system:

```
DGS-3620-28SC:admin#show system_severity
Command: show system_severity

System Severity Trap : warning
System Severity Log  : information

DGS-3620-28SC:admin#
```

# Chapter 100 Tech Support Commands

**show tech_support**

**upload tech_support_toTFTP** <ipaddr> <path_filename 64>

## 100-1 show tech_support

### Description

This command is used to display technical support information. It is especially useful for technical support personnel that need to view the overall device operation information.

### Format

**show tech_support**

### Parameters

None.

### Restrictions

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

**Note:** The switch may become inaccessible when dumping the technical support data.

**Note:** The management session may time out if dumping technical support data takes longer than the configured session timeout period. It is strongly recommended to set the serial port timeout to never to disable the auto disconnection of the console session.

### Example

To display technical support information:

```
DGS-3620-28SC:admin#show tech_support
Command: show tech_support

#-------------------------------------------------------------------------------
#                      DGS-3620-28SC Gigabit Ethernet Switch
#                          Technical Support Information
#
#                            Firmware: Build 2.00.015
#           Copyright(C) 2012  D-Link Corporation. All rights reserved.
```

```
#-----------------------------------------------------------------------------


********************   Basic System Information   ********************


[SYS 2000-1-24 03:05:29]


Boot Time            : 24 Jan 2000  03:01:12

RTC Time             : 2000/01/24 03:05:29

Boot PROM Version    : Build 1.00.016

Firmware Version     : Build 2.00.015

Hardware Version     : A1

Serial number        : QT3Z567890123

MAC Address          : 5C-D9-98-11-22-33

[STACKING 2000-1-24 03:05:29]


 #Topology Information


 Stable Topology:

 My Box ID : 1              Role          : Master

 Box Cnt   : 1              Topology Type : Duplex Chain

 Unit  Prio-                                    Device Runtime   Stacking

 ID    rity  Role           MAC        Type       option version   version

 ----- ----  ------- ----------------- ---------- ------ --------- -------
□ 1     32 32 Master  5C-D9-98-11-22-33 DGS-3620-28SC 0x0002 2.00.015  2.0.1
```

## 100-2 upload tech_support_toTFTP

### Description

This command is used to upload technical support information to a TFTP server. This command can be interrupted by Ctrl – C or ESC when it is executing.

### Format

**upload tech_support_toTFTP <ipaddr> <path_filename 64>**

## Parameters

**<ipaddr>** - Specify the IPv4 address of the TFTP server.

**<path_filename 64>** - Specify the file name of the technical support information file sent to the TFTP server. The maximum size of the file name is 64 characters.

## Restrictions

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

## Example

To upload technical support information:

```
DGS-3620-28SC:admin#upload tech_support_toTFTP 10.0.0.66 tech_suppport.txt
Command: upload tech_support_toTFTP 10.0.0.66 tech_suppport.txt

Connecting to server.................. Done.
Upload techsupport file............... Done.

Success.

DGS-3620-28SC:admin#
```

# Chapter 101 Time and SNTP Commands

| |
|---|
| **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>} (3) |
| **config dst** [disable \| repeating {s_week <start_week 1-4,last> \| s_day <start_day sun-sat> \| s_mth <start_mth 1-12> \| s_time <start_time hh:mm> \| e_week <end_week 1-4, last> \| e_day <end_day sun-sat> \| e_mth <end_mth 1-12> \| e_time <end_time hh:mm> \| offset [30 \| 60 \| 90 \| 120]} (9) \| annual {s_date <start_date 1-31> \| s_mth <start_mth 1-12> \| s_time <start_time hh:mm> \| e_date <end_date 1-31> \| e_mth <end_mth 1-12> \| e_time <end_time hh:mm> \| offset [30 \| 60 \| 90 \| 120]}(7)] |
| **show time** |

## 101-1 config sntp

### Description

This command is used to change SNTP configurations.

### Format

**config sntp {primary <ipaddr> | secondary <ipaddr> | poll-interval <int 30-99999>} (1)**

### Parameters

| |
|---|
| **primary** - (Optional) Specify the SNTP primary server IP address.<br>**<ipaddr>** - Specify the SNTP primary server IP address. |
| **secondary** - (Optional) Specify the SNTP secondary server IP address.<br>**<ipaddr>** - Specify the SNTP secondary server IP address. |
| **poll-interval** - (Optional) Specify the polling interval range.<br>**<int 30-99999>** - Specify the polling interval range between 30 and 99999 seconds. |

### Restrictions

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

### Example

To configure SNTP:

```
DGS-3620-28SC: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-3620-28SC:admin#
```

## 101-2 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>** - Specify the IPv6 address of the Primary SNTP IPv6 server.

**secondary** - SNTP secondary IPv6 server address.
    **<ipv6addr>** - Specify the IPv6 address of the Secondary SNTP IPv6 server.

### Restrictions

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

### Example

To configure SNTP (primary IPv6 server: 1000::1, secondary IPv6 server: 1000::2):

```
DES-3620-28SC:admin#config sntp ipv6server primary 1000::1 secondary 1000::2
Command: config sntp ipv6server primary 1000::1 secondary 1000::2

Success.

DES-3620-28SC:admin#
```

## 101-3 show sntp

### Description

This command is used to display the current SNTP time source and configuration.

### Format

**show sntp**

### Parameters

None.

### Restrictions

None.

### Example

To show SNTP:

```
DGS-3620-28SC:admin#show sntp
Command: show sntp

Current Time Scource      : System Clock
SNTP Status               : Disabled
IPv4 Primary SNTP Server  : None
IPv4 Secondary SNTP Server: None
IPv6 Primary SNTP Server  : None
IPv6 Secondary SNTP Server: None
SNTP Poll Interval        : 720 sec

DGS-3620-28SC:admin#
```

## 101-4 enable sntp

### Description

This command is used to turn on SNTP support.

### Format

**enable sntp**

### Parameters

None.

### Restrictions

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

### Example

To enable SNTP:

```
DGS-3620-28SC:admin#enable sntp
Command: enable sntp

Success.

DGS-3620-28SC:admin#
```

## 101-5 disable sntp

### Description

This command is used to turn off SNTP support.

### Format

**disable sntp**

### Parameters

None.

### Restrictions

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

### Example

To disable SNTP:

```
DGS-3620-28SC:admin#disable sntp
Command: disable sntp

Success.

DGS-3620-28SC:admin#
```

## 101-6 config time

### Description

This command is used to change the time settings.

### Format

**config time <date ddmthyyyy> <time hh:mm:ss>**

### Parameters

| |
|---|
| **<date ddmthyyyy>** - Specify the system clock date. |
| **<time hh:mm:ss>** - Specify the system clock time. |

### Restrictions

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

### Example

To configure time:

```
DGS-3620-28SC:admin# config time 30jun2003 16:30:30
Command: config time 30jun2003 16:30:30

Success.

DGS-3620-28SC:admin#
```

## 101-7 config time_zone

### Description

This command is used to change time zone settings.

### Format

**config time_zone {operator [+ | -] | hour <gmt_hour 0-13> | min <minute 0-59>} (3)**

### Parameters

**operator** - Specify the operator of the time zone.
**+** - Positive.
**-** - Negative.

**hour** - Specify the hour of the time zone.
**<gmt_hour 0-13>** - Specify the hour of the time zone between 0 and 13.

**min** - Specify the minute of the time zone.
**<minute 0-59>** - Specify the minute of the time zone between 0 and 59.

### Restrictions

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

### Example

To configure the time zone:

```
DGS-3620-28SC:admin#config time_zone operator + hour 2 min 30
Command: config time_zone operator + hour 2 min 30

Success.

DGS-3620-28SC:admin#
```

## 101-8 config dst

### Description

This command is used to change Daylight Saving Time settings.

### Format

**config dst [disable | repeating {s_week <start_week 1-4,last> | s_day <start_day sun-sat> | s_mth <start_mth 1-12> | s_time <start_time hh:mm> | e_week <end_week 1-4, last> | e_day <end_day sun-sat> | e_mth <end_mth 1-12> | e_time <end_time hh:mm> | offset [30 | 60 | 90**

**| 120]} (9) | annual {s_date <start_date 1-31> | s_mth <start_mth 1-12> | s_time <start_time hh:mm> | e_date <end_date 1-31> | e_mth <end_mth 1-12> | e_time <end_time hh:mm> | offset [30 | 60 | 90 | 120]} (7) ]**

## Parameters

**disable** - Disable the DST of the switch.

**repeating** - Set the DST to repeating mode.

**s_week** - Configure the start week number of DST.
**<start_week 1-4,last>** - Configure the start week number of DST. The values are 1 to 4.

**s_day** - Configure the start day number of DST.
**<start_day sun-sat>** - Configure the start day number of DST. The values are sun, mon, tue, wed, thu, fri and sat.

**s_mth** - Configure the start month number of DST.
**<start_mth 1-12>** - Configure the start month number of DST. The values are 1 to 12.

**s_time** - Configure the start time of DST.
**<start_time hh:mm>** - Configure the start time in hh:mm of DST.

**e_week** - Configure the end week number of DST.
**<end_week 1-4,last>** - Configure the end week number of DST. The values are 1 to 4.

**e_day** - Configure the end day number of DST.
**<end_day sun-sat>** - Configure the end day number of DST. The values are sun, mon, tue, wed, thu, fri and sat.

**e_mth** - (Optional) Configure the end month number of DST.
**<end_mth 1-12>** - Configure the end month number of DST. The values are 1 to 12.

**e_time** - Configure the end time of DST.
**<end_time hh:mm>** - Configure the end time in hh:mm of DST.

**offset** - Specify the number of minutes to add or to subtract during summertime. The range of offsets are 30, 60, 90, and 120. The default value is 60.
**30** - Specify 30 minutes to add or to subtract during summertime.
**60** - Specify 60 minutes to add or to subtract during summertime.
**90** - Specify 90 minutes to add or to subtract during summertime.
**120** - Specify 120 minutes to add or to subtract during summertime.

**annual** - Set the DST to annual mode.

**s_date** - Configure the start date number of DST.
**<start_date 1-31>** - Configure the start date number of DST. The values are 1 to 31.

**s_mth** - Configure the start month number of DST.
**<start_mth 1-12>** - Configure the start month number of DST. The values are 1 to 12.

**s_time** - Configure the start time of DST.
**<start_time hh:mm>** - Configure the start time in hh:mm of DST.

**e_date** - Configure the end date number of DST.
**<end_date 1-31>** - Configure the end date number of DST. The values are 1 to 31.

**e_mth** - Configure the end month number of DST.
**<end_mth 1-12>** - Configure the end month number of DST. The values are 1 to 12.

**e_time** - Configure the end time of DST.
**<end_time hh:mm>** - Configure the end time in hh:mm of DST.

**offset** - Specify the number of minutes to add or to subtract during summertime. The range of offsets are 30, 60, 90, and 120. The default value is 60.
**30** - Specify 30 minutes to add or to subtract during summertime.
**60** - Specify 60 minutes to add or to subtract during summertime.
**90** - Specify 90 minutes to add or to subtract during summertime.
**120** - Specify 120 minutes to add or to subtract during summertime.

## Restrictions

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

### Example

To configure time:

```
DGS-3620-28SC:admin#config dst repeating s_week 2 s_day tue s_mth 4 s_time
15:00 e_week 2 e_day wed e_mth 10 e_time 15:30 offset 30
Command: config dst repeating s_week 2 s_day tue s_mth 4 s_time 15:00 e_week 2
e_day wed e_mth 10 e_time 15:30 offset 30

Success.

DGS-3620-28SC:admin#
```

## 101-9 show time

### Description

This command is used to display current time states.

### Format

**show time**

### Parameters

None.

### Restrictions

None.

### Example

To show time:

```
DGS-3620-28SC:admin#show time
Command: show time

Current Time Source  : System Clock
Boot Time    : 8 Jan 2000  21:44:33
Current Time : 9 Jan 2000  03:25:17
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-3620-28SC:admin#
```

# Chapter 102 Traffic Segmentation Commands

| |
|---|
| **config traffic_segmentation** [<portlist> \| all] forward_list [null \| all \| <portlist>] |
| **show traffic_segmentation** {<portlist>} |

## 102-1 config traffic_segmentation

### Description

This command is used to configure traffic segmentation.

### Format

**config traffic_segmentation [<portlist> | all] forward_list [null | all | <portlist>]**

### Parameters

| |
|---|
| **<portlist>** - Specify a range of ports to be configured. |
| **all** - Specify all ports. |
| **forward_list** - Specify a range of port forwarding domains.<br>**null** - Specify the range of the port forwarding domain is null.<br>**all** - Specify all ports.<br>**<portlist>** - Specify a range of ports to be configured. |

### Restrictions

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

### Example

To configure traffic segmentation:

```
DGS-3620-28SC:admin#config traffic_segmentation 1-6 forward_list 7-8
Command: config traffic_segmentation 1-6 forward_list 7-8

Success.

DGS-3620-28SC:admin#
```

## 102-2 show traffic_segmentation

### Description

This command is used to display the traffic segmentation table.

## Format

**show traffic_segmentation {<portlist>}**

## Parameters

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

**Note:** If no parameter is specified, the system will display all current traffic segmentation tables.

## Restrictions

None.

## Example

To display the traffic segmentation table for ports 1 to 3:

```
DGS-3620-28SC:admin#show traffic_segmentation 1-3
Command: show traffic_segmentation 1-3

Traffic Segmentation Table

Port    Forward Portlist
------  --------------------------------------------------
1       1-28
2       1-28
3       1-28

DGS-3620-28SC:admin#
```

# Chapter 103 Utility Commands

**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>]}]

**download cfg_fromRCP** [{username <username>} {<ipaddr>} src_file <path_filename 64> | rcp: <string 128>] {[unit <unit_id 1-12> | all]} {dest_file <pathname>}

**download firmware_fromRCP** [{username <username>} {<ipaddr>} src_file <path_filename 64> | rcp: <string 128>] {[unit <unit_id 1-12> | all]} {dest_file <pathname>} {boot_up}

**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>}]

**upload attack_log_toRCP** [{username <username>} {<ipaddr>} dest_file <path_filename 64> | rcp: <string 128>] {unit <unit_id 1-12>}

**upload cfg_toRCP** [{username <username>} {<ipaddr>} dest_file <path_filename 64> | rcp: <string 128>] {unit <unit_id 1-12>} {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 firmware_toRCP** [{username <username>} {<ipaddr>} dest_file <path_filename 64> | rcp: <string 128>] {unit <unit_id 1-12>} {src_file <pathname>}

**upload log_toRCP** [{username <username>} {<ipaddr>} dest_file <path_filename 64> | rcp: <string 128>]

**config firmware image** {unit <unit_id>} <pathname> boot_up

**config configuration** {unit <unit_id>} <pathname> [boot_up | active]

**show config** [effective | modified | current_config | boot_up | 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>}}}}}}

**show boot_file**

**config rcp server** {ipaddress <ipaddr> | username <username>}

**config rcp server clear** [ipaddr | username | both]

**show rcp server**

**ping** [<ipaddr> | <domain_name 255>] {times <value 1-255> | timeout <sec 1-99> | source_ip <ipaddr>}

**ping6** <ipv6addr> {times <value 1-255> | size <value 1-6000> | timeout <sec 1-99> | source_ip <ipv6addr>}

**traceroute** [<ipaddr> | <domain_name 255>] {ttl <value 1-60> | port <value 30000-64900> | timeout <sec 1-65535> | probe <value 1-9>}

**traceroute6** <ipv6addr> {ttl <value 1-60> | port <value 30000-64900> | timeout <sec 1-65535> | probe <value 1-9>}

**telnet** [<ipaddr> | <domain_name 255> | <ipv6addr>] {tcp_port <value 1-65535>}

**enable broadcast_ping_reply**

**disable broadcast_ping_reply**

**show broadcast_ping_reply**

## 103-1 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>** - Specify the IP address of the TFTP server.
**<ipv6addr>** - Specify the IPv6 address of the TFTP server.
**<domain_name 255>** - Specifies 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>** - 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.

**unit** - Specifies which unit on the stacking system. If it is not specified, it refers to the master unit.
**<unit_id>** - Enter the unit ID used here.
**all** - Specifies that all the units in the stacking system will be used.

**dest_file** - (Optional) Specify an absolute path name on the device file system. If path name is not specified, it overwrites the bootup image on the Switch.
**<pathname>** - Specify 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>** - Specify the IP address of the TFTP server.
**<ipv6addr>** - Specify the IPv6 address of the TFTP server.
**<domain_name 255>** - Specifies 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 64>** - 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.

**unit** - Specifies which unit on the stacking system. If it is not specified, it refers to the master unit.
**<unit_id>** - Enter the unit ID used here.
**all** - Specifies that all the units in the stacking system will be used.

**increment** - If increment is specified, then the existing configuration will not be cleared before applying of the new configuration. If it is not specified, then the existing configuration will be cleared before applying of the new configuration.

**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> -** Specify 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-3620-28SC:admin#download firmware_fromTFTP 10.0.0.66 src_file dgs-3620.had
dest_file runtime.had
Command: download firmware_fromTFTP 10.0.0.66 src_file dgs-3620.had dest_file
runtime.had

 Connecting to server.................. Done.
 Download firmware..................... Done.  Do not power off!
 Please wait, programming flash......... Done.



DGS-3620-28SC:admin#
```

## 103-2 download cfg_fromRCP

### Description

This command is used to download a configuration file from a Remote Copy Protocol (RCP) server.

### Format

**download cfg_fromRCP [{username <username>} {<ipaddr>} src_file <path_filename 64> | rcp: <string 128>] {[unit <unit_id 1-12> | all]} {dest_file <pathname>}**

### Parameters

**username** - (Optional) Specify the remote user name on the RCP server.
**<username>** - Specify the remote user name on the RCP server.

**<ipaddr>** - (Optional) Specify the IP address of the RCP server.

**src_file** - Specify the path and file name of the switch configuration file on the RCP server. The maximum length is 64.
**<path_filename 64> -** Specify the path and file name of the switch configuration file on the RCP server. The maximum length is 64.

**rcp:** - Syntax: rcp: username@ipaddr/directory/filename. Example for full path: user_name@10.1.1.1/home/user_name/desxxxx.had; Example for relative path: user_name@10.1.1.1./desxxxx.had. Note: No spaces in the whole <string>.
**<string 128>** - Syntax: rcp: username@ipaddr/directory/filename. Example for full path: user_name@10.1.1.1/home/user_name/desxxxx.had; Example for relative path: user_name@10.1.1.1./desxxxx.had. Example for omitted user name in RCP string: 10.1.1.1./desxxxx.had. Note: No spaces in the whole <string>.

**unit** - Specifies which unit on the stacking system. If it is not specified, it refers to the master unit.
**<unit_id 1-12>** - Enter the unit ID used here. This value must be between 1 and 12.
**all** - Specifies that all the units in the stacking system will be used.

**dest_file** - (Optional) Specify the path and file name of the destination file on the device.
**<pathname>** - Specify the path and file name of the destination file.

### Restrictions

Only Administrator-level users can issue this command.

### Example

To download a configuration file from an RCP server:

```
DGS-3620-28SC:admin#download cfg_fromRCP username rcp_user 172.18.212.106
src_file /home/DGS-3620.cfg
Command: download cfg_fromRCP username rcp_user 172.18.212.106 src_file
/home/DGS-3620.cfg

Connecting to server.................. Done.
Download configuration................ Done.

DGS-3620-28SC:admin#
```

## 103-3 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 1-12> | all]} {dest_file <pathname>} {boot_up}**

### Parameters

| |
|---|
| **username** - (Optional) Specify the remote user name on the RCP server.<br>**<username>** - Specify the remote user name on the RCP server. |
| **<ipaddr>** - (Optional) Specify the IP address of the RCP server. |
| **src_file** - Specify the path name on the RCP server or local. Note: If a user specifies the relative file path, the path search strategy depends on the server system.<br>**<path_filename 64>** - Specify the path name on the RCP server or local. Note: If a user specifies the relative file path, the path search strategy depends on the server system. |
| **rcp:** - Syntax: rcp: username@ipaddr/directory/filename. Example for full path: user_name@10.1.1.1/home/user_name/desxxxx.had; Example for relative path: user_name@10.1.1.1./desxxxx.had; Example for omitted user name in RCP string: 10.1.1.1./desxxxx.had. Note: No spaces are allowed in the <string>.<br>**<string 128>** - Syntax: rcp: username@ipaddr/directory/filename. Example for full path: user_name@10.1.1.1/home/user_name/desxxxx.had; Example for relative path: user_name@10.1.1.1./desxxxx.had; Example for omitted user name in RCP string: 10.1.1.1./desxxxx.had. Note: No spaces are allowed in the <string>. |
| **unit** - Specifies which unit on the stacking system. If it is not specified, it refers to the master unit.<br>**<unit_id 1-12>** - Enter the unit ID used here. This value must be between 1 and 12.<br>**all** - Specifies that all the units in the stacking system will be used. |
| **dest_file** - (Optional) Specify the path and file name of the destination file on the device.<br>**<pathname>** - Specify the path and file name of the destination file. |
| **boot_up** - Specifies it as a boot up file. |

### Restrictions

Only Administrator-level users can issue this command.

### Example

To download firmware from an RCP server:

```
DGS-3620-28SC:admin#download firmware_fromRCP username rcp_user 10.90.90.90
src_file /home/DGS-3620.had
Command: download firmware_fromRCP username rcp_user 10.90.90.90 src_file
/home/DGS-3620.had

Connecting to server.................. Done.
Download firmware..................... Done.   Do not power off !!
Please wait, programming flash......... Done.
Saving current settings to NV-RAM...... Done.

DGS-3620-28SC:admin#
```

## 103-4 upload

### Description

This command is used to upload a firmware or a configuration file from device to 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 a device to a TFTP server.
**<ipaddr>** - Specify the IP 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 here. This name can be up to 255 characters long.

**dest_file** - Specify the path name on the TFTP server. It can be a relative path name or an absolute path name
**<path_filename 64>** - Specify 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** - (Optinal) Specifies which unit on the stacking system. If it is not specified, it refers to the master unit.
**<unit_id>** - Enter the unit ID used here.

**src_file** - (Optional) Specify an absolute path name on the device file system. If a path name is not specified, it refers to the boot up configuration file.
**<pathname>** - Specify the location of the switch configuration file on device.

**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>** - Specify 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>** - Specify a filter string enclosed by the quotation mark symbol.
**<filter_string 80>** - Specify a filter string enclosed by the quotation mark symbol.

**log_toTFTP** - Used to upload a log file from the device to a TFTP server.
**<ipaddr>** - Specify the IP 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 here. This name can be up to 255 characters long.

**dest_file** - Specify the path name if the TFTP server.
**<path_filename 64>** - Specify the path name on the TFTP server. It can be a relative path name or an absolute path name.

**attack_log_toTFTP** - Used to upload the attack log to a TFTP server.
**<ipaddr>** - Specify the IP 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 here. This name can be up to 255 characters long.

**dest_file** - Specify the path name if the TFTP server.
**<path_filename 64>** - Specify the path name on the TFTP server. It can be a relative path name or an absolute path name.

**unit** - (Optinal) Specifies which unit on the stacking system. If it is not specified, it refers to the master unit.
**<unit_id>** - Enter the unit ID used here.

**firmware_toTFTP** - Used to upload firmware from the device to a TFTP server.
**<ipaddr>** - Specify the IP 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 here. This name can be up to 255 characters long.

**dest_file** - Specify the path name if the TFTP server.
**<path_filename 64>** - Specify the path name if the TFTP server.

**unit** - (Optinal) Specifies which unit on the stacking system. If it is not specified, it refers to the master unit.
**<unit_id>** - Enter the unit ID used here.

**src_file** - (Optional) Specify an absolute path name on the device file system. If the path name is not specified, it refers to the boot up image.
**<pathname>** - Specify an absolute path name on the device file system. If the path name is not specified, it refers to the boot up image.

## Restrictions

Only Administrator, Operator level users can issue this command.

## Example

To upload firmware from a file system device to a TFTP server:

```
DGS-3620-28SC:admin#upload firmware_toTFTP 10.1.1.1 dest_file D:\firmware.had
src_file 2.00.009.had
Command: upload firmware_toTFTP 10.1.1.1 dest_file D:\firmware.had src_file
2.00.009.had


Connecting to server................. Done.
Upload firmware...................... Done.


DGS-3620-28SC:admin#
```

To upload the current configuration file to a TFTP server:

```
DGS-3620-28SC:admin#upload cfg_toTFTP 10.48.74.121 dest_file c:\cfg\DGS-
3620.cfg
Command: upload cfg_toTFTP 10.48.74.121 dest_file c:\cfg\DGS-3620.cfg

Connecting to server................. Done.
Upload configuration................. Done.

DGS-3620-28SC:admin#
```

To upload all logs to a TFTP server:

```
DGS-3620-28SC:admin#upload log_toTFTP 10.48.74.121 dest_file c:\log\DGS-
3620.log
Command: upload log_toTFTP 10.48.74.121 dest_file c:\log\DGS-3620.log

Connecting to server................. Done.
Upload log........................... Done.

DGS-3620-28SC:admin#
```

To upload a dangerous log:

```
DGS-3620-28SC:admin# upload attack_log_toTFTP 10.48.74.121 dest_file
c:\alert.txt
Command: upload attack_log_toTFTP 10.48.74.121 dest_file c:\alert.txt

 Connecting to server.................. Done.
 Upload attack log..................... Done.

Success.

DGS-3620-28SC:admin#
```

## 103-5 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 specifies 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 1-12>}**

### Parameters

**username** - (Optional) The remote user name on the RCP Server.
**<username>** - Enter the remote username used here.

**<ipaddr>** - (Optional) Enter the IP address used for the configuration here.

**dest_file** – Specifies the destination file used.
**<path_filename 64>** - The pathname specifies the pathname on the RCP server or local device.

**rcp:** - Syntax: rcp: username@ipaddr/directory/filename. Example for FULL path: user_name@10.1.1.1/home/user_name/desxxxx.had. Example for relative path: user_name@10.1.1.1./desxxxx.had. Note: Do not use any blank spaces in the <string>.
**<string 128>** - Enter the RCP string here.

**unit** - (Optinal) Specifies which unit on the stacking system. If it is not specified, it refers to the master unit.
**<unit_id 1-12>** - Enter the unit ID used here. This value must be between 1 and 12.

### Restrictions

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

### Example

To upload the attack log from the device to an RCP server:

```
DGS-3620-28SC:admin# upload attack_log_toRCP username rcp_user 172.18.212.104
dest_file /home/DGS-3620.log unit 2
Command: upload attack_log_toRCP username rcp_user 172.18.212.104 dest_file
/home/DGS-3620.log unit 2

Connecting to server.......... Done.
Upload Attack log............. Done.
Success.

DGS-3620-28SC:admin#
```

## 103-6 upload cfg_toRCP

### Description

This command is used to upload a configuration file from the device to a Remote Copy Protocol (RCP) server.

### Format

**upload cfg_toRCP [{username <username>} {<ipaddr>} dest_file <path_filename 64> | rcp: <string 128>] {unit <unit_id 1-12>} {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>** - Specify the remote user name on the RCP server.

**<ipaddr>** - (Optional) Specify the IP address of the RCP server.

**dest_file** - Specify the path name on the RCP server. Note: If a user specifies the relative file path, the path search strategy will depend on the server system. For some systems, the current user working directory will be searched first, followed by the environment paths.
**<path_filename 64>** - Specify the path name on the RCP server or local RCP client.

**rcp:** - Specify the path on the RCP server or local RCP client. Note: If a user specifies the relative file path, the path search strategy will depend on the server system. For some systems, the current user working directory will be searched first, followed by the environment paths.
**<string 128>** - Specify the path on the RCP server or local RCP client.

**unit** - (Optinal) Specifies which unit on the stacking system. If it is not specified, it refers to the master unit.
**<unit_id 1-12>** - Enter the unit ID used here. This value must be between 1 and 12.

**src_file** - (Optional) Specify the path name of the source file.
**<pathname>** - Specify the path name of the source file. Note that if no path name is specifies, 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>** - Specify 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>** - Specify a filter string enclosed by the quotation mark symbol.
**<filter_string 80>** - Specify a filter string enclosed by the quotation mark symbol.

### Restrictions

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

### Example

To upload the current configuration from the device to an RCP server:

```
DGS-3620-28SC:admin#upload cfg_toRCP username rcp_user 10.48.74.121 dest_file
/home/DGS-3620.cfg
Command: upload cfg_toRCP username rcp_user 10.48.74.121 dest_file /home/DGS-
3620.cfg


Connecting to server... Done.
Upload configuration... Done.


DGS-3620-28SC:admin#
```

## 103-7 upload firmware_toRCP

### Description

This command is used to upload firmware from a device to a Remote Copy Protocol (RCP) server.

### Format

**upload firmware_toRCP [{username <username>} {<ipaddr>} dest_file <path_filename 64> | rcp: <string 128>] {unit <unit_id 1-12>} {src_file <pathname>}**

### Parameters

**username** - (Optional) Specify the remote user name on the RCP server.
**<username>** - Specify the remote user name on the RCP server.

**<ipaddr>** - (Optional) Specify the IP address of the RCP server.

**dest_file** - Specify the path name on the RCP server. Note: If a user specifies the relative file

path, the path search strategy will depend on the server system. For some systems, the current user working directory will be searched first, followed by the environment paths.
**<path_filename 64>** - Specify the path name on the RCP server.

**rcp:** - Specify the path name on the RCP server or local RCP client. Syntax: rcp: username@ipaddr/directory/filename. Example for full path: user_name@10.1.1.1/home/user_name/desxxxx.had. Example for relative path: user_name@10.1.1.1./desxxxx.had. Note: No spaces allowed in the <string>.
**<string 128>** - Specify the path name on the RCP server or local RCP client. Syntax: rcp: username@ipaddr/directory/filename. Example for full path: user_name@10.1.1.1/home/user_name/desxxxx.had. Example for relative path: user_name@10.1.1.1./desxxxx.had. Note: No spaces allowed in the <string>.

**unit** - (Optinal) Specifies which unit on the stacking system. If it is not specified, it refers to the master unit.
**<unit_id 1-12>** - Enter the unit ID used here. This value must be between 1 and 12.

**src_file** - (Optional) Specify the path name of the source file. If not specified, the bootup image on the device will be uploaded.
**<pathname>** - Specify the path name of the source file.

### Restrictions

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

### Example

To upload firmware image to an RCP server:

```
DGS-3620-28SC:admin#upload firmware_toRCP rcp: rcp_user@172.18.212.106/DGS-
3620.had src_file 2.00.009.had
Command: upload firmware_toRCP rcp: rcp_user@172.18.212.106/DGS-3620.had
src_file 2.00.009.had

Connecting to server............... Done.
Upload firmware.................... Done.

DGS-3620-28SC:admin#
```

## 103-8 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>** - Specify the remote user name on the RCP server.

**<ipaddr>** - (Optional) Specify the IP address of the RCP server.

**dest_file** - Specify the path name of the RCP server. Note: If a user specifies the relative file path, the path search strategy will depend on the server system. For some systems, the

current user working directory will be searched first, followed by the environment paths.
**<path_filename 64>** - Specify the path name of the RCP server.

**rcp:** - Specify the path name on the RCP server.
**<string 128>** - Specify the path name on the RCP server. Syntax: rcp: username@ipaddr/directory/filename. Example for full path: user_name@10.1.1.1/home/user_name/desxxxx.had. Example for relative path: user_name@10.1.1.1./desxxxx.had. Note: No spaces are allowed in the whole <string>.

### Restrictions

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

### Example

To upload the log from the device to an RCP server:

```
DGS-3620-28SC:admin#upload log_toRCP username rcp_user 172.18.212.104 dest_file
/home/DGS-3620.log
Command: upload log_toRCP username rcp_user 172.18.212.104 dest_file /home/DGS-
3620.log

 Connecting to server................... Done.
 Upload log............................. Done.

Success.
```

To upload log from the device to an RCP server using an RCP string:

```
DGS-3620-28SC:admin#upload log_toRCP rcp: tld2@172.18.212.104/home/DGS-3620.log
Command: upload log_toRCP rcp: tld2@172.18.212.104/home/DGS-3620.log

 Connecting to server................... Done.
 Upload log............................. Done.

Success.

DGS-3620-28SC:admin#
```

## 103-9 config firmware image

### Description

This command is used to configure firmware as a boot-up image.

### Format

**config firmware image {unit <unit_id>} <pathname> boot_up**

### Parameters

**unit** – (Optional) Specifies the unit ID used for this configuration.
**<unit_id>** - Enter the unit ID used for this configuration here.

**<pathname>** - Specify a firmware on the device file system.

**boot_up** - Specify as a boot-up file.

### Restrictions

Only Administrator-level users can issue this command.

### Example

To configure a firmware file to bootup:

```
DGS-3620-28SC:admin#config firmware image 2.00.009.had boot_up
Command: config firmware image 2.00.009.had boot_up

Success.

DGS-3620-28SC:admin#
```

## 103-10 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.

### Format

**config configuration {unit <unit_id>} <pathname> [boot_up | active]**

### Parameters

**unit** – (Optional) Specifies the unit ID used.
    **<unit_id>** - Enter the unit ID used here.

**<pathname>** - Specifies a configuration file on the device file system.

**boot_up** - Specifies as a boot up file.

**active** - Specifies to apply the configuration.

### Restrictions

Only Administrator-level users can issue this command.

### Example

To configure the specific configuration file as boot up:

```
DGS-3620-28SC:admin#config configuration 1 boot_up
Command: config configuration 1 boot_up

Success

DGS-3620-28SC:admin#
```

## 103-11 show config

### Description

This command is used to display configuration information. 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; and begin: The first line that contains the specified filter string will be the first line of the output.

The relationship of multiple filter strings following the same filter type is OR. That is, one line is qualified if one of specified filter strings is matched. If more than one filter evaluation is specified, the output of filtered by the former evaluation will be used as the input of the latter evaluation.

### Format

**show config [effective | modified | current_config | boot_up | file <pathname>] {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}} {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}} {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}}}}}**

### Parameters

**effective** - Specifies to display only commands which affect the behavior of the device.

**modified** - Specifies to display only the commands which are not from the ‘reset’ default setting.

**current_config** - Specifies the current configuration.

**boot_up** - Specifies the boot up configuration.

**file** - Specify an absolute path name on the device file system.
  **<pathname>** - Specify an absolute path name on the device file system.

**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>** - Specify 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>** - Specify a filter string enclosed by the quotation mark symbol.
  **<filter_string 80>** - Specify a filter string enclosed by the quotation mark symbol.

### Restrictions

Only Administrator-level users can issue this command.

### Example

To display configuration information:

```
DGS-3620-28SC:admin#show config current_config
Command: show config current_config

#-----------------------------------------------------------------------------
#                  DGS-3620-28SC Gigabit Ethernet Switch
#                              Configuration
```

```
#
#                         Firmware: Build 2.00.015
#         Copyright(C) 2012 D-Link Corporation. All rights reserved.
#-----------------------------------------------------------------------------


# 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

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

## 103-12 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 configuration file and firmware image assigned as a boot up file:

```
DGS-3620-28SC:admin#show boot_file
Command: show boot_file

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

DGS-3620-28SC:admin#
```

## 103-13 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>}**

### Parameters

**ipaddress** - (Optional) Specify the IP address of the global RCP server. By default, the server is unspecified.
**<ipaddr>** - Specify the IP address of the RCP server.

**username** - (Optional) Specify the remote user name on the RCP server.
**<username>** - Specify the remote user name on the RCP server.

### Restrictions

Only Administrator-level users can issue this command.

### Example

To configure RCP global server information for the username “travel”:

```
DGS-3620-28SC:admin#config rcp server username travel
Command: config rcp server username travel

Success.

DGS-3620-28SC:admin#
```

## 103-14 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 Administrator-level users can issue this command.

### Example

To clear the current username of the RCP global server:

```
DGS-3620-28SC:admin#config rcp server clear username
Command: config rcp server clear username

Success.

DGS-3620-28SC:admin#
```

## 103-15 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 Administrator-level users can issue this command.

### Example

To display RCP global server information:

```
DGS-3620-28SC:admin#show rcp server
Command: show rcp server

RCP Server Address         :
RCP Server Username        : travel

DGS-3620-28SC:admin#
```

## 103-16 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>}**

### Parameters

**<ipaddr>** - Specify the IP address of the host.
**<domain_name 255>** - Specifies the domain name of the host. This name can be up to 255 characters long.

**times** – (Optional) Specify the number of individual ICMP echo messages to be sent.
**<value 1-255>** - Specify the number of individual ICMP echo messages to be sent. A value of 0 will send an infinite ICMP echo messages. The maximum value is 255. The default is 0

**timeout** – (Optional) Specify 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>** - Specify 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.

**source_ip** - Specifies the source IP address of the ping packets. If specified, the IP address will be used as the packets’ source IP address that ping send to remote host.
**<ipaddr>** - Enter the source IP addres used here.

### Restrictions

None.

### Example

To send ICMP echo message to “10.51.17.1” for 4 times:

```
DGS-3620-28SC: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-3620-28SC:admin#
```

## 103-17 ping6

### Description

This command is used to send Internet Control Message Protocol (ICMP) echo messages to a remote IPv6 address. The remote IPv6 address will then “echo” or return the message. This is used to confirm connectivity between the switch and the remote device.

### Format

**ping6 <ipv6addr> {times <value 1-255> | size <value 1-6000> | timeout <sec 1-99> | source_ip <ipv6addr>}**

### Parameters

**<ipv6addr>** - Specify the IPv6 address of the host.

**times** - (Optional) Specify the number of individual ICMP echo messages to be sent.
**<value 1-255>** - Specify the number of individual ICMP echo messages to be sent. A value of 0 will send an infinite ICMP echo messages. The maximum value is 255. The default is 0.

**size** - (Optional) Specify the size.
**<value 1-6000>** - Specify the size. A value of 1 to 6000 can be specified. The default is 100.

**timeout** - (Optional) Specify the time-out period while waiting for a response from the remote device.
**<value 1-99>** - Specify the time-out period while waiting for a response from the remote device. A value of 1 to 99 can be specified. The default is 1 second.

**source_ip** - Specifies the source IPv6 address of the ping packets. If specified, the IPv6 address will be used as the packets' source IPv6 address that ping send to remote host.
**<ipv6addr>** - Enter the source IPv6 addres used here.

### Restrictions

None.

### Example

To send ICMP echo message to "3FFE:2::D04D:7878:66D:E5BC" for 10 times:

```
DGS-3620-28SC:admin#ping6 3FFE:2::D04D:7878:66D:E5BC times 10 size 6000 timeout
10
Command: ping6 3FFE:2::D04D:7878:66D:E5BC times 10 size 6000 timeout 10

Reply from 3FFE:2::D04D:7878:66D:E5BC, bytes=6000 time<10 ms
Reply from 3FFE:2::D04D:7878:66D:E5BC, bytes=6000 time<10 ms
Reply from 3FFE:2::D04D:7878:66D:E5BC, bytes=6000 time<10 ms
Reply from 3FFE:2::D04D:7878:66D:E5BC, bytes=6000 time<10 ms
Reply from 3FFE:2::D04D:7878:66D:E5BC, bytes=6000 time<10 ms
Reply from 3FFE:2::D04D:7878:66D:E5BC, bytes=6000 time<10 ms
Reply from 3FFE:2::D04D:7878:66D:E5BC, bytes=6000 time<10 ms
Reply from 3FFE:2::D04D:7878:66D:E5BC, bytes=6000 time<10 ms
Reply from 3FFE:2::D04D:7878:66D:E5BC, bytes=6000 time<10 ms
Reply from 3FFE:2::D04D:7878:66D:E5BC, bytes=6000 time<10 ms
Ping Statistics for 3FFE:2::D04D:7878:66D:E5BC
Packets: Sent =10, Received =10, Lost =0

DGS-3620-28SC:admin#
```

## 103-18 traceroute

### Description

This command is used to trace a route between the switch and a given host on the network.

### Format

**traceroute [<ipaddr> | <domain_name 255>] {ttl <value 1-60> | port <value 30000-64900> | timeout <sec 1-65535> | probe <value 1-9>}**

### Parameters

**<ipaddr>** - Specify the IP address of the destination end station.
**<domain_name 255>** - Specify the domain name of the destination end station.

**ttl** - (Optional) Specify the time to live value of the trace route request.
  **<value 1-60>** - Specify the time to live value of the trace route request. This is the maximum number of routers that a trace route packet can pass while seeking the network path between two devices. The range for the TTL is 1 to 60 hops. The default value is 30.

**port** - (Optional) Specify the port number.
  **<value 30000-649000>** - Specify the port number. The value range is from 30000 to 64900. The default is 33435.

**timeout** - (Optional) Specify the timeout period while waiting for a response from the remote device.
  **<sec 1-65535>** - 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.

**probe** – (Optional) Specify the number of probes.
  **<value 1-9>** - Specify the number of probes. The range is from 1 to 9. If unspecified, the default value is 1.

### Restrictions

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

### Example

To trace the route path between the switch and 10.48.74.121:

```
DGS-3620-28SC:admin#traceroute 10.48.74.121 probe 3
Command: traceroute 10.48.74.121 probe 3

 <10 ms  10.12.73.254
 <10 ms  10.12.73.254
 <10 ms  10.12.73.254
 <10 ms  10.19.68.1
 <10 ms  10.19.68.1
 <10 ms  10.19.68.1
 <10 ms  10.48.74.121
Trace complete.

DGS-3620-28SC:admin#
```

## 103-19 traceroute6

### Description

This command is used to trace the IPv6 routed path between the Switch and a destination end station.

### Format

**traceroute6 <ipv6addr> {ttl <value 1-60> | port <value 30000-64900> | timeout <sec 1-65535> | probe <value 1-9>}**

### Parameters

**<ipv6addr>** - Specify the IPv6 address of the destination end station.

**ttl** - (Optional) Specify the time to live value of the trace route request.
- **<value 1-60>** - Specify the time to live value of the trace route request. This is the maximum number of routers that a trace route packet can pass while seeking the network path between two devices. The range for the TTL is 1 to 60 hops. The default value is 30.

**port** - (Optional) Specify the port number.
- **<value 30000-649000>** - Specify the port number. The value range is from 30000 to 64900. The default is 33435.

**timeout** - (Optional) Specify the timeout period while waiting for a response from the remote device.
- **<sec 1-65535>** - 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.

**probe** – (Optional) Specify the number of probes.
- **<value 1-9>** - Specify the number of probes. The range is from 1 to 9. If unspecified, the default value is 1.

### Restrictions

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

### Example

Trace the IPv6 routed path between the switch and 3000::1:

```
DGS-3620-28SC: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-3620-28SC:admin#
```

Trace the IPv6 routed path between the switch and 1210:100::11 with port 40000:

```
DGS-3620-28SC: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-3620-28SC:admin#
```

## 103-20 telnet

### Description

This command is used to login a Telnet server.

### Format

**telnet [<ipaddr> | <domain_name 255> | <ipv6addr>] {tcp_port <value 1-65535>}**

### Parameters

**<ipaddr>** - Specify the IP address of the Telnet server.
**<domain_name 255>** - Specify the domain name of the telnet server.
**<ipv6addr>** - Specify the IPv6 address of the Telnet server.

**tcp_port** - (Optional) Specify the Telnet server port number to be connected to. If not specified, the default port is 23.
**<value 1-65535>** - Enter a value between 1 and 65535.

### Restrictions

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

### Example

To Telnet to a switch by specifying the IP address:

```
DGS-3620-28SC:admin#telnet 10.1.1.1
Command: telnet 10.1.1.1

                      DGS-3620-28SC Gigabit Ethernet Switch
                             Command Line Interface

                            Firmware: Build 2.00.015
           Copyright(C) 2012 D-Link Corporation. All rights reserved.

UserName:
```

## 103-21 enable broadcast_ping_reply

### Description

The enable broadcast_ping_reply command used to enable broadcast ping reply state, device will reply broadcast ping request.

### Format

**enable broadcast_ping_reply**

### Parameters

None.

### Restrictions

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

### Example

To enable broadcast ping reply state:

```
DGS-3620-28SC:admin# enable broadcast_ping_reply
Command: enable broadcast_ping_reply

Success.

DGS-3620-28SC:admin#
```

## 103-22 disable broadcast_ping_reply

### Description

The disable broadcast_ping_reply command used to disable broadcast ping reply state, device won’t reply broadcast ping request.

### Format

**disable broadcast_ping_reply**

### Parameters

None.

### Restrictions

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

### Example

To disable broadcast ping reply state:

```
DGS-3620-28SC:admin# disable broadcast_ping_reply
Command: disable broadcast_ping_reply

Success.

DGS-3620-28SC:admin#
```

## 103-23 show broadcast_ping_reply

### Description

The show broadcast_ping_reply command is used to show the broadcast ping reply state.

### Format

**show broadcast_ping_reply**

## Parameters

None.

## Restrictions

None.

## Example

To show broadcast ping reply state:

```
DGS-3620-28SC:admin# show broadcast_ping_reply
Command: show broadcast_ping_reply

Broadcast Ping Reply State:  Enabled

DGS-3620-28SC:admin#
```

# Chapter 104 Virtual Router Redundancy Protocol (VRRP) Command List

**enable vrrp** {ping}

**disable vrrp** {ping}

**create vrrp vrid** <vrid 1-255> ipif <ipif_name 12> ipaddress <ipaddr> {state [enable | disable] | priority <int 1-254> | advertisement_interval <int 1-255> | preempt [true | false] | critical_ip <ipaddr> | critical_ip_state [enable | disable]}

**config vrrp vrid** <vrid 1-255> ipif <ipif_name 12> {state [enable | disable] | priority <int 1-254> | ipaddress <ipaddr> | advertisement_interval <int 1-255> | preempt [true | false] | critical_ip <ipaddr> | critical_ip_state [enable | disable]}

**config vrrp ipif** <ipif_name 12> [authtype [none | simple authdata <string 8> | ip authdata <string 16>]]

**delete vrrp** {vrid <vrid 1-255> ipif <ipif_name 12>}

**show vrrp** {ipif <ipif_name 12> {vrid <vrid 1-255>}}

## 104-1 enable vrrp

### Description

This command is used to enable VRRP globally.

### Format

**enable vrrp {ping}**

### Parameters

**ping** - (Optional) Specifies that the ping option will be enabled.

### Restrictions

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

### Example

To enable VRRP:

```
DGS-3620-28SC:admin# enable vrrp
Command: enable vrrp

Success.

DGS-3620-28SC:admin#
```

## 104-2 disable vrrp

### Description

This command is used to disable VRRP globally.

### Format

**disable vrrp {ping}**

### Parameters

**ping** - (Optional) Specifies that the ping option will be disabled.

### Restrictions

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

### Example

To disable VRRP:

```
DGS-3620-28SC:admin# disable vrrp
Command: disable vrrp

Success.

DGS-3620-28SC:admin#
```

## 104-3 create vrrp vrid

### Description

This command is used to create a virtual router entry by VRID.

### Format

**create vrrp vrid <vrid 1-255> ipif <ipif_name 12> ipaddress <ipaddr> {state [enable | disable] | priority <int 1-254> | advertisement_interval <int 1-255> | preempt [true | false] | critical_ip <ipaddr> | critical_ip_state [enable | disable]}**

### Parameters

**vrid** - Specifies the ID of the Virtual Router used.
**<vrid 1-255>** - Enter the Virtual Router ID used here. This value must be between 1 and 255.

**ipif** - Specifies the IP interface used for this configuration.
**<ipif_name 12>** - Enter the IP interface name used here. This name can be up to 12 characters long.

**ipaddress** - Specifies the virtual router's IP address used.
**<ipaddr>** - Enter the virtual router's IP address used here.

**state** - (Optional) Specifies the state of the virtual router function.
**enable** - Specifies that the virtual router function will be enabled.
**disable** - Specifies that the virtual router function will be disabled.

**priority** - (Optional) Specifies the priority to be used for the Virtual Router Master election process
  **<int 1-254>** - Enter the priority value used here. This value must be between 1 and 254.

**advertisement_interval** - (Optional) Specifies the time interval used between sending advertisement messages.
  **<int 1-255>** - Enter the advertisement interval value here. This value must be between 1 and 255 seconds.

**preempt** - (Optional) Controls whether a higher priority virtual router will preempt a lower priority master. The preempt setting must be consistent with all the routers participating within the same VRRP group. Default is settings is true.
  **true** - Specifies that if the backup router's priority is set higher than the masters priority, it will become the master instead of the current one.
  **false** - Specifies that if the backup router's priority is higher than the masters priority, it will not become the master until the master failed.

**critical_ip** - (Optional) Specifies an IP address that will provide the most direct route to the Internet or other critical network connections from this virtual router. This IP address must be a real IP address of a real device on the network. If the connection from the virtual router to this IP address fails, the virtual router will automatically be disabled. A new Master will be elected from the backup routers participating in the VRRP group. Different critical IP addresses may be assigned to different routers participating in the VRRP group and can therefore define multiple routes to the Internet or other critical network connections.
  **<ipaddr>** - Enter the critical interface's IP address used here.

**critical_ip_state** - (Optional) Specifies the state of checking the status (active or inactive) of a critical IP address.
  **enable** - Specifies that the critical IP state checking will be enabled.
  **disable** - Specifies that the critical IP state checking will be disabled.

### Restrictions

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

### Example

To create a VRRP entry:

```
DGS-3620-28SC:admin# create vrrp vrid 1 ipif System ipaddress 10.90.90.91 state
enable
Command: create vrrp vrid 1 ipif System ipaddress 10.90.90.91 state enable

Success.

DGS-3620-28SC:admin#
```

## 104-4 config vrrp vrid

### Description

This command is used to configure the virtual router settings by VRID.

### Format

**config vrrp vrid <vrid 1-255> ipif <ipif_name 12> {state [enable | disable] | priority <int 1-254> | ipaddress <ipaddr> | advertisement_interval <int 1-255> | preempt [true | false] | critical_ip <ipaddr> | critical_ip_state [enable | disable]}**

## Parameters

**vrid** - Specifies the ID of the Virtual Router used.
**<vrid 1-255>** - Enter the Virtual Router ID used here. This value must be between 1 and 255.

**ipif** - Specifies the IP interface used for this configuration.
**<ipif_name 12>** - Enter the IP interface name used here. This name can be up to 12 characters long.

**state** - (Optional) Specifies the state of the virtual router function.
**enable** - Specifies that the virtual router function will be enabled.
**disable** - Specifies that the virtual router function will be disabled.

**priority** - (Optional) Specifies the priority to be used for the Virtual Router Master election process
**<int 1-254>** - Enter the priority value used here. This value must be between 1 and 254.

**ipaddress** - (Optional) Specifies the virtual router's IP address used.
**<ipaddr>** - Enter the virtual router's IP address used here.

**advertisement_interval** - (Optional) Specifies the time interval used between sending advertisement messages.
**<int 1-255>** - Enter the advertisement interval value here. This value must be between 1 and 255 seconds.

**preempt** - (Optional) Controls whether a higher priority virtual router will preempt a lower priority master. The preempt setting must be consistent with all the routers participating within the same VRRP group. Default is setting is true.
**true** - Specifies that if the backup router's priority is set higher than the masters priority, it will become the master instead of the current one.
**false** - Specifies if the backup router's priority is higher than the masters priority, it will not become the master until the master failed.

**critical_ip** - (Optional) Specifies an IP address that will provide the most direct route to the Internet or other critical network connections from this virtual router. This IP address must be a real IP address of a real device on the network. If the connection from the virtual router to this IP address fails, the virtual router will automatically be disabled. A new Master will be elected from the backup routers participating in the VRRP group. Different critical IP addresses may be assigned to different routers participating in the VRRP group and can therefore define multiple routes to the Internet or other critical network connections.
**<ipaddr>** - Enter the critical interface's IP address used here.

**critical_ip_state** - (Optional) Specifies the state of checking the status (active or inactive) of a critical IP address.
**enable** - Specifies that the critical IP state checking will be enabled.
**disable** - Specifies that the critical IP state checking will be disabled.

## Restrictions

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

## Example

To configure VRRP:

```
DGS-3620-28SC:admin# config vrrp vrid 1 ipif System state enable
Command: config vrrp vrid 1 ipif System state enable

Success.

DGS-3620-28SC:admin#
```

## 104-5 config vrrp ipif

### Description

This command is used to configure a virtual router authentication type on an interface.

### Format

**config vrrp ipif <ipif_name 12> [authtype [none | simple authdata <string 8> | ip authdata <string 16>]]**

### Parameters

**ipif** - Specifies the name of IP interface used for this configuration.
- **<ipif_name 12>** - Enter the IP interface name used here. This name can be up to 12 characters long.

**authtype** - Specifies the VRRP’s authentication type.
- **none** - Specifies that no authentication algorithm will be used on this interface.
- **simple** - Specifies that the authentication algorithm will be set to simple text on this interface.
  - **authdata** - Specifies the authentication data used in the simple text authentication algorithm.
    - **<string 8>** - Enter the authentication data used in the simple text authentication algorithm here. This value can be up to 8 characters long.
- **ip** - Specifies that the authentication algorithm will be set to IP authentication header on this interface.
  - **authdata** - Specifies the authentication data used in the IP authentication header algorithm.
    - **<string 16>** - Enter the authentication data used in the IP authentication header algorithm here. This value can be up to 16 characters long.

### Restrictions

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

### Example

To configure a VRRP IP interface:

```
DGS-3620-28SC:admin# config vrrp ipif System authtype simple authdata 12345678
Command: config vrrp ipif System authtype simple authdata 12345678

Success.

DGS-3620-28SC:admin#
```

## 104-6 delete vrrp

### Description

This command is used to delete the VRRP settings.

### Format

**delete vrrp {vrid <vrid 1-255> ipif <ipif_name 12>}**

### Parameters

**vrid** - (Optional) Specifies the Virtual Router ID used.
    **<vrid 1-255>** - Enter the Virtual Router ID used here. This value must be between 1 and 255.

**ipif** - (Optional) Specifies the IP interface name used.
    **<ipif_name 12>** - Enter the IP interface name used here. This name can be up to 12 characters long.

If no parameter is specified, all the VRRP entries will be deleted.

### Restrictions

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

### Example

To delete VRRP:

```
DGS-3620-28SC:admin# delete vrrp vrid 3 ipif System
Command: delete vrrp vrid 3 ipif System

Success.

DGS-3620-28SC:admin#
```

## 104-7 show vrrp

### Description

This command is used to display the VRRP settings.

### Format

**show vrrp {ipif <ipif_name 12> {vrid <vrid 1-255>}}**

### Parameters

**ipif** - (Optional) Specifies the IP interface name to be displayed.
    **<ipif_name 12>** - Enter the IP interface name to be displayed here. This name can be up to 12 characters long.

**vrid** - (Optional) Specifies the Virtual Router ID to be displayed.
    **<vrid 1-255>** - Enter the Virtual Router ID to be displayed here. This value must be between 1 and 255.

If no parameter is specified, then all the VRRP entries will be displayed.

### Restrictions

None.

### Example

To display the VRRP configuration:

```
DGS-3620-28SC:admin# show vrrp
Command: show vrrp

 Global VRRP            : Disabled
 Non-owner response Ping: Disabled

 Interface Name                : System
 Authentication type           : No Authentication

         VRID                   : 1
         Virtual IP Address     : 10.90.90.91
         Virtual MAC Address    : 00-00-5E-00-01-01
         Virtual Router State   : Initialize
         State                  : Enabled
         Priority               : 100
         Master IP Address      : 10.90.90.90
         Critical IP Address    : 0.0.0.0
         Checking Critical IP   : Disabled
         Advertisement Interval : 1 secs
         Preempt Mode           : True
         Virtual Router Up Time : 0 centi-secs
 Total Entries: 1

DGS-3620-28SC:admin#
```

# Chapter 105 Voice VLAN Commands

**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 log state** [enable | disable]
**config voice_vlan aging_time** <min 1-65535>
**show voice_vlan**
**show voice_vlan lldp_med voice_device**
**show voice_vlan oui**
**show voice_vlan ports** {<portlist>}
**show voice_vlan voice_device** {ports <portlist>}

## 105-1 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>** - Specify the name of the voice VLAN. The maximum length is 32 characters. The name must be an existing static VLAN name.

**vlanid** - Specify the VLAN ID of the voice VLAN. The ID must be an existing static VLAN ID.
**<vlanid 1-4094>** - Specify the VLAN ID between 1 and 4094.

### Restrictions

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

### Example

To enable voice VLAN named v2:

```
DGS-3620-28SC:admin#enable voice_vlan v2
Command: enable voice_vlan v2

Success.

DGS-3620-28SC:admin#
```

## 105-2 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 Administrator, Operator and Power-User level users can issue this command.

### Example

To disable voice VLAN:

```
DGS-3620-28SC:admin#disable voice_vlan
Command: disable voice_vlan

Success.

DGS-3620-28SC:admin#
```

## 105-3 config voice_vlan priority

### Description

This command is used to configure 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>** - Specify the priority of the voice VLAN. The range is 0 to 7. The default priority is 5.

### Restrictions

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

### Example

To set the priority of the voice VLAN to be six:

```
DGS-3620-28SC:admin#config voice_vlan priority 6
Command: config voice_vlan priority 6

Success.

DGS-3620-28SC:admin#
```

## 105-4 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** - Specify to add a user-defined OUI of Voice device vendor.

**delete** - Specify to delete a user-defined OUI of Voice device vendor.

**<macaddr>** - Specify a user-defined OUI MAC address.

**<macmask>** - Specify a user-defined OUI MAC address mask.

**description** - (Optional) Specify a description for the user-defined OUI.
**<desc 32>** - Specify a description for the user-defined OUI. The maximum length is 32 characters.

### Restrictions

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

### Example

To add a user-defined OUI of a voice device:

```
DGS-3620-28SC: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-3620-28SC:admin#
```

## 105-5 config voice_vlan ports

### Description

This command is used to enable or disable the voice VLAN function on ports or mode per port.

### Format

**config voice_vlan ports [<portlist>|all] [state [enable |disable]|mode [auto { [tag |untag]}|manual] ]**

### Parameters

**<portlist>** - Specify a range of ports to set.

**all** - Specify to set all ports.

**state** - Specify the voice VLAN function state on ports. The default state is disabled.
- **enable** - Specify to enable the voice VLAN function state on ports.
- **disable** - Specify to disable the voice VLAN function state on ports.

**mode** - The voice VLAN mode. The default mode is auto.
- **auto** - When the mode is auto, the port may become the voice VLAN member port by auto-learning. If the MAC address of the received packet matches the configured OUI, the port will be learned as dynamic member port. The dynamic membership will be removed via the aging out mechanism.
- **manual** - When the mode is set to manual, the port needs to be manually added into or removed from the voice VLAN by 802.1Q VLAN configuration command.

**tag | untag** – Specify the port to join the voice VLAN as a tagged or an untagged member.

1. 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 the port’s PVID VLAN.
2. 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 change its priority. Should the voice device send untagged packets, the switch will assign priority to those and add the voice VLAN ID in this packet.
3. 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.

### Restrictions

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

### Example

To configure voice VLAN ports 4 to 6 to enable:

```
DGS-3620-28SC:admin#config voice_vlan ports 4-6 state enable
Command: config voice_vlan ports 4-6 state enable

Success.

DGS-3620-28SC:admin#
```

To set voice VLAN ports 4 to 6 to auto mode:

```
DGS-3620-28SC:admin#config voice_vlan ports 4-6 mode auto
Command: config voice_vlan ports 4-6 mode auto

Success.

DGS-3620-28SC:admin#
```

## 105-6 config voice_vlan log state

### Description

This command is used to configure the voice VLAN log state.

### Format

**config voice_vlan log state [enable | disable]**

### Parameters

**enable** - Specify to enable the voice VLAN log state.

**disable** - Specify to disable the voice VLAN log state.

### Restrictions

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

### Example

To enable the voice VLAN log state:

```
DGS-3620-28SC:admin#config voice_vlan log state enable
Command: config voice_vlan log state enable

Success.

DGS-3620-28SC:admin#
```

## 105-7 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 voice VLAN aging timer. If the voice traffic resumes during the aging time, the aging timer will be reset and stop.

### Format

**config voice_vlan aging_time <min 1-65535>**

### Parameters

**<min 1-65535>** - Specify the aging time. The range is 1 to 65535 minutes. The default value is 720 minutes.

### Restrictions

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

### Example

To set 60 minutes as the aging time of voice VLAN:

```
DGS-3620-28SC:admin#config voice_vlan aging_time 60
Command: config voice_vlan aging_time 60

Success.

DGS-3620-28SC:admin#
```

## 105-8 show voice_vlan

### Description

This command is used to display voice VLAN global information.

### Format

**show voice_vlan**

### Parameters

None.

### Restrictions

None.

### Example

To display voice VLAN information:

```
DGS-3620-28SC:admin#show voice_vlan
Command: show voice_vlan

Voice VLAN State    : Disabled
Voice VLAN          : Unassigned
Priority            : 5
Aging Time          : 720 minutes
Log State           : Enabled

DGS-3620-28SC:admin#
```

## 105-9 show voice_vlan lldp_med voice_device

### Description

This command is used to display the voice devices that are discovered by LLDP-MED.

### Format

**show voice_vlan lldp_med voice_device**

### Parameters

None.

### Restrictions

None.

### Example

To display the voice devices that were discovered by LLDP-MED:

```
DGS-3620-28SC:admin# show voice_vlan lldp_med voice_device
Command: show voice_vlan lldp_med voice_device

Index               : 1
Local Port          : 1:1
Chassis ID Subtype  : MAC Address
Chassis ID          : 00-E0-BB-00-00-11
Port ID Subtype     : Network Address
Port ID             : 00-01-E3-00-00-00
Create Time         : 10/6/2008 09:00
Remain Time         : 120 Seconds

Index               : 2
Local Port          : 1:3
```

```
Chassis ID Subtype  : MAC Address
Chassis ID          : 00-E0-BB-00-00-12
Port ID Subtype     : Network Address
Port ID             : 00-01-E3-00-00-00
Create Time         : 10/6/2008 09:00
Remain Time         : 120 Seconds

Total Entries: 2

DGS-3620-28SC:admin#
```

## 105-10 show voice_vlan oui

### Description

This command is used to display the OUI information for voice VLAN.

### Format

**show voice_vlan oui**

### Parameters

None.

### Restrictions

None.

### Example

To display voice VLAN OUI:

```
DGS-3620-28SC: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
00-0F-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&Phillips
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: 8

DGS-3620-28SC:admin#
```

## 105-11 show voice_vlan ports

### Description

This command is used to display port voice VLAN information.

### Format

**show voice_vlan ports {<portlist>}**

### Parameters

| | |
|---|---|
| **<portlist>** - (Optional) Specify a range of ports to display. | |

**Note:** If no parameter is specified, all voice VLAN port information will be displayed.

### Restrictions

None.

### Example

To display voice VLAN ports 1 to 3:

```
DGS-3620-28SC:admin#show voice_vlan ports 1-3
Command: show voice_vlan ports 1-3

Ports  Status     Mode
-----  ---------  --------
 1      Disabled   Auto
 2      Disabled   Auto
 3      Disabled   Auto Tagged/Auto Untagged

DGS-3620-28SC:admin#
```

## 105-12 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 when the device sends the traffic.

### Format

**show voice_vlan voice_device {ports <portlist>}**

### Parameters

| | |
|---|---|
| **<portlist>** - (Optional) Specify a range of ports to display. | |

**Note:** If no parameter is specified, the system will display the connected Voice device of all ports.

## Restrictions

None.

## Example

To display voice VLAN device ports 1 to 2:

```
DGS-3620-28SC:admin#show voice_vlan voice_device ports 1-2
Command: show voice_vlan voice_device ports 1-2

Ports  Voice Device       Start Time        Last Active Time
-----  -----------------  ----------------  -----------------

Total Entries : 0

DGS-3620-28SC:admin#
```

# Chapter 106 VLAN Commands

**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 port_vlan** {<portlist>}

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

**enable gvrp**

**disable gvrp**

**show vlan** {<vlan_name 32>}

**show vlan vlanid** <vidlist>

**show vlan ports** {<portlist>}

**show gvrp**

**config private_vlan** [<vlan_name 32> | vid <vlanid 1-4094>] [add [isolated | community] | remove] [<vlan_name 32> | vlanid <vidlist>]

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

**enable pvid auto_assign**

**disable pvid auto_assign**

**show pvid auto_assign**

## 106-1 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 >** - Specify the name of the VLAN to be created. The maximum length is 32 characters.

**tag** - Specify the VLAN ID of the VLAN to be created.
**<vlanid 2-4094>** - The range is from 2 to 4094.

**type** - (Optional) Specify the type of VLAN to be created.
**1q_vlan** - Specify the VLAN is a 802.1q VLAN.
**private_vlan** - Specify the VLAN is a private VLAN.

**advertisement** - (Optional) Specify to allow the Switch sending out GVRP packets to outside sources, notifying that they may join the existing VLAN.

### Restrictions

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

### Example

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

```
DGS-3620-28SC:admin#create vlan v2 tag 2 type 1q_vlan advertisement
Command: create vlan v2 tag 2 type 1q_vlan advertisement

Success.

DGS-3620-28SC:admin#
```

To create a private VLAN with the name “v3” and VLAN ID 3:

```
DGS-3620-28SC:admin#create vlan v3 tag 3 type private_vlan
Command: create vlan v3 tag 3 type private_vlan

Success.

DGS-3620-28SC:admin#
```

## 106-2 create vlan vlanid

### 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 vlanid <vidlist> {type [1q_vlan | private_vlan]} {advertisement}**

### Parameters

**<vidlist>** - Specify the VLAN ID of the VLAN to be created.

**type** - (Optional) Specify the type of VLAN to be created.
**1q_vlan** - Specify the VLAN is a 802.1q VLAN.
**private_vlan** - Specify the VLAN is a private VLAN.

**advertisement** - (Optional) Specify to allow the Switch sending out GVRP packets to outside sources, notifying that they may join the existing VLAN.

### Restrictions

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

### Example

To create a VLAN with VLAN ID 2:

```
DGS-3620-28SC:admin#create vlan vlanid 2 type 1q_vlan advertisement
Command: create vlan vlanid 2 type 1q_vlan advertisement
```

```

Success.

DGS-3620-28SC:admin#
```

To create a private VLAN with VLAN ID 3:

```
DGS-3620-28SC:admin#create vlan vlanid 3 type private_vlan
Command: create vlan vlanid 3 type private_vlan

Success.

DGS-3620-28SC:admin#
```

## 106-3 delete vlan

### Description

This command is used to delete a previously configured VLAN on the switch.

### Format

**delete vlan <vlan_name 32>**

### Parameters

**<vlan_name 32>** - Specify the VLAN name of the VLAN to be deleted. The maximum length is 32 characters.

### Restrictions

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

### Example

To remove VLAN v1:

```
DGS-3620-28SC:admin#delete vlan v1
Command: delete vlan v1

Success.

DGS-3620-28SC:admin#
```

## 106-4 delete vlan vlanid

### Description

This command is used to delete a previously configured VLAN ID on the switch.

### Format

**delete vlan vlanid <vidlist>**

### Parameters

**<vidlist>** - Specify a range of VLAN ID to be deleted.

### Restrictions

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

### Example

To remove a VLAN ID 2:

```
DGS-3620-28SC:admin#delete vlan vlanid 2
Command: delete vlan vlanid 2

Success.

DGS-3620-28SC:admin#
```

## 106-5 config vlan

### Description

This command is used to add or delete ports to or from the port list of a previously configured VLAN. Users can specify the additional ports as tagged, untagged, or forbidden.

### Format

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

### Parameters

**<vlan_name 32> -** Specify the name of the VLAN to add or delete ports to. The maximum length is 32 characters.

**add** - Specify the port attribute to add.
- **tagged** - Specify the additional ports as tagged.
- **untagged** - Specify the additional ports as untagged.
- **forbidden** - Specify the ports to be forbidden from becoming members of the VLAN dynamically and not able to forward packets in this VLAN.

**delete** - Specify the port status to delete.

**<portlist>** - Specify a range of ports to add or delete to the VLAN.

**advertisement** - Specify to send GVRP out for this VLAN or not. If not, the VLAN cannot be joint dynamically.
- **enable** - Specify to enable GVRP.
- **disable** - Specify to disable GVRP.

### Restrictions

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

### Example

To add 4 through 8 as tagged ports to the VLAN v1:

```
DGS-3620-28SC:admin#config vlan v1 add tagged 4-8
Command: config vlan v1 add tagged 4-8

Success.

DGS-3620-28SC:admin#
```

To delete ports 4 through 8 from VLAN v1:

```
DGS-3620-28SC:admin#config vlan v1 delete 4-8
Command: config vlan v1 delete 4-8

Success.

DGS-3620-28SC:admin#
```

To enable the VLAN default advertisement:

```
DGS-3620-28SC:admin#config vlan default advertisement enable
Command: config vlan default advertisement enable

Success.

DGS-3620-28SC:admin#
```

## 106-6 config vlan vlanid

### Description

This command is used to add or delete ports to the port list of a previously configured VLAN. Users can specify the additional ports as tagged, untagged, or forbidden.

### Format

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

### Parameters

**<vidlist>** - Specify the VLAN ID of the VLAN to add or delete ports to.

**add** - Specify the port attribute to add.
 **tagged** - Specify the additional ports as tagged.
 **untagged** - Specify the additional ports as untagged.
 **forbidden** - Specify the ports to be forbidden from becoming members of the VLAN dynamically and not able to forward packets in this VLAN.

**delete** - Specify the port status to delete.

**<portlist>** - Specify a range of ports to add or delete to the VLAN.

**advertisement** - Specify to send GVRP out for this VLAN or not. If not, the VLAN cannot be joint dynamically.

**enable** - Specify to enable GVRP.
**disable** - Specify to disable GVRP.

**name** - Specify the VLAN name.
**<vlan_name 32>** - The maximum length is 32 characters.

## Restrictions

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

## Example

To add 4 through 8 as tagged ports to the VLAN 1:

```
DGS-3620-28SC:admin#config vlan vlanid 1 add tagged 4-8
Command: config vlan vlanid 1 add tagged 4-8

Success.

DGS-3620-28SC:admin#
```

To delete ports 4 through 8 from VLAN 1:

```
DGS-3620-28SC:admin#config vlan vlanid 1 delete 4-8
Command: config vlan vlanid 1 delete 4-8

Success.

DGS-3620-28SC:admin#
```

To enable the VLAN default advertisement:

```
DGS-3620-28SC:admin#config vlan vlanid default advertisement enable
Command: config vlan vlanid default advertisement enable

Success.

DGS-3620-28SC:admin#
```

# 106-7 config port_vlan

## Description

This command is used to set the ingress checking status and the sending and receiving of 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>** - Specify a range of ports to be set.

**all** - Specify to make all ports to be set.

**gvrp_state** - Specify if the port is allowed to dynamically become a member of a VLAN when receiving GVRP.
**enable** - Enable GVRP for the ports specified in the port list.
**disable** - Disable GVRP for the ports specified in the port list.

**ingress_checking** - When ingress checking is enabled, the Switch checks if the incoming packet was assigned a VLAN on which the ingress port is a VLAN member. If the incoming packet and the ingress port are not in the same VLAN, the packet will be dropped.
**enable** - Enable ingress checking for the specified port list.
**disable** - Disable ingress checking for the specified port list.

**acceptable_frame** - Specify the type of frame that will be accepted by the port.
**tagged_only** - Only tagged frame will be received.
**admit_all** - Both tagged and untagged frames will be accepted.

**pvid** - Specify the Port VID (PVID) that will be associated with the port.
**<vlanid 1- 4094>** - Specify the VLAN ID between 1 and 4094.

### Restrictions

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

### Example

To configure the port VLAN:

```
DGS-3620-28SC: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-3620-28SC:admin#
```

## 106-8 show port_vlan

### Description

This command is used to display the GVRP status for a port list on the switch.

### Format

**show port_vlan {<portlist>}**

### Parameters

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

**Note:** If no parameter is specified, the system will display GVRP information for all ports.

### Restrictions

None.

### Example

To display 802.1q port settings for ports 1 to 3:

```
DGS-3620-28SC:admin#show port_vlan 1-3
Command: show port_vlan 1-3

Port     PVID  GVRP      Ingress Checking  Acceptable Frame Type
-------  ----  --------  ----------------  ----------------------------
 1       1     Disabled  Enabled           All Frames
 2       1     Disabled  Enabled           All Frames
 3       1     Disabled  Enabled           All Frames

Total Entries : 3

DGS-3620-28SC:admin#
```

## 106-9 config gvrp

### Description

This command is used to set the GVRP timer’s value.

### Format

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

### Parameters

**timer** – Specify GVRP timer.
**join** - Specify the Join time will be set. The default value is 200 milliseconds.
**leave** - Specify the Leave time will be set. The default value is 600 milliseconds.
**leaveall** - Specify the LeaveAll time. The default value is 10000 milliseconds.

**<value 100-100000>** - Specify the time value. The value range is 100 to 100000 milliseconds. In addition, the Leave time should greater than 2 Join times and the LeaveAll time should greater than Leave time.

**nni_bpdu_addr** - Determine the BPDU protocol address for GVRP in service provide site. It can use 802.1d GVRP address, or 802.1ad service provider GVRP address.
**dot1d** - Specify a 802.1d GVRP address.
**dot1ad** - Specify a 802.1ad service provider GVRP address.

### Restrictions

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

### Example

To set the Join time to 200 milliseconds:

```
DGS-3620-28SC:admin#config gvrp timer join 200
Command: config gvrp timer join 200

Success.

DGS-3620-28SC:admin#
```

## 106-10 enable gvrp

### Description

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

### Format

**enable gvrp**

### Parameters

None.

### Restrictions

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

### Example

To enable the generic VLAN Registration Protocol (GVRP):

```
DGS-3620-28SC:admin#enable gvrp
Command: enable gvrp

Success.

DGS-3620-28SC:admin#
```

## 106-11 disable gvrp

### Description

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

### Format

**disable gvrp**

### Parameters

None.

### Restrictions

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

### Example

To disable Generic VLAN Registration Protocol (GVRP):

```
DGS-3620-28SC:admin#disable gvrp
Command: disable gvrp

Success.

DGS-3620-28SC:admin#
```

## 106-12 show vlan

### Description

This command is used to display summary information about each VLAN, which includes: VLAN ID, VLAN Name, Tagged/Untagged/Forbidden status for each port, and Member/Non-member status for each port.

### Format

**show vlan {<vlan_name 32>}**

### Parameters

**<vlan_name 32>** - (Optional) Specify the name of the VLAN to be displayed. The maximum length is 32 characters.

### Restrictions

None.

### Example

To display VLAN settings:

```
DGS-3620-28SC: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    : 1-28
Static Ports    : 1-28
Current Tagged Ports  :
Current Untagged Ports: 1-28
Static Tagged Ports   :
Static Untagged Ports : 1-28
Forbidden Ports       :

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

DGS-3620-28SC:admin#
```

## 106-13 show vlan vlanid

### Description

This command is used to display summary information about each VLAN, which includes: VLAN ID, VLAN Name, Tagged/Untagged/Forbidden status for each port, and Member/Non-member status for each port.

### Format

**show vlan vlanid <vidlist>**

### Parameters

**<vidlist>** - Specify the VLAN ID number to be displayed.

### Restrictions

None.

### Example

To display VLAN settings for VLAN ID 1:

```
DGS-3620-28SC:admin#show vlan vlanid 1
Command: show vlan vlanid 1

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

```
Forbidden Ports       :

Total Entries : 1

DGS-3620-28SC:admin#
```

## 106-14 show vlan ports

### Description

This command is used to display summary information about Tagged, Untagged, and Forbidden status for each port.

### Format

**show vlan ports {<portlist>}**

### Parameters

**<portlist>** - (Optional) Specify a range of ports for which you want to display VLAN. The beginning and end of the port list range are separated by a dash.

### Restrictions

None.

### Example

To display VLAN port settings:

```
DGS-3620-28SC:admin#show vlan ports 1-2
Command: show vlan ports 1-2

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

DGS-3620-28SC:admin#
```

## 106-15 show gvrp

### Description

This command is used to display the GVRP status for the switch.

### Format

**show gvrp**

### Parameters

None.

### Restrictions

None.

### Example

To display the GVRP status of the switch:

```
DGS-3620-28SC: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-3620-28SC:admin#
```

## 106-16 config private_vlan

### Description

A private VLAN is comprised of a primary VLAN, up to one isolated VLAN, and a number of community VLANs. A private VLAN ID is presented by the VLAN ID of the primary VLAN. The command used to associate or de-associate a secondary VLAN with a primary VLAN. A primary VLAN is created via the command **create vlan type private_vlan**. A secondary VLAN is created via the command **create vlan type 1q_vlan**. A secondary VLAN cannot be associated with multiple primary VLANs. The untagged member port of the primary VLAN is named as the promiscuous port. The tagged member port of the primary VLAN is named as the trunk port. A promiscuous port of a private VLAN cannot be promiscuous port of other private VLANs. The primary VLAN member port cannot be a secondary VLAN member at the same time, or vice versa. A secondary VLAN can only have the untagged member port. The member port of a secondary VLAN cannot be member port of other secondary VLAN at the same time. When a VLAN is associated with a primary VLAN as the secondary VLAN, the promiscuous port of the primary VLAN will behave as the untagged member of the secondary VLAN, and the trunk port of the primary VLAN will behave as the tagged member of the secondary VLAN. A secondary VLAN cannot be specified with advertisement. Only the primary VLAN can be configured as a layer 3 interface. The private VLAN member port cannot be configured with the traffic segmentation function.

### Format

**config private_vlan [<vlan_name 32> | vid <vlanid 1-4094>] [add [isolated | community] | remove] [<vlan_name 32> | vlanid <vidlist>]**

### Parameters

**<vlan_name 32>** - Specify the name of the private VLAN. The maximum length is 32 characters.

**vid** - Specify the VLAN ID of the private VLAN.
  **<vlanid 1-4094>** - Specify the VLAN ID between 1 and 4094.

**add** - Specify to add isolated or community.
  **isolated** - Specify the secondary VLAN as an isolated VLAN.
  **community** - Specify the secondary VLAN as a community VLAN.

**remove** - Specify to remove the specified private VLAN.

**<vlan_name 32>** - Specify the VLAN of a range of secondary VLANs to add to the private VLAN or remove from it. The maximum length is 32 characters.

**vlanid** - Specify a range of the second VLAN IDs to add to the private VLAN or remove from it.
  **<vidlist>** - Specify the VLAN ID.

### Restrictions

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

### Example

To associate secondary VLAN to private VLAN p1:

```
DGS-3620-28SC:admin#config private_vlan p1 add community vlanid 2-5
Command: config private_vlan p1 add community vlanid 2-5

Success.

DGS-3620-28SC:admin#
```

## 106-17 show private_vlan

### Description

This command is used to display private VLAN information on the switch.

### Format

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

### Parameters

**<vlan_name 32>** - (Optional) Specify the name of the private VLAN. The maximum length is 32 characters.

**vlanid** - (Optional) Specify the VLAN ID of the private VLAN.
  **<vidlist>** - Specify the VLAN ID of the private VLAN.

### Restrictions

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

### Example

To display private VLAN settings:

```
DGS-3620-28SC:admin#show private_vlan
Command: show private_vlan

Private VLAN 100
------------------
   Promiscuous Ports: 1
   Trunk Ports      : 2
   Isolated Ports   : 3-5          Isolated VLAN : 20
   Community Ports  : 6-8          Community VLAN: 30
   Community Ports  : 9-10         Community VLAN: 40

Private VLAN 200
------------------
   Promiscuous Ports: 11
   Trunk Ports      : 12
   Isolated Ports   : 13-15          Isolated VLAN : 50
   Community Ports  : 16-18          Community VLAN: 60


DGS-3620-28SC:admin#
```

## 106-18 enable pvid auto_assign

### Description

This command is used to enable the auto-assignment of PVID. If auto-assign PVID is disabled, PVID can only be changed by PVID configuration (user changes explicitly). The VLAN configuration will not automatically change PVID. If Auto-assign PVID is enabled, PVID can be changed by PVID or VLAN configuration. When a user configures a port to VLAN X’s untagged membership, this port’s PVID will be updated with VLAN X. PVID is updated with the last item of the VLAN list. When a user removes a port from the untagged membership of the PVID’s VLAN, the port’s PVID will be assigned with “default VLAN”.

### Format

**enable pvid auto_assign**

### Parameters

None. The default setting is enabled.

### Restrictions

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

### Example

To enable the auto-assign PVID:

```
DGS-3620-28SC:admin#enable pvid auto_assign
Command: enable pvid auto_assign

```

```
Success.

DGS-3620-28SC:admin#
```

## 106-19 disable pvid auto_assign

### Description

The command is used to disable the auto-assignment of PVID. If auto-assign PVID is disabled, PVID can only be changed by PVID configuration (user changes explicitly). The VLAN configuration will not automatically change PVID. If auto-assign PVID is enabled, PVID can be changed by PVID or VLAN configuration. When a user configures a port to VLAN X's untagged membership, this port's PVID will be updated with VLAN X. PVID is updated with the last item of the VLAN list. When a user removes a port from the untagged membership of the PVID's VLAN, the port's PVID will be assigned with "default VLAN".

### Format

**disable pvid auto_assign**

### Parameters

None.

### Restrictions

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

### Example

To disable the auto-assign PVID:

```
DGS-3620-28SC:admin#disable pvid auto_assign
Command: disable pvid auto_assign

Success.

DGS-3620-28SC:admin#
```

## 106-20 show pvid auto_assign

### Description

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

### Format

**show pvid auto_assign**

### Parameters

None.

## Restrictions

None.

## Example

To display the PVID auto-assignment state:

```
DGS-3620-28SC:admin#show pvid auto_assign

PVID Auto-assignment: Enabled.

DGS-3620-28SC:admin#
```

# Chapter 107 VLAN Trunking Commands

**enable vlan_trunk**

**disable vlan_trunk**

**config vlan_trunk ports** [<portlist> | all] state [enable | disable]

**show vlan_trunk**

## 107-1 enable vlan_trunk

### Description

This command is used to enable VLAN trunking. When VLAN trunking 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 Administrator, Operator and Power-User level users can issue this command.

### Example

To enable VLAN trunking:

```
DGS-3620-28SC:admin#enable vlan_trunk
Command: enable vlan_trunk

Success

DGS-3620-28SC:admin#
```

## 107-2 disable vlan_trunk

### Description

This command is used to disable VLAN trunking.

### Format

**disable vlan_trunk**

### Parameters

None.

### Restrictions

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

### Example

To disable VLAN trunking:

```
DGS-3620-28SC:admin#disable vlan_trunk
Command: disable vlan_trunk

Success.

DGS-3620-28SC:admin#
```

## 107-3 config vlan_trunk ports

### Description

This command is used to configure a port as a VLAN trunking port. By default, none of the ports is a VLAN trunking port. A VLAN trunking port and a non-VLAN trunking port cannot be grouped as an aggregated link. To change the VLAN trunking setting for an aggregated link, the user must apply the command to the master port. If the command is applied to link aggregation member port excluding the master, the command will be rejected. Ports with different VLAN configurations are not allowed to form an aggregated link. However, if they are specified as a VLAN trunking port, they are allowed to form an aggregated link.

For a VLAN trunking port, the VLANs on which the packets can be by passed will not be advertised by GVRP on this port. However, since the traffic on these VLANs is forwarded, this VLAN trunking port should participate in the MSTP instances corresponding to these VLANs.

### Format

**config vlan_trunk ports [<portlist> | all] | state [enable | disable]**

### Parameters

**ports** - Specify the ports to be configured.
**<portlist>** - Specify the list of ports to be configured.
**all** - Specify all ports will be configured.

**state** - Specify the ports as VLAN or non-VLAN trunking ports.
**enable** - Specify the ports as VLAN trunking ports.
**disable** - Specify the ports as non-VLAN trunking ports.

### Restrictions

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

### Example

To configure ports 1 to 5 as VLAN trunking ports:

```
DGS-3620-28SC:admin#config vlan_trunk ports 1-5 state enable
Command: config vlan_trunk ports 1-5 state enable

Success.

DGS-3620-28SC:admin#
```

To configure port 6 as an LA-1 member port and port 7 as an LA-2 master port:

```
DGS-3620-28SC: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-3620-28SC:admin# config vlan_trunk ports 7 state disable
Command: config vlan_trunk ports 7 state disable

Success.

DGS-3620-28SC: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-3620-28SC:admin#
```

To configure port 6 as an LA-1 member port and port 7 as an LA-1 master port:

```
DGS-3620-28SC:admin# config vlan_trunk ports 6-7 state enable
Command: config vlan_trunk ports 6-7 state enable

Success.

DGS-3620-28SC:admin#
```

Ports 6 and 7 have the same VLAN configuration before enabling VLAN trunking. To configure port 6 as an LA-1 member port and port 7 as an LA-1 master port:

```
DGS-3620-28SC:admin# config vlan_trunk ports 7 state disable
Command: config vlan_trunk ports 7 state disable

Success.
```

```
DGS-3620-28SC:admin# config vlan_trunk ports 6-7 state disable
Command: config vlan_trunk ports 6-7 state disable

Success.

DGS-3620-28SC:admin#
```

## 107-4 show vlan_trunk

### Description

This command is used to display VLAN trunking information.

### Format

**show vlan_trunk**

### Parameters

None.

### Restrictions

None.

### Example

To display the current VLAN trunking information:

```
DGS-3620-28SC:admin#show vlan_trunk
Command: show vlan_trunk

VLAN Trunk Global Setting
----------------------------
VLAN Trunk Status  : Disabled
VLAN Trunk Member Ports :

DGS-3620-28SC:admin#
```

# Chapter 108 Web-based Access Control (WAC) Commands

| |
|---|
| **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>} |
| **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** |

## 108-1 enable wac

### Description

This command is used to enable the WAC function.

### Format

**enable wac**

### Parameters

None.

### Restrictions

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

### Example

To enable the WAC function:

```
DGS-3620-28SC:admin#enable wac
Command: enable wac

Success.

DGS-3620-28SC:admin#
```

## 108-2 disable wac

### Description

This command is used to disable the WAC function.

### Format

**disable wac**

### Parameters

None.

### Restrictions

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

### Example

To disable the WAC function:

```
DGS-3620-28SC:admin#disable wac
Command: disable wac

Success.

DGS-3620-28SC:admin#
```

## 108-3 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 Administrator, Operator and Power-User level users can issue this command.

### Example

To configure the acceptance of an authorized configuration:

```
DGS-3620-28SC:admin#config wac authorization attributes local disable
Command: config wac authorization attributes local disable

Success.

DGS-3620-28SC:admin#
```

## 108-4 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>** - Specify 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>** - Specify 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>** - Specify 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>** - Specify a block time between 0 and 300 seconds.

### Restrictions

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

### Example

To configure the WAC port state:

```
DGS-3620-28SC:admin#config wac ports 1-8 state enable
Command: config wac ports 1-8 state enable

Success.

DGS-3620-28SC:admin#
```

To configure the WAC port aging time:

```
DGS-3620-28SC:admin#config wac ports 1-5 aging_time 200
Command: config wac ports 1-5 aging_time 200

Success.

DGS-3620-28SC:admin#
```

## 108-5 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 Administrator, Operator and Power-User level users can issue this command.

### Example

To configure the WAC authentication method:

```
DGS-3620-28SC:admin#config wac method radius
Command: config wac method radius

Success.

DGS-3620-28SC:admin#
```

## 108-6 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>** - Specify the URL that the client will be redirected to after successful authentication. By default, the redirected path is cleared.

### Restrictions

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

### Example

To configure the WAC default redirect path:

```
DGS-3620-28SC:admin#config wac default_redirpath http://www.dlink.com
Command: config wac default_redirpath http://www.dlink.com

Success.

DGS-3620-28SC:admin#
```

## 108-7 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 Administrator, Operator and Power-User level users can issue this command.

### Example

To clear the WAC default redirect path:

```
DGS-3620-28SC:admin#config wac clear_default_redirpath
Success.

DGS-3620-28SC:admin#
```

## 108-8 config wac virtual_ip

### Description

This command is used to configure the WAC virtual IP address. When virtual IP is specified, the TCP packets sent to the virtual IP will get a reply. If virtual IP is enabled, TCP packets sent to the virtual IP or physical IPIF’s IP address will both get the reply. When virtual IP is set 0.0.0.0, the virtual IP will be disabled. By default, the virtual IP is 0.0.0.0. The virtual IP will not respond to any ARP requests or ICMP packets. To make this function work properly, the virtual IP should not be an existing IP address. It also cannot be located on an existing subnet.

### Format

**config wac virtual_ip {<ipaddr> | <ipv6addr>}**

### Parameters

**<ipaddr>** - Specifies the IPv4 address of the virtual IP.

**<ipv6addr>** - Specifies the IPv6 address of the virtual IP.

### Restrictions

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

### Example

To configure the WAC virtual IP address used to accept authentication requests from unauthenticated hosts:

```
DGS-3620-28SC:admin# config wac virtual_ip 1.1.1.1
Command: config wac virtual_ip 1.1.1.1

Success.

DGS-3620-28SC:admin#
```

## 108-9 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>** - Specify 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 Administrator, Operator and Power-User level users can issue this command.

### Example

To configure a TCP port which the WAC switch listens to:

```
DGS-3620-28SC:admin# config wac switch_http_port 8888 http
Command: config wac switch_http_port 8888 http

Success.

DGS-3620-28SC:admin#
```

## 108-10 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> -** Specify the user account for Web-based Access Control. |
| **vlan** - (Optional) Specify the authentication VLAN name.<br>**<vlan_name 32>** - Specify 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>** - Specify the authentication VLAN ID number. The VLAN ID must be between 1 and 4094.

### Restrictions

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

### Example

To create a WAC account:

```
DGS-3620-28SC: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-3620-28SC:admin#
```

## 108-11 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>** - Specify 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 Administrator, Operator and Power-User level users can issue this command.

### Example

To delete a WAC account:

```
DGS-3620-28SC:admin#delete wac user duhon
Command: delete wac user duhon

Success.

DGS-3620-28SC:admin#
```

## 108-12 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>** - Specify the name of user account which will change its VID. |
| **vlan** - Specify the authentication VLAN name.<br>**<vlan_name 32>** - Specify the authentication VLAN name. The VLAN name can be up to 32 characters long. |
| **vlanid** - Specify the authentication VLAN ID.<br>**<vlanid 1-4094>** - Specify the authentication VLAN ID. The VLAN ID must be between 1 and 4094. |
| **clear_vlan** - Specify to clear the specified VLAN. |

### Restrictions

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

### Example

To configure the user's VLAN:

```
DGS-3620-28SC: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-3620-28SC:admin#
```

## 108-13 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-3620-28SC: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

DGS-3620-28SC:admin#
```

## 108-14 show wac ports

### Description

This command is used to display WAC port information.

### Format

**show wac ports {<portlist>}**

### Parameters

**<portlist>** - (Optional) Specify a range of member ports to display the status.

### Restrictions

None.

### Example

To display WAC ports 1 to 3:

```
DGS-3620-28SC: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-3620-28SC:admin#
```

## 108-15 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-3620-28SC:admin# show wac user
Command: show wac user

User Name          Password           VID
-----------------  -----------------  ---------
123                ************       1000

Total Entries   : 1

DGS-3620-28SC:admin#
```

## 108-16 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) Specify the list of ports whose WAC authentication state will be displayed. |

### Restrictions

None.

### Example

To display the WAC authentication status of ports:

```
DGS-3620-28SC: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-3620-28SC:admin#
```

## 108-17 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.<br>**<portlist>** - Specify a range of ports.<br>**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 Administrator, Operator and Power-User level users can issue this command.

### Example

To clear the WAC authentication state of ports 1 to 5:

```
DGS-3620-28SC:admin# clear wac auth_state ports 1-5
Command: clear wac auth_state ports 1-5

Success.

DGS-3620-28SC:admin#
```

## 108-18 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** - Specifies to reset the page elements to default.

**page_title** - Specifies to configure the title of the authentication page.
**<desc 128>** - Enter the page title used here. This value can be up to 128 characters long.

**login_window_title** - Specifies to configure the login window title of the authentication page
**<desc 64>** - Enter the login window title used here. This value can be up to 64 characters long.

**user_name_title** - Specifies to configure the user name title of the authentication page
**<desc 32>** - Enter the user name title used here. This value can be up to 32 characters long.

**password_title** - Specifies to configure the password title of the authentication page.
**<desc 32>** - Enter the password title used here. This value can be up to 32 characters long.

**logout_window_title** - Specifies to configure the logout window title of the authentication page.
**<desc 64>** - Enter the lohout window title used here. This value can be up to 64 characters long.

**notification_line** - Specifies to set the notification information by line in authentication Web pages.
**<value 1-5>** - Enter the notification line number used here. This value must be between 1 and 5.
**<desc 128>** - Enter the notification line description used here. This value can be up to 128 characters long.

### Restrictions

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

### Example

To customize the authenticate page elements:

```
DGS-3620-28SC:admin# config wac authentication_page element notification_line 1
Copyright @ 2011 D-Link All Rights Reserved
Command: config wac authentication_page element notification_line 1 Copyright @
2011 D-Link All Rights Reserved

Success.

DGS-3620-28SC:admin#
```

## 108-19 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-3620-28SC: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 @ 2011 D-Link All Rights Reserved
Site: http://support.dlink.com

DGS-3620-28SC: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:

- 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.
- Power on the switch. After the runtime image and UART init are loaded to 100%, the switch will allow 2 seconds for the user to press the hotkey [^] (Shift + 6) to enter the “Password Recovery Mode.” Once the switch enters the “Password Recovery Mode,” all ports on the switch will be disabled and all port LEDs will be lit.

```
  Boot Procedure                                          V1.00.013
-------------------------------------------------------------------------------


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

  MAC Address   : 00-03-38-10-28-01
  H/W Version   : A1

  Please Wait, Loading V2.00.009 Runtime Image .............  100 %
  UART init ................................................  100 %
```

```
Password Recovery Mode
>
```

- 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.<br>*force_agree* – Specify to forcibly agree with the command. |
| **reboot {force_agree}** | 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 |
|---|---|
| | *force_agree* - Specify to forcibly agree with the command. |
| **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 | Note |
|---|---|---|---|
| **MAC-based Access Control** | **Event description:** A host failed to pass the authentication<br>**Log Message:** MAC-based Access Control unauthenticated host (MAC: <macaddr>, Port <[unitID:]portNum>, VID: <vid>)<br>**Parameters description:**<br>**macaddr:** MAC address<br>**unitID:** The unit ID.<br>**portNum:** The port number.<br>**vid:** VLAN ID on which the host exists | Critical | |
| | **Event description:** The authorized user number on a port has reached the maximum user limit.<br>**Log Message:** Port < [unitID:]portNum> enters MAC-based Access Control stop learning state.<br>**Parameters description:**<br>**unitID:** The unit ID.<br>**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).<br>**Log Message:** Port <[unitID:]portNum> recovers from MAC-based Access Control stop learning state.<br>**Parameters description:**<br>**unitID:** The unit ID.<br>**portNum:** The port number. | Warning | |
| | **Event description:** The authorized user number on the whole device has reached the maximum user limit.<br>**Log Message:** MAC-based Access Control enters stop learning state.<br>**Parameters description:**<br>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).<br>**Log Message:** MAC-based Access Control recovers from stop learning state. | Warning | |

| | | | |
|---|---|---|---|
| | **Parameters description:**<br>None | | |
| | **Event description:** A host has passed the authentication.<br>**Log Message:** MAC-based Access Control host login successful (MAC: <macaddr>, port: <[unitID]portNum>, VID: <vid>)<br>**Parameters description:**<br>**macaddr:** The MAC address.<br>**unitID:** The unit ID.<br>**portNum:** The port number.<br>**vid:** The VLAN ID on which the host exists. | Informational | |
| | **Event description:** A host has aged out.<br>**Log Message:** MAC-based Access Control host aged out (MAC: <macaddr>, port: <[unitID]portNum>, VID: <vid>)<br>**Parameters description:**<br>**macaddr:** The MAC address<br>**unitID:** The unit ID.<br>**portNum:** The port number.<br>**vid:** The VLAN ID on which the host exists. | Informational | |
| **PTP** | **Event description:** PTP port role changed<br>**Log Message:** PTP port <[unitID:]portNum> role changed to <ptp_role>.<br>**Parameters description:**<br>**unitID:** The unit ID.<br>**portNum:** The port number.<br>**ptp_role:** The PTP role of the port. | Informational | |
| | **Event description:** PTP clock synchronized<br>**Log Message:** The boundary clock synchronized to its master, the offset value is <+\|-><Offset> second(s).<br>**Parameters description:**<br>**Offset:** The value of the offset between the slave and master. | Informational | Only when the synchronized more than one second, this log message will be send. |
| **DHCPv6 Client** | **Event description:** DHCPv6 client interface administrator state changed.<br>**Log Message:** DHCPv6 client on interface <ipif-name> changed state to [enabled \| disabled].<br>**Parameters description:**<br>**<ipif-name>:** Name of the DHCPv6 client interface. | Informational | |
| | **Event description:** DHCPv6 client obtains an ipv6 address from a DHCPv6 server. | Informational | |

| | | | |
|---|---|---|---|
| | **Log Message:** DHCPv6 client obtains an ipv6 address < ipv6address > on interface <ipif-name>.<br>**Parameters description:**<br>**ipv6address:** ipv6 address obtained from a DHCPv6 server.<br>**ipif-name:** Name of the DHCPv6 client interface. | | |
| | **Event description:** The ipv6 address obtained from a DHCPv6 server starts renewing.<br>**Log Message:** The IPv6 address < ipv6address > on interface <ipif-name> starts renewing.<br>**Parameters description:**<br>**ipv6address:** ipv6 address obtained from a DHCPv6 server.<br>**ipif-name:** Name of the DHCPv6 client interface. | Informational | |
| | **Event description:** The ipv6 address obtained from a DHCPv6 server renews success.<br>**Log Message:** The IPv6 address < ipv6address > on interface <ipif-name> renews success.<br>**Parameters description:**<br>**ipv6address:** ipv6 address obtained from a DHCPv6 server.<br>**ipif-name:** Name of the DHCPv6 client interface. | Informational | |
| | **Event description:** The ipv6 address obtained from a DHCPv6 server starts rebinding<br>**Log Message:** The IPv6 address < ipv6address > on interface <ipif-name> starts rebinding.<br>**Parameters description:**<br>**ipv6address:** ipv6 address obtained from a DHCPv6 server.<br>**ipif-name:** Name of the DHCPv6 client interface. | Informational | |
| | **Event description:** The ipv6 address obtained from a DHCPv6 server rebinds success<br>**Log Message:** The IPv6 address < ipv6address > on interface <ipif-name> rebinds success.<br>**Parameters description:**<br>**ipv6address:** ipv6 address obtained from a DHCPv6 server.<br>**ipif-name:** Name of the DHCPv6 client interface.. | Informational | |
| | **Event description:** The ipv6 address from a DHCPv6 server was deleted.<br>**Log Message:** The IPv6 address < ipv6address > on interface <ipif-name> was deleted.<br>**Parameters description:**<br>**ipv6address:** ipv6 address obtained from a DHCPv6 server. | Informational | |

| | | | |
|---|---|---|---|
| | **ipif-name:** Name of the DHCPv6 client interface. | | |
| **DHCPv6 Relay** | **Event description:** DHCPv6 relay on a specify interface's administrator state changed<br>**Log Message:** DHCPv6 relay on interface <ipif-name> changed state to [enabled \| disabled]<br>**Parameters description:**<br>**<ipif-name>:** Name of the DHCPv6 relay agent interface. | Informational | |
| **DHCPv6 Server** | **Event description:** The address of the DHCPv6 Server pool is used up<br>**Log Message:** The address of the DHCPv6 Server pool <pool-name> is used up.<br>**Parameters description:**<br>**<pool-name>:** Name of the DHCPv6 Server pool. | Informational | |
| | **Event description:** The number of allocated ipv6 addresses is equal to 4096<br>**Log Message:** The number of allocated ipv6 addresses of the DHCPv6 Server pool is equal to 4096.<br>**Parameters description:** | Informational | |
| **IP Directed-Broadcast** | **Event description:** IP Directed-broadcast rate exceed 50 packets per second on a certain subnet.<br>**Log Message:** IP Directed Broadcast packet rate is high on subnet. [(IP: %s)]<br>**Parameters description:**<br>**IP:** the Broadcast IP destination address. | Informational | |
| | **Event description:** IP Directed-broadcast rate exceed 100 packets per second<br>**Log Message:** IP Directed Broadcast rate is high.<br>**Parameters description:** | Informational | |
| **RCP** | **Event description:** Firmware upgraded successfully.<br>**Log Message:** [RCP(1):] [Unit <unitID>,] Firmware upgraded by <session> successfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)<br>**Parameters description:**<br>**unitID:** Represent the id of the device in the stacking system.<br>**session:** The user's session.<br>**username:** Represent current login user.<br>**ipaddr:** Represent client IP address.<br>**macaddr :** Represent client MAC address. | Informational | |
| | **Event description:** Firmware upgrade unsuccessfully.<br>**Log Message:** [RCP(2):] [Unit <unitID>,] Firmware upgrade by | warning | |

| | | | |
|---|---|---|---|
| | <session> unsuccessfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)<br>**Parameters description:**<br>**unitID:** Represent the id of the device in the stacking system.<br>**session:** The user's session.<br>**username:** Represent current login user.<br>**ipaddr:** Represent client IP address.<br>**macaddr :** Represent client MAC address. | | |
| | **Event description:** Firmware uploaded successfully.<br>**Log Message:** [RCP(3):]Firmware uploaded by <session> successfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)<br>**Parameters description:**<br>**session:** The user's session.<br>**username:** Represent current login user.<br>**ipaddr:** Represent client IP address.<br>**macaddr :** Represent client MAC address. | informational | |
| | **Event description:** Firmware upload unsuccessfully.<br>**Log Message:** [RCP(4):]Firmware upload by <session> unsuccessfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)<br>**Parameters description:**<br>**session:** The user's session.<br>**username:** Represent current login user.<br>**ipaddr:** Represent client IP address. | warning | |
| | **Event description:** Configuration downloaded successfully.<br>**Log Message:** [RCP(5):]Configuration downloaded by <session> successfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)<br>**Parameters description:**<br>**session:** The user's session.<br>**username:** Represent current login user.<br>**ipaddr:** Represent client IP address.<br>**macaddr :** Represent client MAC address. | informational | |
| | **Event description:** Configuration download unsuccessfully.<br>**Log Message:** [RCP(6):]Configuration download by <session> unsuccessfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)<br>**Parameters description:**<br>**session:** The user's session. | warning | |

| | | | |
|---|---|---|---|
| | **username:** Represent current login user.<br>**ipaddr:** Represent client IP address.<br>**macaddr :** Represent client MAC address. | | |
| | **Event description:** Configuration uploaded successfully.<br>**Log Message:** [RCP(7):]Configuration uploaded by <session> successfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)<br>**Parameters description:**<br>**session:** The user’s session.<br>**username:** Represent current login user.<br>**ipaddr:** Represent client IP address.<br>**macaddr :** Represent client MAC address. | informational | |
| | **Event description:** Configuration upload unsuccessfully.<br>**Log Message:** [RCP(8):]Configuration upload by <session> unsuccessfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)<br>**Parameters description:**<br>**session:** The user’s session.<br>**username:** Represent current login user.<br>**ipaddr:** Represent client IP address.<br>**macaddr :** Represent client MAC address. | warning | |
| | **Event description:** Log message uploaded successfully.<br>**Log Message:** [RCP(9):]Log message uploaded by <session> successfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)<br>**Parameters description:**<br>**session:** The user’s session.<br>**username:** Represent current login user.<br>**ipaddr:** Represent client IP address.<br>**macaddr :** Represent client MAC address. | informational | |
| | **Event description:** Log message upload unsuccessfully.<br>**Log Message:** [RCP(10):]Log message upload by <session> unsuccessfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)<br>**Parameters description:**<br>**session:** The user’s session.<br>**username:** Represent current login user.<br>**ipaddr:** Represent client IP address.<br>**macaddr :** Represent client MAC address. | warning | |
| | **Event description:** The downloaded configurations executed successfully. | informational | |

| | | | |
|---|---|---|---|
| | **Log Message:** [RCP(11):]The downloaded configurations executed by <session> successfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)<br>**Parameters description:**<br>**session:** The user's session.<br>**username:** Represent current login user.<br>**ipaddr:** Represent client IP address.<br>**macaddr :** Represent client MAC address. | | |
| | **Event description:** The downloaded configurations execute unsuccessfully.<br>**Log Message:** [RCP(12):]The downloaded configurations executed by <session> unsuccessfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)<br>**Parameters description:**<br>**session:** The user's session.<br>**username:** Represent current login user.<br>**ipaddr:** Represent client IP address.<br>**macaddr :** Represent client MAC address. | warning | |
| | **Event description:** Attack log message uploaded successfully.<br>**Log Message:** [RCP(13):]Attack log message uploaded by <session> successfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)<br>**Parameters description:**<br>**session:** The user's session.<br>**username:** Represent current login user.<br>**ipaddr:** Represent client IP address.<br>**macaddr :** Represent client MAC address. | informational | |
| | **Event description:** Attack log message upload unsuccessfully.<br>**Log Message:** [RCP(14):]Attack log message upload by <session> unsuccessfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)<br>**Parameters description:**<br>**session:** The user's session.<br>**username:** Represent current login user.<br>**ipaddr:** Represent client IP address.<br>**macaddr :** Represent client MAC address. | warning | |
| **TFTP Client** | **Event description:** Firmware upgraded successfully.<br>**Log Message:** [TFTP(1):] [Unit <unitID>,] Firmware upgraded by <session> successfully (Username: <username>, IP: <ipaddr>, MAC: <macaddr>) | Informational | |

| | | | |
|---|---|---|---|
| | **Parameters description:**<br>**UnitID:** Represent the id of the device in the stacking system.<br>**session:** The user's session.<br>**Username:** Represent current login user.<br>**Ipaddr:** Represent client IP address.<br>**macaddr :** Represent client MAC address. | | |
| | **Event description:** Firmware upgrade was unsuccessful.<br>**Log Message:** [TFTP(2):] [Unit <unitID>,] Firmware upgrade by <session> was unsuccessful! (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)<br>**Parameters description:**<br>**UnitID:** Represent the id of the device in the stacking system.<br>**session:** The user's session.<br>**Username:** Represent current login user.<br>**Ipaddr:** Represent client IP address.<br>**macaddr :** Represent client MAC address. | warning | |
| | **Event description:** Firmware successfully uploaded.<br>**Log Message:** [TFTP(3):]Firmware successfully uploaded by <session> (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)<br>**Parameters description:**<br>**session:** The user's session.<br>**Username:** Represent current login user.<br>**Ipaddr:** Represent client IP address.<br>**macaddr :** Represent client MAC address. | informational | |
| | **Event description:** Firmware upload was unsuccessful.<br>**Log Message:** [TFTP(4):]Firmware upload by <session> was unsuccessful! (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)<br>**Parameters description:**<br>**session:** The user's session.<br>**Username:** Represent current login user.<br>**Ipaddr:** Represent client IP address. | warning | |
| | **Event description:** Configuration successfully downloaded.<br>**Log Message:** [TFTP(5):]Configuration successfully downloaded by <session> (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)<br>**Parameters description:**<br>**session:** The user's session.<br>**Username:** Represent current login user. | informational | |

| | | | |
|---|---|---|---|
| | **Ipaddr:** Represent client IP address.<br>**macaddr :** Represent client MAC address. | | |
| | **Event description:** Configuration download was unsuccessful.<br>**Log Message:** [TFTP(6):]Configuration download by <session> was unsuccessful! (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)<br>**Parameters description:**<br>**session:** The user's session.<br>**Username:** Represent current login user.<br>**Ipaddr:** Represent client IP address.<br>**macaddr :** Represent client MAC address. | warning | |
| | **Event description:** Configuration successfully uploaded.<br>**Log Message:** [TFTP(7):]Configuration successfully uploaded by <session> (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)<br>**Parameters description:**<br>**session:** The user's session.<br>**Username:** Represent current login user.<br>**Ipaddr:** Represent client IP address.<br>**macaddr :** Represent client MAC address. | informational | |
| | **Event description:** Configuration upload was unsuccessful.<br>**Log Message:** [TFTP(8):]Configuration upload by <session> was unsuccessful! (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)<br>**Parameters description:**<br>**session:** The user's session.<br>**Username:** Represent current login user.<br>**Ipaddr:** Represent client IP address.<br>**macaddr :** Represent client MAC address. | warning | |
| | **Event description:** Log message successfully uploaded.<br>**Log Message:** [TFTP(9):]Log message successfully uploaded by <session> (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)<br>**Parameters description:**<br>**session:** The user's session.<br>**Username:** Represent current login user.<br>**Ipaddr:** Represent client IP address.<br>**macaddr :** Represent client MAC address. | informational | |
| | **Event description:** Log message upload was unsuccessful.<br>**Log Message:** [TFTP(10):]Log message upload by <session> was unsuccessful! (Username: <username>, IP: <ipaddr>, MAC: | warning | |

| | | | |
|---|---|---|---|
| | <macaddr>)<br>**Parameters description:**<br>**session:** The user's session.<br>**Username:** Represent current login user.<br>**Ipaddr:** Represent client IP address.<br>**macaddr :** Represent client MAC address. | | |
| | **Event description:** Attack log message successfully uploaded.<br>**Log Message:** [TFTP(13):]Attack log message successfully uploaded by <session> (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)<br>**Parameters description:**<br>**session:** The user's session.<br>**Username:** Represent current login user.<br>**Ipaddr:** Represent client IP address.<br>**macaddr :** Represent client MAC address. | informational | |
| | **Event description:** Attack log message upload was unsuccessful.<br>**Log Message:** [TFTP(14):]Attack log message upload by <session> was unsuccessful! (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)<br>**Parameters description:**<br>**session:** The user's session.<br>**Username:** Represent current login user.<br>**Ipaddr:** Represent client IP address.<br>**macaddr :** Represent client MAC address. | warning | |
| **DNS Resolver** | **Event description:** Duplicate Domain name cache added, leads a dynamic domain name cache be deleted<br>**Log Message:** [DNS_RESOLVER(1):]Duplicate Domain name case name: <domainname>, static IP: <ipaddr>, dynamic IP:<ipaddr><br>**Parameters description:**<br>**domainame:** the domain name string.<br>**ipaddr:** IP address. | Informational | |
| **ARP** | **Event description:** Gratuituios ARP detected duplicate IP.<br>**Log Message:** Conflict IP was detected with this device (IP: <ipaddr>, MAC: <macaddr>, Port <[unitID:]portNum>, Interface: <ipif_name>).<br>**Parameters description:**<br>**ipaddr:** The IP address which is duplicated with our device.<br>**macaddr:** The MAC address of the device that has duplicated IP | Warning | |

| | | | |
|---|---|---|---|
| | address as our device.<br>**unitID:** 1.Interger value;2.Represent the id of the device in the stacking system.<br>**portNum:** 1.Interger value;2.Represent the logic port number of the device.<br>**ipif_name:** The name of the interface of the switch which has the conflic IP address. | | |
| **Telnet** | **Event description:** Successful login through Telnet.<br>**Log Message:** Successful login through Telnet (Username: <username>, IP: <ipaddr>)<br>**Parameters description:**<br>**ipaddr:** The IP address of telnet client.<br>**username:** the user name that used to login telnet server. | Informational | |
| | **Event description:** Login failed through Telnet.<br>**Log Message:** Login failed through Telnet (Username: <username>, IP: <ipaddr>)<br>**Parameters description:**<br>**ipaddr:** The IP address of telnet client.<br>**username:** the user name that used to login telnet server. | Warning | |
| | **Event description:** Logout through Telnet.<br>**Log Message:** Logout through Telnet (Username: <username>, IP: <ipaddr>)<br>**Parameters description:**<br>**ipaddr:** The IP address of telnet client.<br>**username:** the user name that used to login telnet server. | Informational | |
| | **Event description:** Telnet session timed out.<br>**Log Message:** Telnet session timed out (Username: <username>, IP: <ipaddr>).<br>**Parameters description:**<br>**ipaddr:** The IP address of telnet client.<br>**username:** the user name that used to login telnet server. | Informational | |
| **Interface** | **Event description:** Port link up.<br>**Log Message:** Port <[unitID:]portNum> link up, <link state><br>**Parameters description:**<br>**unitID:** 1.Interger value;2.Represent the id of the device in the stacking system.<br>**portNum:** 1.Interger value;2.Represent the logic port number of the device.<br>**link state:** for ex: , 100Mbps FULL duplex | Informational | |
| | **Event description:** Port link down. | Informational | |

| | | | |
|---|---|---|---|
| | **Log Message:** Port <[unitID:]portNum> link down<br>**Parameters description:**<br>**unitID:** 1.Interger value;2.Represent the id of the device in the stacking system.<br>**portNum:** 1.Interger value;2.Represent the logic port number of the device. | | |
| **802.1X** | **Event description:** 802.1X Authentication failure.<br>**Log Message:** 802.1X Authentication failure [for <reason> ] from (Username: <username>, Port: <[unitID:]portNum>, MAC: <macaddr> )<br>**Parameters description:**<br>**reason:** The reason for the failed authentication.<br>**username:** The user that is being authenticated.<br>**unitID:** The unit ID.<br>**portNum:** The switch port number.<br>**macaddr:** The MAC address of thr authenticated device. | Warning | |
| | **Event description:** 802.1X Authentication successful.<br>**Log Message:** 802.1X Authentication successful from (Username: <username>, Port: <[unitID:]portNum>, MAC: <macaddr>)<br>**Parameters description:**<br>**username:** The user that is being authenticated.<br>**unitID:** The unit ID.<br>**portNum:** The switch port number.<br>**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.<br>**Log Message:** RADIUS server <ipaddr>  assigned VID :<vlanID> to port  <[unitID:]portNum> (account :<username> )<br>**Parameters description:**<br>**ipaddr:** The IP address of the RADIUS server.<br>**vlanID:** The VID of RADIUS assigned VLAN.<br>**unitID:** The unit ID.<br>**portNum:** The port number.<br>**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.<br>**Log Message:** RADIUS server <ipaddr>  assigned ingress bandwith :<ingressBandwidth> to port  <[unitID:]portNum> (account : <username>) | Informational | |

| | | | |
|---|---|---|---|
| | **Parameters description:**<br>**ipaddr:** The IP address of the RADIUS server.<br>**ingressBandwidth:** The ingress bandwidth of RADIUS assign.<br>**unitID:** The unit ID.<br>**portNum:** The port number.<br>**Username:** The user that is being authenticated. | | |
| | **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.<br>**Log Message:** RADIUS server <ipaddr>  assigned egress bandwith :<egressBandwidth> to  port  <[unitID:]portNum> (account: <username>)<br>**Parameters description:**<br>**ipaddr:** The IP address of the RADIUS server.<br>**egressBandwidth:** The egress bandwidth of RADIUS assign.<br>**unitID:** The unit ID.<br>**portNum:** The port number.<br>**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.<br>**Log Message:** RADIUS server <ipaddr>  assigned 802.1p default priority:<priority> to  port  <[unitID:]portNum> (account : <username>)<br>**Parameters description:**<br>**ipaddr:** The IP address of the RADIUS server.<br>**priority:** Priority of RADIUS assign.<br>**unitID:** The unit ID.<br>**portNum:** The port number.<br>**Username:** The user that is being authenticated. | Informational | |
| | **Event description:** Failed to assign ACL profiles/rules from RADIUS server.<br>**Log Message:** RADIUS server <ipaddr> assigns <username> ACL failure at port <[unitID]portNum> (<string>)<br>**Parameters description:**<br>**ipaddr:** The IP address of the RADIUS server.<br>**unitID:** The unit ID.<br>**portNum:** The port number.<br>**Username:** The user that is being authenticated.<br>**string**: The failed RADIUS ACL command string. | Warning | |

| | | | |
|---|---|---|---|
| **LLDP (MED)** | **Event description:** LLDP-MED topology change detected<br>**Log Message:** LLDP-MED topology change detected (on port <portNum>. chassis id: <chassisType>, <chassisID>, port id: <portType>, <portID>, device class: <deviceClass>)<br>**Parameters description:**<br>**portNum:** The port number.<br>**chassisType:** chassis ID subtype.<br>Value list:<br>1. chassisComponent(1)<br>2. interfaceAlias(2)<br>3. portComponent(3)<br>4. macAddress(4)<br>5. networkAddress(5)<br>6. interfaceName(6)<br>7. local(7)<br>**chassisID:** chassis ID.<br>**portType:** port ID subtype.<br>Value list:<br>1. interfaceAlias(1)<br>2. portComponent(2)<br>3. macAddress(3)<br>4. networkAddress(4)<br>5. interfaceName(5)<br>6. agentCircuitId(6)<br>7. local(7)<br>**portID:** port ID.<br>**deviceClass:** LLDP-MED device type. | Notice | |
| | **Event description:** Conflict LLDP-MED device type detected<br>**Log Message:** Conflict LLDP-MED device type detected ( on port < portNum >, chassis id: < chassisType>, <chassisID>, port id: < portType>, <portID>, device class: <deviceClass>)<br>**Parameters description:**<br>**portNum:** The port number.<br>**chassisType:** chassis ID subtype.<br>Value list:<br>1. chassisComponent(1)<br>2. interfaceAlias(2)<br>3. portComponent(3)<br>4. macAddress(4)<br>5. networkAddress(5)<br>6. interfaceName(6) | Notice | |

| | | | |
|---|---|---|---|
| | 7. local(7)<br>**chassisID:** chassis ID.<br>**portType:** port ID subtype.<br>Value list:<br>1. interfaceAlias(1)<br>2. portComponent(2)<br>3. macAddress(3)<br>4. networkAddress(4)<br>5. interfaceName(5)<br>6. agentCircuitId(6)<br>7. local(7)<br>**portID:** port ID.<br>**deviceClass:** LLDP-MED device type. | | |
| | **Event description:** Incompatible LLDP-MED TLV set detected<br>**Log Message:** Incompatible LLDP-MED TLV set detected ( on port < portNum >, chassis id: < chassisType>, <chassisID>, port id: < portType>, <portID>, device class: <deviceClass>)<br>**Parameters description:**<br>**portNum:** The port number.<br>**chassisType:** chassis ID subtype.<br>Value list:<br>1. chassisComponent(1)<br>2. interfaceAlias(2)<br>3. portComponent(3)<br>4. macAddress(4)<br>5. networkAddress(5)<br>6. interfaceName(6)<br>7. local(7)<br>**chassisID:** chassis ID.<br>**portType:** port ID subtype.<br>Value list:<br>1. interfaceAlias(1)<br>2. portComponent(2)<br>3. macAddress(3)<br>4. networkAddress(4)<br>5. interfaceName(5)<br>6. agentCircuitId(6)<br>7. local(7)<br>**portID:** port ID.<br>**deviceClass:** LLDP-MED device type. | Notice | |
| **Voice VLAN** | **Event description:** When a new voice device is detected in the | Informational | |

| | | | |
|---|---|---|---|
| | port.<br>**Log Message:** New voice device detected (Port <portNum>, MAC <macaddr>)<br>**Parameters description:**<br>**portNum :** The port number.<br>**macaddr:** Voice device MAC address | | |
| | **Event description:** When a port which is in auto Voice VLAN mode joins the Voice VLAN<br>**Log Message:** Port < portNum > add into Voice VLAN <vid ><br>**Parameters description:**<br>**portNum :** The port number.<br>**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.<br>**Log Message:** Port < portNum > remove from Voice VLAN <vid ><br>**Parameters description:**<br>**portNum :** The port number.<br>**vid:**VLAN ID | Informational | |
| **DULD** | **Event description:** A unidirectional link has been detected on this port<br>**Log Message:** [DULD(1):] port:<[unitID:]<br>portNum> is unidirectional.<br>**Parameters description:**<br>**unitID:** the unit ID<br>**portNum:** port number | Informational | |
| **BGP** | **Event description:** BGP FSM with Peer has gone to the successfully established state.<br>**Log Message:** [BGP(1):] BGP connection is successfully established (Peer:<ipaddr>).<br>**Parameters description:**<br>**ipaddr:** IP address of BGP peer. | Informational | |
| | **Event description:** BGP connection is normally closed.<br>**Log Message**:[BGP(2):] BGP connection is normally closed(Peer:<ipaddr>).<br>**Parameters description:**<br>**ipaddr:** IP address of BGP peer. | Informational | |
| | **Event description:** BGP connection is closed due to error (Error | warning | |

| | | | |
|---|---|---|---|
| | Code, Error Subcode and Data fields Refer to RFC).<br>**Log Message:** [BGP(3):] BGP connection is closed due to error (Code:<num> Subcode:<num> Field:<field> Peer:<ipaddr>).<br>**Parameters description:**<br>**num:** Error Code or Error Subcode is defined in RFC 4271 etc.<br>**field:** field value when an error happen.<br>**ipaddr:** IP address of the BGP peer. | | |
| | **Event description:** Receive a BGP notify packet with an undefined error code or sub error code in RFC 4271.<br>**Log Message:** [BGP(4):] BGP Notify: unkown Error code(num), Sub Error code(num), Peer:<ipaddr>.<br>**Parameters description:**<br>**num:** Error Code or Error Subcode is defined in RFC 4271 etc.<br>**ipaddr:** IP address of BGP peer. | warning | |
| | **Event description:** Receive a BGP update packet but the next_hop points to a local interface.<br>**Log Message:** [BGP(5):] BGP Update Attr NHop: Erroneous NHop <ipaddr> Peer:<ipaddr>.<br>**Parameters description:**<br>**ipaddr:** IP address of BGP peer. | warning | |
| | **Event description:** BGP connection is closed due to some events happens. (Event refer to RFC)<br>**Log Message:** [BGP(6):] BGP connection is closed due to Event: <num> (Peer:<ipaddr>).<br>**Parameters description:**<br>**num:** Event is defined in RFC 4271 etc.<br>**ipaddr:** IP address of BGP peer. | warning | |
| | **Event description:** BGP connection is closed due to receive notify packet. (Error Code and Error Subcode refer to RFC)<br>**Log Message:** [BGP(7):] BGP connection is closed due to Notify: Code <num> Subcode <num> (Peer:<ipaddr>).<br>**Parameters description:**<br>**num:** Error Code or Error Subcode is defined in RFC 4271 etc.<br>**ipaddr:** IP address of BGP peer. | warning | |
| | **Event description:** The number of bgp prefix received from this neighbor reaches the threshold.<br>**Log Message:** [BGP(8):] The number of prefix received reaches <num>, max <limit> (Peer < ipaddr >).<br>**Parameters description:** | warning | |

| | | | |
|---|---|---|---|
| | **num:** The number of prefix received.<br>**limit:** Max number of prefix allowed to receive.<br>**ipaddr:** IP address of BGP peer. | | |
| | **Event description:** The total bgp prefix number received exceeds the limit.<br>**Log Message:** [BGP(9):] The total number of prefix received reaches max prefix limit. | warning | |
| **Stacking** | **Event description:** Hot insertion.<br>**Log Message:** Unit: <unitID>, MAC: <macaddr> Hot insertion.<br>**Parameters description:**<br>**unitID:** Box ID.<br>**Macaddr:** MAC address. | Informational | |
| | **Event description:** Hot removal.<br>**Log Message:** Unit: <unitID>, MAC: <macaddr> Hot removal.<br>**Parameters description:**<br>**unitID:** Box ID.<br>**Macaddr:** MAC address. | Informational | |
| | **Event description:** Stacking topology change.<br>**Log Message:** Stacking topology is <Stack_TP_TYPE>. Master(Unit <unitID>, MAC:<macaddr>).<br>**Parameters description:**<br>**Stack_TP_TYPE:** The stacking topology type is one of the following:<br>1. Ring,<br>2. Chain.<br>**unitID:** Box ID.<br>**Macaddr:** MAC address. | Informational | |
| | **Event description:** Backup master changed to master.<br>**Log Message:** Backup master changed to master. Master (Unit: <unitID>).<br>**Parameters description:**<br>**unitID:** Box ID. | Informational | |
| | **Event description:** Slave changed to master<br>**Log Message:** Slave changed to master. Master (Unit: <unitID>).<br>**Parameters description:**<br>**unitID:** Box ID. | Informational | |
| | **Event description:** Box ID conflict.<br>**Log Message:** Hot insert failed, box ID conflict: Unit <unitID> | Critical | |

| | | | |
|---|---|---|---|
| | conflict (MAC: <macaddr> and MAC: <macaddr>).<br>**Parameters description:**<br>**unitID:** Box ID.<br>**macaddr:** The MAC addresses of the conflicting boxes. | | |
| **SNMP** | **Event Description:** SNMP request received with invalid community string<br>**Log Message:** SNMP request received from <ipaddr> with invalid community string.<br>**Parameters Description:**<br>**ipaddr:** The IP address. | Informational | |
| **OSPFv2 Enhancement Function** | **Event description:** OSPF interface link state changed.<br>**Log Message:** OSPF interface <intf-name> changed state to [Up \| Down]<br>**Parameters description:**<br>**intf-name:** Name of OSPF interface. | Informational | |
| | **Event description:** OSPF interface administrator state changed.<br>**Log Message:** OSPF protocol on interface <intf-name> changed state to [Enabled \| Disabled]<br>**Parameters description:**<br>**intf-name:** Name of OSPF interface. | Informational | |
| | **Event description:** One OSPF interface changed from one area to another.<br>**Log Message:** OSPF interface <intf-name> changed from area <area-id> to area <area-id><br>**Parameters description:**<br>**intf-name:** Name of OSPF interface.<br>**area-id:** OSPF area ID. | Informational | |
| | **Event description:** One OSPF neighbor state changed from Loading to Full.<br>**Log Message:** OSPF nbr <nbr-id> on interface <intf-name> changed state from Loading to Full<br>**Parameters description:**<br>**intf-name:** Name of OSPF interface.<br>**nbr-id:** Neighbor's router ID. | notice | |
| | **Event description:** One OSPF neighbor state changed from Full to Down.<br>**Log Message:** OSPF nbr <nbr-id> on interface <intf-name> changed state from Full to Down<br>**Parameters description:** | notice | |

| | | | |
|---|---|---|---|
| | **intf-name:** Name of OSPF interface.<br>**nbr-id:** Neighbor's router ID. | | |
| | **Event description:** One OSPF neighbor state's dead timer expired.<br>**Log Message:** OSPF nbr <nbr-id> on interface <intf-name> dead timer expired<br>**Parameters description:**<br>**intf-name:** Name of OSPF interface.<br>**nbr-id:** Neighbor's router ID. | notice | |
| | **Event description:** One OSPF virtual neighbor state changed from Loading to Full.<br>**Log Message:** OSPF nbr <nbr-id> on virtual link changed state from Loading to Full<br>**Parameters description:**<br>**nbr-id:** Neighbor's router ID. | notice | |
| | **Event description:** One OSPF virtual neighbor state changed from Full to Down.<br>**Log Message:** OSPF nbr <nbr-id> on virtual link changed state from Full to Down<br>**Parameters description:**<br>**nbr-id:** Neighbor's router ID. | notice | |
| | **Event description:** OSPF router ID was changed.<br>**Log Message:** OSPF router ID changed to <router-id><br>**Parameters description:**<br>**router-id:** OSPF router ID. | Informational | |
| | **Event description:** Enable OSPF.<br>**Log Message:** OSPF state changed to Enabled | Informational | |
| | **Event description:** Disable OSPF.<br>**Log Message:** OSPF state changed to Disabled | Informational | |
| **VRRP Debug** | **Event description:** One virtual router state becomes Master.<br>**Log Message:** VR <vr-id> at interface <intf-name> switch to Master<br>**Parameters description:**<br>**vr-id:** VRRP virtual router ID.<br>**intf-name:** Interface name on which virtual router is based. | Informational | |
| | **Event description:** One virtual router state becomes Backup.<br>**Log Message:** VR <vr-id> at interface <intf-name> switch to Backup<br>**Parameters description:**<br>**vr-id:** VRRP virtual router ID.<br>**intf-name:** Interface name on which virtual router is based. | Informational | |

| | | | |
|---|---|---|---|
| | **Event description:** One virtual router state becomes Init.<br>**Log Message:** VR <vr-id> at interface <intf-name> switch to Init<br>**Parameters description:**<br>**vr-id:** VRRP virtual router ID.<br>**intf-name:** Interface name on which virtual router is based. | Informational | |
| | **Event description:** Authentication type mismatch of one received VRRP advertisement message.<br>**Log Message:** Authentication type mismatch on VR <vr-id> at interface <intf-name><br>**Parameters description:**<br>**vr-id:** VRRP virtual router ID.<br>**intf-name:** Interface name on which virtual router is based. | Warning | |
| | **Event description:** Authentication checking fail of one received VRRP advertisement message.<br>**Log Message:** Authentication fail on VR <vr-id> at interface <intf-name>. Auth type <auth-type><br>**Parameters description:**<br>**vr-id:** VRRP virtual router ID.<br>**intf-name:** Interface name on which virtual router is based.<br>**Auth-type:** VRRP interface authentication type. | Warning | |
| | **Event description:** Checksum error of one received VRRP advertisement message.<br>**Log Message:** Received an ADV msg with incorrect checksum on VR <vr-id> at interface <intf-name><br>**Parameters description:**<br>**vr-id:** VRRP virtual router ID.<br>**intf-name:** Interface name on which virtual router is based. | Warning | |
| | **Event description:** Virtual router ID mismatch of one received VRRP advertisement message.<br>**Log Message:** Received ADV msg virtual router ID mismatch. VR <vr-id> at interface <intf-name><br>**Parameters description:**<br>**vr-id:** VRRP virtual router ID.<br>**intf-name:** Interface name on which virtual router is based. | Warning | |
| | **Event description:** Advertisement interval mismatch of one received VRRP advertisement message.<br>**Log Message:** Received ADV msg adv interval mismatch. VR <vr-id> at interface <intf-name><br>**Parameters description:**<br>**vr-id:** VRRP virtual router ID.<br>**intf-name:** Interface name on which virtual router is based. | Warning | |
| | **Event description:** A virtual MAC address is added into switch L2 table<br>**Log Message:** Added a virtual MAC <vrrp-mac-addr> into L2 table<br>**Parameters description:** | Notice | |

| | | | |
|---|---|---|---|
| | **vrrp-mac-addr:** VRRP virtual MAC address | | |
| | **Event description:** A virtual MAC address is deleted from switch L2 table.<br>**Log Message:** Deleted a virtual MAC <vrrp-mac-addr> from L2 table<br>**Parameters description:**<br>**vrrp-mac-addr:** VRRP virtual MAC address | Notice | |
| | **Event description:** A virtual MAC address is adding into switch L3 table.<br>**Log Message:** Added a virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table<br>**Parameters description:**<br>**vrrp-ip-addr:** VRRP virtual IP address<br>**vrrp-mac-addr:** VRRP virtual MAC address | Notice | |
| | **Event description:** A virtual MAC address is deleting from switch L3 table.<br>**Log Message:** Deleted a virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> from L3 table<br>**Parameters description:**<br>**vrrp-ip-addr:** VRRP virtual IP address<br>**vrrp-mac-addr:** VRRP virtual MAC address | Notice | |
| | **Event description:** Failed when adding a virtual MAC into switch chip L2 table.<br>**Log Message:** Failed to add virtual MAC <vrrp-mac-addr> into chip L2 table.  Errcode <vrrp-errcode><br>**Parameters description:**<br>**vrrp-mac-addr:** VRRP virtual MAC address<br>**vrrp-errcode:** Errcode of VRRP protocol behavior. | Error | |
| | **Event description:** Failed when deleting a virtual MAC from switch chip L2 table.<br>**Log Message:** Failed to delete virtual MAC <vrrp-mac-addr> from chip L2 table. Errcode <vrrp-errcode><br>**Parameters description:**<br>**vrrp-mac-addr:** VRRP virtual MAC address<br>**vrrp-errcode:** Errcode of VRRP protocol behaviour. | Error | |
| | **Event description:** Failed when adding a virtual MAC into switch L3 table. The L3 table is full.<br>**Log Message:** Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table. L3 table is full<br>**Parameters description:**<br>**vrrp-ip-addr:** VRRP virtual IP address<br>**vrrp-mac-addr:** VRRP virtual MAC address | Error | |
| | **Event description:** Failed when adding a virtual MAC into switch L3 table. The port where the MAC is learned from is invalid.<br>**Log Message:** Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table. Port <mac-port> is invalid | Error | |

| | | | |
|---|---|---|---|
| | **Parameters description:**<br>**vrrp-ip-addr:** VRRP virtual IP address<br>**vrrp-mac-addr:** VRRP virtual MAC address<br>**mac-port:** port number of VRRP virtual MAC. | | |
| | **Event description:** Failed when adding a virtual MAC into switch L3 table. The interface where the MAC is learned from is invalid.<br>**Log Message:** Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table. Interface <mac-intf> is invalid<br>**Parameters description:**<br>**vrrp-ip-addr:** VRRP virtual IP address<br>**vrrp-mac-addr:** VRRP virtual MAC address<br>**mac-intf:** interface id on which VRRP virtual MAC address is based. | Error | |
| | **Event description:** Failed when adding a virtual MAC into switch L3 table. The box where the MAC is learned from is invalid.<br>**Log Message:** Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table. Box id <mac-box> is invalid<br>**Parameters description:**<br>**vrrp-ip-addr:** VRRP virtual IP address<br>**vrrp-mac-addr:** VRRP virtual MAC address<br>**mac-box:** stacking box number of VRRP virtual MAC. | Error | |
| | **Event description:** Failed when adding a virtual MAC into switch chip's L3 table.<br>**Log Message:** Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into chip L3 table. Errcode <vrrp-errcode><br>**Parameters description:**<br>**vrrp-ip-addr:** VRRP virtual IP address<br>**vrrp-mac-addr:** VRRP virtual MAC address<br>**vrrp-errcode:** Err code of VRRP protocol behavior. | Error | |
| | **Event description:** Failed when deleting a virtual MAC from switch chip's L3 table.<br>**Log Message:** Failed to delete virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> from chip L3 table. Errcode <vrrp-errcode><br>**Parameters description:**<br>**vrrp-ip-addr:** VRRP virtual IP address<br>**vrrp-mac-addr:** VRRP virtual MAC address<br>**vrrp-errcode:** Err code of VRRP protocol behavior. | Error | |
| **Web (SSL)** | **Event description:** Successful login through Web.<br>**Log Message:** Successful login through Web (Username: <username>, IP: <ipaddr>).<br>**Parameters description:**<br>**username:** The use name that used to login HTTP server.<br>**ipaddr:** The IP address of HTTP client. | Informational | |
| | **Event description:** Login failed through Web. | Warning | |

| | | | |
|---|---|---|---|
| | **Log Message:** Login failed through Web (Username: <username>, IP: <ipaddr>).<br>**Parameters description:**<br>**username:** The use name that used to login HTTP server.<br>**ipaddr:** The IP address of HTTP client. | | |
| | **Event description:** Web session timed out.<br>**Log Message:** Web session timed out (Username: <username>, IP: <ipaddr>).<br>**Parameters description:**<br>**username:** The use name that used to login HTTP server.<br>**ipaddr:** The IP address of HTTP client. | Informational | |
| | **Event description:** Logout through Web.<br>**Log Message:** Logout through Web (Username: <username>, IP: <ipaddr>".).<br>**Parameters description:**<br>**username:** The use name that used to login HTTP server.<br>**ipaddr:** The IP address of HTTP client. | Informational | |
| | **Event description:** Successful login through Web(SSL).<br>**Log Message:** Successful login through Web(SSL) (Username: <username>, IP: <ipaddr>).<br>**Parameters description:**<br>**username:** The use name that used to login SSL server.<br>**ipaddr:** The IP address of SSL client. | Informational | |
| | **Event description:** Login failed through Web(SSL).<br>**Log Message:** Login failed through Web(SSL) (Username: <username>, IP: <ipaddr>).<br>**Parameters description:**<br>**username:** The use name that used to login SSL server.<br>**ipaddr:** The IP address of SSL client. | Warning | |
| | **Event description:** Web(SSL) session timed out.<br>**Log Message:** Web(SSL) session timed out (Username: <username>, IP: <ipaddr>).<br>**Parameters description:**<br>**username:** The use name that used to login SSL server.<br>**ipaddr:** The IP address of SSL client. | Information | |
| | **Event description:** Logout through Web(SSL).<br>**Log Message:** Logout through Web(SSL) (Username: <username>, IP: <ipaddr>). | Information | |

| | | | |
|---|---|---|---|
| | **Parameters description:**<br>**username:** The use name that used to login SSL server.<br>**ipaddr:** The IP address of SSL client. | | |
| **Port Security** | **Event description:** Address full on a port<br>**Log Message:** Port security violation<br>(MAC: < macaddr > on port:: < unitID: portNum >)<br>**Parameters description:**<br>**macaddr:** The violation MAC address.<br>**unitID:** The unit ID.<br>**portNum:** The port number. | Warning | |
| **Safeguard** | **Event description:** The host enters the mode of normal.<br>**Log Message:** Unit< unitID >, Safeguard Engine enters NORMAL mode<br>**Parameters description:**<br>**unitID:** The unit ID. | Informational | |
| | **Event description:** The host enters the mode of exhausted.<br>**Log Message:** Unit< unitID >, Safeguard Engine enters EXHAUSTED mode<br>**Parameters description:**<br>**unitID:** The unit ID. | Warning | |
| **DoS** | **Event description:** The DOS is possibly spoofed.<br>**Log Message:** Possible spoofing attack from IP: <ipaddr>, MAC: <macaddr>, port: <unitID: portNum><br>**Parameters description:**<br>**Ipaddr:** The ip address<br>**macaddr:** The violation MAC address.<br>**unitID:** The unit ID.<br>**portNum:** The port number. | Critical | |
| **AAA** | **Event description**: Successful login.<br>**Log Message**: Successful login through <Console \| Telnet \| Web(SSL) \| SSH>(Username: <username>, IP: <ipaddr \| ipv6address>).<br>**Parameters description**:<br>**ipaddr**: IP address.<br>**username**: user name.<br>**ipv6address**: IPv6 address. | Informational | |
| | **Event description**: Login failed.<br>**Log Message**: Login failed through <Console \| Telnet \| Web(SSL)\| SSH> (Username: <username>, IP: <ipaddr \| ipv6address>). | Warning | |

| | | | |
|---|---|---|---|
| | **Parameters description**:<br>**ipaddr**: IP address.<br>**username**: user name.<br>**ipv6address**: IPv6 address. | | |
| | **Event description**: Logout.<br>**Log Message**: Logout through <Console \| Telnet \| Web(SSL)\| SSH> (Username: <username>, IP: <ipaddr \| ipv6address>).<br>**Parameters description**:<br>**ipaddr**: IP address.<br>**username**: user name.<br>**ipv6address**: IPv6 address. | Informational | |
| | **Event description**: session timed out.<br>**Log Message**: <Console \| Telnet \| Web(SSL)\| SSH> session timed out (Username: <username>, IP: <ipaddr \| ipv6address>).<br>**Parameters description**:<br>**ipaddr**: IP address.<br>**username**: user name.<br>**ipv6address**: IPv6 address. | Informational | |
| | **Event description**: SSH server is enabled.<br>**Log Message**: SSH server is enabled | Informational | |
| | **Event description**: SSH server is disabled.<br>**Log Message**: SSH server is disabled | Informational | |
| | **Event description**: Authentication Policy is enabled.<br>**Log Message**: Authentication Policy is enabled (Module: AAA). | Informational | |
| | **Event description**: Authentication Policy is disabled.<br>**Log Message**: Authentication Policy is disabled (Module: AAA). | Informational | |
| | **Event description**: Login failed due to AAA server timeout or improper configuration.<br>**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>).<br>**Parameters description**:<br>**ipaddr**: IP address.<br>**ipv6address**: IPv6 address.<br>**username**: user name. | Warning | |
| | **Event description**: Successful Enable Admin authenticated by AAA local or none or server.<br>**Log Message**: Successful Enable Admin through <Console \| Telnet \| Web(SSL)\| SSH> from <ipaddr \| ipv6address> authenticated by AAA <local \| none \| server <ipaddr \| ipv6address>> (Username: <username>). | Informational | |

| | | | |
|---|---|---|---|
| | **Parameters description**:<br>**local**: enable admin by AAA local method.<br>**none**: enable admin by AAA none method.<br>**server**: enable admin by AAA server method.<br>**ipaddr**: IP address.<br>**ipv6address**: IPv6 address.<br>**username**: user name. | | |
| | **Event description**: Enable Admin failed due to AAA server timeout or improper configuration.<br>**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>)<br>**Parameters description**:<br>**ipaddr**: IP address.<br>**ipv6address**: IPv6 address.<br>**username**: user name. | Warning | |
| | **Event description**: Enable Admin failed authenticated by AAA local or server.<br>**Log Message**: Enable Admin failed through <Console \| Telnet \| Web(SSL)\| SSH> from <ipaddr \| ipv6address> authenticated by AAA < local \| server <ipaddr \| ipv6address>> (Username: <username>).<br>**Parameters description**:<br>**local**: enable admin by AAA local method.<br>**server**: enable admin by AAA server method.<br>**ipaddr:** IP address.<br>**ipv6address:** IPv6 address.<br>**username:** user name. | Warning | |
| | **Event description**: Successful login authenticated by AAA local or none or server.<br>**Log Message**: Successful login through <Console \| Telnet \| Web(SSL) \| SSH> from < ipaddr \| ipv6address > authenticated by AAA <local \| none \| server <ipaddr \| ipv6address>> (Username: <username>).<br>**Parameters description**:<br>**local**: specify AAA local method.<br>**none**: specify none method.<br>**server**: specify AAA server method.<br>**ipaddr**: IP address.<br>**ipv6address**: IPv6 address.<br>**username**: user name. | Informational | |
| | **Event description**: Login failed authenticated by AAA local or server.<br>**Log Message**: Login failed through <Console \| Telnet \| Web(SSL)\| | Warning | |

| | | | |
|---|---|---|---|
| | SSH> from <ipaddr \| ipv6address> authenticated by AAA <local \| server <ipaddr \| ipv6address>> (Username: <username>).<br>**Parameters description**:<br>**local**: specify AAA local method.<br>**server**: specify AAA server method.<br>**ipaddr**: IP address.<br>**ipv6address**: IPv6 address.<br>**username**: user name. | | |
| **WAC** | **Event description:** When a client host fails to authenticate.<br>**Log Message**: WAC unauthenticated user (User Name: <string>, IP: <ipaddr \| ipv6address>, MAC: <macaddr>, Port: <[unitID:]portNum>)<br>**Parameters description:**<br>**string**: User name<br>**ipaddr**: IP address<br>**ipv6address**: IPv6 address<br>**macaddr**: MAC address<br>**unitID**: The unit ID<br>**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.<br>**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).<br>**Log Message**: WAC recovered from stop learning state. | Warning | |
| | **Event description:** When a client host authenticated successful.<br>**Log Message:** WAC authenticated user (Username: <string>, IP: <ipaddr \| ipv6address>, MAC: <macaddr>, Port: <[unitID:] portNum>)<br>**Parameters description:**<br>**string**: User name<br>**ipaddr**: IP address<br>**ipv6address**: IPv6 address<br>**macaddr**: MAC address<br>**unitID**: The unit ID<br>**portNum** : The port number | Informational | |
| **JWAC** | **Event description:** When a client host authenticated successful.<br>**Log Message:** JWAC authenticated user (Username: <string>, IP: <ipaddr>, MAC: <macaddr>, Port: <[unitID:]portNum>) | Informational | |

| | | | |
|---|---|---|---|
| | **Parameters description:**<br>**string**: Username<br>**ipaddr**: IP address<br>**macaddr**: MAC address<br>**unitID**: The unit ID<br>**portNum** : The port number | | |
| | **Event description:** When a client host fails to authenticate.<br>**Log Message:** JWAC unauthenticated user (User Name: <string>, IP: <ipaddr>, MAC: <macaddr>, Port: <[unitID:]portNum>)<br>**Parameters description:**<br>**string**: User name<br>**ipaddr**: IP address<br>**macaddr**: MAC address<br>**unitID**: The unit ID<br>**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.<br>**Log Message:** JWAC 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 the whole device in a time interval (5 min).<br>**Log Message:** JWAC recovered from stop learning state. | Warning | |
| **LBD** | **Event Description**: Loop back is detected under port-based mode.<br>**Log Message**:<br>Port < [unitID:] portNum> LBD loop occurred. Port blocked.<br>**Parameters Description:**<br>**portNum**: The port number. | Critical | |
| | **Event Description**: Port recovered from LBD blocked state under port-based mode.<br>**Log Message**:<br>Port < [unitID:] portNum>LBD port recovered. Loop detection restarted<br>**Parameters Description:**<br>**portNum**: The port number. | Informational | |
| | **Event Description**: Loop back is detected under VLAN-based mode.<br>**Log Message**:<br>Port < [unitID:] portNum> VID <vlanID> LBD loop occurred. Packet discard begun<br>**Parameters Description:**<br>**portNum**: The port number. | Critical | |

| | | | |
|---|---|---|---|
| | **vlanID**: the VLAN ID number. | | |
| | **Event Description**: Port recovered from LBD blocked state under VLAN-based mode.<br>**Log Message**:<br>Port < [unitID:] portNum> VID <vlanID> LBD recovered. Loop detection restarted<br>**Parameters Description:**<br>**portNum**: The port number.<br>**vlanID**: the VLAN ID number. | Informational | |
| | **Event Description**: The number of VLAN in which loop back occurs hit the specified number.<br>**Log Message**:<br>Loop VLAN number overflow.<br>**Parameters Description:**<br>None | Informational | |
| **IMPB** | **Event description:** Dynamic IMPB entry conflicts with static ARP.<br>**Log Message:** Dynamic IMPB entry conflicts with static ARP(IP: <ipaddr>, MAC: <macaddr>, Port <[unitID:]portNum>)<br>**Parameters description:**<br>**ipaddr:** IP address<br>**macaddr:** MAC address<br>**unitID:** The unit ID<br>**portNum :** The port number | Warning | |
| | **Event description:** Dynamic IMPB entry conflicts with static FDB.<br>**Log Message:** Dynamic IMPB entry conflicts with static FDB(IP: [<ipaddr> \| <ipv6addr>], MAC: <macaddr>, Port <[unitID:]portNum>)<br>**Parameters description:**<br>**ipaddr:** IP address<br>**ipv6addr:** IPv6 address<br>**macaddr:** MAC address<br>**unitID:** The unit ID<br>**portNum :** The port number | Warning | |
| | **Event description:** Dynamic IMPB entry conflicts with static IMPB.<br>**Log Message:** Dynamic IMPB entry conflicts with static IMPB(IP: [<ipaddr> \| <ipv6addr>], MAC: <macaddr>, Port <[unitID:]portNum>).<br>**Parameters description:**<br>**ipaddr:** IP address<br>**ipv6addr:** IPv6 address<br>**macaddr:** MAC address | Warning | |

| | | | |
|---|---|---|---|
| | **unitID:** The unit ID<br>**portNum :** The port number | | |
| | **Event description:** Creating IMPB entry failed due to no ACL rule being available.<br>**Log Message:** Creating IMPB entry failed due to no ACL rule being available(IP:[<ipaddr> \| <ipv6addr>], MAC: <macaddr>, Port <[unitID:]portNum>)<br>**Parameters description:**<br>**ipaddr:** IP address<br>**ipv6addr:** IPv6 address<br>**macaddr:** MAC address<br>**unitID:** The unit ID<br>**portNum :** The port number | Warning | |
| | **Event description:** IMPB checks a host illegal.<br>**Log Message:** Unauthenticated IP-MAC address and discarded by IMPB (IP: [< ipaddr > \| < ipv6addr >], MAC :< macaddr >, Port <[unitID:]portNum >).<br>**Parameters description:**<br>**ipaddr:** IP address<br>**ipv6addr:** IPv6 address<br>**macaddr:** MAC address<br>**unitID:** The unit ID<br>**portNum :** The port number | Warning | |
| | **Event description:** Dynamic IMPB entry conflicts with static ND<br>**Log Message:** Dynamic IMPB entry conflicts with static ND (IP: [< ipaddr > \| < ipv6addr >], MAC: <macaddr>, Port <[unitID:]portNum>)<br>**Parameters description:**<br>**ipaddr:** IP address<br>**ipv6addr:** IPv6 address<br>**macaddr:** MAC address<br>**unitID:** The unit ID<br>**portNum :** The port number | Warning | |
| **Traffic Control** | **Event description:** Broadcast storm occurrence.<br>**Log Message:** Port <portNum> Broadcast storm is occurring.<br>**Parameters description:**<br>**portNum:** The port number. | Warning | |
| | **Event description:** Broadcast storm cleared.<br>**Log Message:** Port <portNum> Broadcast storm has cleared. | Informational | |

| | | | |
|---|---|---|---|
| | **Parameters description:**<br>**portNum:** The port number. | | |
| | **Event description:** Multicast storm occurrence.<br>**Log Message:** Port <portNum> Multicast storm is occurring.<br>**Parameters description:**<br>**portNum:** The port number. | Warning | |
| | **Event description:** Multicast Storm cleared.<br>**Log Message:** Port <portNum>Multicast storm has cleared.<br>**Parameters description:**<br>**portNum:** The port number. | Informational | |
| | **Event description:** Port shut down due to a packet storm<br>**Log Message:** Port <portNum> is currently shut down due to a packet storm<br>**Parameters description:**<br>**portNum:** The port number. | Warning | |
| **DHCP Server Screening Function** | **Event description:** Detected untrusted DHCP server IP address.<br>**Log Message:** Detected untrusted DHCP server(IP: <ipaddr>, Port <portNum> )<br>**Parameters description:**<br>**ipaddr:** The untrusted IP address which has beenis detected with our device.<br>**portNum :** Represent the logic port number of the device. | Informational | |
| **ERPS** | **Event description:** Signal failure detected<br>**Log Message:** Signal failure detected on node (MAC: <macaddr>)<br>**Parameters description:**<br>**macaddr:** The system MAC address of the node | Notice | |
| | **Event description:** Signal failure cleared<br>**Log Message:** Signal failure cleared on node (MAC: <macaddr>)<br>**Parameters description:**<br>**macaddr:** The system MAC address of the node | Notice | |
| | **Event description:** RPL owner conflict<br>**Log Message:** RPL owner conflicted on the ring (MAC: <macaddr>)<br>**Parameters description:**<br>**macaddr:** The system MAC address of the node | Warning | |
| **MSTP Debug Enhancement** | **Event description:** Topology changed.<br>**Log Message:** Topology changed<br>[( [Instance:<InstanceID> ] ,port:<[unitID:] portNum> ,MAC: | Notice | |

| | | | |
|---|---|---|---|
| | <macaddr>)]<br>**Parameters description:**<br>**InstanceID:** Instance ID.<br>**portNum:**Port ID<br>**macaddr:** MAC address | | |
| | **Event description:** Spanning Tree new Root Bridge<br>**Log Message:** [CIST \| CIST Regional \| MSTI Regional]  New Root bridge selected( [Instance: <InstanceID> ]MAC: <macaddr> Priority :<value>)<br>**Parameters description:**<br>**InstanceID:** Instance ID.<br>**macaddr:** Mac address<br>**value:** priority value | Informational | |
| | **Event description:** Spanning Tree Protocol is enabled<br>**Log Message:** Spanning Tree Protocol is enabled | Informational | |
| | **Event description:** Spanning Tree Protocol is disabled<br>**Log Message:** Spanning Tree Protocol is disabled | Informational | |
| | **Event description:**  New root port<br>**Log Message:** New root port selected [( [Instance:<InstanceID> ], port:<[unitID:] portNum>)]<br>**Parameters description:**<br>**InstanceID:** Instance ID.<br>**portNum:**Port ID | Notice | |
| | **Event description:** Spanning Tree port status changed<br>**Log Message:** Spanning Tree port status changed [( [Instance:<InstanceID> ], port:<[unitID:] portNum>)] <old_status> -> <new_status><br>**Parameters description:**<br>**InstanceID:** Instance ID.<br>**portNum:** Port ID<br>**old_status:** Old status<br>**new_status:** New status | Notice | |
| | **Event description:** Spanning Tree port role changed.<br>**Log Message:** Spanning Tree port status changed. [( [Instance:<InstanceID> ], port:<[unitID:] portNum>)] <old_role> -> <new_role><br>**Parameters description:**<br>**InstanceID:** Instance ID.<br>**portNum:**Port ID/<br>**old_role:** Old role | Informational | |

| | | | |
|---|---|---|---|
| | **new_status:**New role | | |
| | **Event description:** Spannnig Tree instance created.<br>**Log Message:** Spanning Tree instance created. Instance:<InstanceID><br>**Parameters description:**<br>**InstanceID:** Instance ID. | Informational | |
| | **Event description:** Spannnig Tree instance deleted.<br>**Log Message:** Spanning Tree instance deleted. Instance:<InstanceID><br>**Parameters description:**<br>**InstanceID:** Instance ID. | Informational | |
| | **Event description:** Spanning Tree Version changed.<br>**Log Message:** Spanning Tree version changed. New version:<new_version><br>**Parameters description:**<br>**new_version:** New STP version. | Informational | |
| | **Event description:** Spanning Tree MST configuration ID name and revision level changed.<br>**Log Message:** Spanning Tree MST configuration ID name and revision level changed (name:<name> ,revision level <revision_level>).<br>**Parameters description:**<br>**name :** New name.<br>**revision_level:**New revision level. | Informational | |
| | **Event description:** Spanning Tree MST configuration ID VLAN mapping table deleted.<br>**Log Message:** Spanning Tree MST configuration ID VLAN mapping table changed (instance: <InstanceID> delete vlan <startvlanid> [- <endvlanid>]).<br>**Parameters description:**<br>**InstanceID:** Instance ID.<br>**startvlanid- endvlanid**:VLANlist | Informational | |
| | **Event description:** Spanning Tree MST configuration ID VLAN mapping table added.<br>**Log Message:** Spanning Tree MST configuration ID VLAN mapping table changed (instance: <InstanceID> add vlan <startvlanid> [- <endvlanid>]).<br>**Parameters description:**<br>**InstanceID:** Instance ID.<br>**startvlanid- endvlanid**:VLANlist | Informational | |

| | | | |
|---|---|---|---|
| **CFM** | **Event description:** Cross-connect is detected<br>**Log Message:** CFM cross-connect. VLAN:<vlanid>, Local(MD Level:<mdlevel>, Port <[unitID:]portNum>, Direction:<mepdirection>) Remote(MEPID:<mepid>, MAC:<macaddr>)<br>**Parameters description:**<br>**vlanid:** Represents the VLAN identifier of the MEP.<br>**mdlevel:** Represents the MD level of the MEP.<br>**unitID:** Represents the ID of the device in the stacking system.<br>**portNum:** Represents the logical port number of the MEP.<br>**mepdirection:** Can be "inward" or "outward".<br>**mepid:** Represents the MEPID of the MEP. The value 0 means unknown MEPID.<br>**macaddr:** Represents the MAC address of the MEP. The value all zeros mean unknown MAC address.<br>Note: In CFM hardware mode, remote MEP information (mepid and macaddr) is unknown. | Critical | |
| | **Event description:** Error CFM CCM packet is detected<br>**Log Message:** CFM error ccm. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <[unitID:]portNum>, Direction:<mepdirection>) Remote(MEPID:<mepid>, MAC:<macaddr>)<br>**Parameters description:**<br>**vlanid:** Represents the VLAN identifier of the MEP.<br>**mdlevel:** Represents MD level of the MEP.<br>**unitID:** Represents the ID of the device in the stacking system.<br>**portNum:** Represents the logical port number of the MEP.<br>**mepdirection:** Can be "inward" or "outward".<br>**mepid:** Represents the MEPID of the MEP. The value 0 means unknown MEPID.<br>**macaddr:** Represents the MAC address of the MEP. The value all zeros means unknown MAC address.<br>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<br>**Log Message:** CFM remote down. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <[unitID:]portNum>, Direction:<mepdirection>)<br>**Parameters description:**<br>**vlanid:** Represents the VLAN identifier of the MEP.<br>**mdlevel:** Represents the MD level of the MEP. | Warning | |

| | | | |
|---|---|---|---|
| | **unitID:** Represents the ID of the device in the stacking system.<br>**portNum:** Represents the logical port number of the MEP.<br>**mepdirection:** Represents the MEP direction, which can be "inward" or "outward". | | |
| | **Event description:** Remote MEP's MAC reports an error status<br>**Log Message:** CFM remote MAC error. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <[unitID:]portNum>, Direction:<mepdirection>)<br>**Parameters description:**<br>**vlanid:** Represents the VLAN identifier of the MEP.<br>**mdlevel:** Represents the MD level of the MEP.<br>**unitID:** Represents the ID of the device in the stacking system.<br>**portNum:** Represents the logical port number of the MEP.<br>**mepdirection:** Represents the MEP direction, which can be "inward" or "outward". | Warning | |
| | **Event description:** Remote MEP detects CFM defects<br>**Log Message:** CFM remote detects a defect. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <[unitID:]portNum>, Direction:<mepdirection>)<br>**Parameters description:**<br>**vlanid:** Represents the VLAN identifier of the MEP.<br>**mdlevel:** Represents the MD level of the MEP.<br>**unitID:** Represents the ID of the device in the stacking system.<br>**portNum:** Represents the logical port number of the MEP.<br>**mepdirection:** Represents the MEP direction, which can be "inward" or "outward". | Informational | |
| **CFM Extension** | **Event description:** AIS condition detected<br>**Log Message:** AIS condition detected. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <[unitID:]portNum>, Direction:<mepdirection>, MEPID:<mepid>)<br>**Parameters description:**<br>**vlanid:** Represents the VLAN identifier of the MEP.<br>**mdlevel:** Represents the MD level of the MEP.<br>**unitID:** Represents the ID of the device in the stacking system.<br>**portNum:** Represents the logical port number of the MEP.<br>**mepdirection:** Represents the direction of the MEP. This can be "inward" or "outward".<br>**mepid:** Represents the MEPID of the MEP. | Notice | |
| | **Event description:** AIS condition cleared<br>**Log Message:** AIS condition cleared. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <[unitID:]portNum>, Direction:<mepdirection>, MEPID:<mepid>) | Notice | |

| | | | |
|---|---|---|---|
| | **Parameters description:**<br>**vlanid:** Represents the VLAN identifier of the MEP.<br>**mdlevel:** Represents the MD level of the MEP.<br>**unitID:** Represents the ID of the device in the stacking system.<br>**portNum:** Represents the logical port number of the MEP.<br>**mepdirection:** Represents the direction of the MEP. This can be "inward" or "outward".<br>**mepid:** Represents the MEPID of the MEP. | | |
| | **Event description:** LCK condition detected<br>**Log Message:** LCK condition detected. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <[unitID:]portNum>, Direction:<mepdirection>, MEPID:<mepid>)<br>**Parameters description:**<br>**vlanid:** Represents the VLAN identifier of the MEP.<br>**mdlevel:** Represents the MD level of the MEP.<br>**unitID:** Represents the ID of the device in the stacking system.<br>**portNum:** Represents the logical port number of the MEP.<br>**mepdirection:** Represents the direction of the MEP. This can be "inward" or "outward".<br>**mepid:** Represents the MEPID of the MEP. | Notice | |
| | **Event description:** LCK condition cleared<br>**Log Message:** LCK condition cleared. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <[unitID:]portNum>, Direction:<mepdirection>, MEPID:<mepid>)<br>**Parameters description:**<br>**vlanid:** Represents the VLAN identifier of the MEP.<br>**mdlevel:** Represents the MD level of the MEP.<br>**unitID:** Represents the ID of the device in the stacking system.<br>**portNum:** Represents the logical port number of the MEP.<br>**mepdirection:** Represents the direction of the MEP. This can be "inward" or "outward".<br>**mepid:** Represents the MEPID of the MEP. | Notice | |
| **Port** | **Event description:** port linkup<br>**Log Message:** Port <port> link up, <nway><br>**Parameters description:**<br>**port:** Represents the logical port number.<br>**nway:** Represents the speed and duplex of link. | Informational | |
| | **Event description:** port linkdown<br>**Log Message:** Port <port> link down<br>**Parameters description:** | Informational | |

| | | | |
|---|---|---|---|
| | **port:** Represents the logical port number. | | |
| **BPDU Attack Protection** | **Event description:** BPDU attack happened.<br>**Log Message:** Port<[unitID:]portNum> enter BPDU under protection state (mode: drop / block / shutdown)<br>**Parameters description:**<br>**unitID:** The unit ID.<br>**portNum:** The port number.<br>**mode:**The BPDU currnt state | Informational | |
| | **Event description:** BPDU attack automatically recover.<br>**Log Message:** Port <[unitID:]portNum> recover from BPDU under protection state automatically<br>**Parameters description:**<br>**unitID:** The unit ID.<br>**portNum:** The port number. | Informational | |
| | **Event description:** BPDU attack manually recover.<br>**Log Message:** Port<[unitID:]portNum> recover from BPDU under protection state automatically<br>**Parameters description:**<br>**unitID:** The unit ID.<br>**portNum:** The port number. | Informational | |
| **External Alarm** | **Event description:** External alarm occurred<br>**Log Message:** [Unit <unitID>] External Alarm Channel <channel_id> : <alarm_message><br>**Parameters description:**<br>**unitID:** The unit ID.<br>**channel_id:** Represent the channel ID detected the external alarm<br>**alarm_message:** Alarm message when alarm occurred, this is configurable by user. | Critical | |
| **RIPng** | **Event description:** The RIPng state of interface changed<br>**Log Message:** RIPng protocol on interface <intf-name> changed state to <enabled \| disabled><br>**Parameters description:**<br>**intf-name:** Interface name. | Informational | |
| **DLMS** | **Event Description**:<br>Input an illegal activation code.<br>**Log Message**: | Informational | |

| | | | |
|---|---|---|---|
| | Illegal activation code (AC: <string25>).<br>**Parameters Description**:<br><string25>: Activation Code | | |
| | **Event Description**:<br>License Expired.<br>**Log Message**:<br>License expired (license:<license-model>, AC: <string25>).<br>**Parameters Description**:<br><license-model>: License Model Name.<br><string25>: Activation Code | Critical | |
| | **Event Description**:<br>License successfully installed.<br>**Log Message**:<br>License successfully installed (license:<license-model>, AC: <string25>).<br>**Parameters Description**:<br><license-model>: License Model Name.<br><string25>: Activation Code | Informational | |
| | **Event Description**:<br>The Activation Code is unbound.<br>**Log Message**:<br>Unbound Activation Code (AC: <string25>).<br>**Parameters Description**:<br><string25>: Activation Code | Critical | |
| | **Event Description**:<br>When a license is going to expire, it will be logged before 30 days.<br>**Log Message**:<br>License will expire in 30 days. (license:<license-model>, AC: <string25>)<br>.<br>**Parameters Description**:<br><license-model>: License Model Name.<br><string25>: Activation Code | Informational | |

# Appendix C Trap 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<br>Binding objects:<br>(1)swL2macNotifyInfo | 1.3.6.1.4.1.171.11.118.X.2.100.1.2.0.1<br>(X:module ID) |
| ***MAC-based Access Control*** | swMacBasedAccessControlLoggedSuccess | The trap is sent when a MAC-based Access Control host is successfully logged in.<br>Binding objects：<br>(1) swMacBasedAuthInfoMacIndex<br>(2) swMacBasedAuthInfoPortIndex<br>(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.<br>Binding objects：<br>(1) swMacBasedAuthInfoMacIndex<br>(2) swMacBasedAuthInfoPortIndex<br>(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.<br>Binding objects：<br>(1) swMacBasedAuthInfoMacIndex<br>(2) swMacBasedAuthInfoPortIndex<br>(3) swMacBasedAuthVID | 1.3.6.1.4.1.171.12.35.11.1.0.3 |
| ***PIM6*** | pimNeighborLoss | A pimNeighborLoss notification signifies the loss of an adjacency with a neighbor. This notification should be generated when the neighbor timer expires, and the router has no other neighbor on the same interface with the same IP version and a lower IP address than itself.<br>This notification is generated whenever the counter pimNeighborLossCount is incremented, subject to the rate limit specified by pimNieghborLossNotificationsPeriod.<br>Binding objects:<br>(1) pimNeighborUpTime | 1.3.6.1.2.1.157.0.1 |

| | | | |
|---|---|---|---|
| | pimInvalidRegister | A pimInvalidRegister notification signifies that an invalid PIM Register message was received by this device.<br>This notification is generated whenever the counter pimInvalidRegisterMsgsRcvd is incremented, subject to the rate limit specified by pimInvalidRegisterNotificationPeriod.<br>Binding objects:<br>(1) pimGroupMappingPimMode<br>(2) pimInvalidRegisterAddressType<br>(3) pimInvalidRegisterOrigin<br>(4) pimInvalidRegisterGroup<br>(5) pimInvalidRegisterRp | 1.3.6.1.2.1.157.0.2 |
| | pimInvalidJoinPrune | A pimInvalidJoinPrune notification signifies that an invalid PIM Join/Prune message was received by this device.<br>This notification is generated whenever the counter pimInvalidJoinPruneMsgsRcvd is incremented, subject to the rate limit specified by pimInvalidJoinPruneNotificationPeriod.<br>Binding objects:<br>(1) pimGroupMappingPimMode<br>(2) pimInvalidJoinPruneAddressType<br>(3) pimInvalidJoinPruneOrigin<br>(4) pimInvalidJoinPruneGroup<br>(5) pimInvalidJoinPruneRp<br>(6) pimNeighborUpTime | 1.3.6.1.2.1.157.0.3 |
| | pimRPMappingChage | A pimRPMappingChange notification signifies a change to the active RP mapping on this device.<br>This notification is generated whenever the counter pimRPMappingChangeCount is incremented, subject to the rate limit specified by pimRPMappingChangeNotificationPeriod.<br>Binding objects:<br>(1) pimGroupMappingPimMode<br>(2) pimGroupMappingPrecedence | 1.3.6.1.2.1.157.0.4 |
| | pimInterfaceElection | A pimInterfaceElection notification | 1.3.6.1.2.1.157.0.5 |

| | | | |
|---|---|---|---|
| | | signifies that a new DR or DF has been elected on a network.<br>This notification is generated whenever the counter pimInterfaceElectionWinCount is incremented, subject to the rate limit specified by pimInterfaceElectionNotificationPeriod .<br>Binding objects:<br>(1) pimInterfaceAddressType<br>(2) pimInterfaceAddress | |
| ***LLDP*** | lldpRemTablesChange | A lldpRemTablesChange notification is sent when<br>the value of lldpStatsRemTableLastChangeTime<br>changes.<br>Binding objects：<br>(1) lldpStatsRemTablesInserts<br>(2) lldpStatsRemTablesDeletes<br>(3) lldpStatsRemTablesDrops<br>(4) lldpStatsRemTablesAgeouts | 1.0.8802.1.1.2.0.0.1 |
| ***LLDP-MED*** | lldpXMedTopologyCha<br>ngeDetected | A notification generated by the local device sensing<br>a change in the topology that indicates that a new<br>remote device attached to a local port, or a remote<br>device disconnected or moved from one port to<br>another.<br>Binding objects：<br>(1) lldpRemChassisIdSubtype<br>(2) lldpRemChassisId<br>(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.<br>**Binding objects:**<br>(1) dot3OamEventLogTimestamp<br>(2) dot3OamEventLogOui<br>(3)dot3OamEventLogType<br>(4)dot3OamEventLogLocation<br>(5)dot3OamEventLogWindowHi | 1.3.6.1.2.1.158.0.1 |

| | | | |
|---|---|---|---|
| | | (6)dot3OamEventLogWindowLo<br>(7)dot3OamEventLogThresholdHi<br>(8)dot3OamEventLogThresholdLo<br>(9)dot3OamEventLogValue<br>(10)dot3OamEventLogRunningTotal<br>(11)dot3OamEventLogEventTotal | |
| | dot3OamNonThresholdEvent | This notification is sent when a local or remote non-threshold crossing event is detected.<br>Binding objects:<br>(1) dot3OamEventLogTimestamp<br>(2) dot3OamEventLogOui<br>(3) dot3OamEventLogType<br>(4)dot3OamEventLogLocation<br>(5)dot3OamEventLogEventTotal | 1.3.6.1.2.1.158.0.2 |
| ***Up/Download*** | agentFirmwareUpgrade | This trap is sent when the process of upgrading the firmware via SNMP has finished.<br>**Binding objects：**<br>(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<br>**Binding objects：**<br>(1) unitID<br>(2) agentCfgOperate<br>(3) 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.<br>**Binding objects：**<br>(1) ipaddr<br>(2) macaddr<br>(3) portNumber<br>(4) agentGratuitousARPInterfaceName | 1.3.6.1.4.1.171.12.1.7.2.0.5 |
| ***BGP*** | bgpEstablishedNotification | The BGP established event is generated when the BGP FSM enters the ESTABLISHED state.<br>**Binding objects:**<br>(1) bgpPeerRemoteAddr<br>(2) bgpPeerLastError<br>(3) bgpPeerState | 1.3.6.1.2.1.15.0.1 |
| | bgpBackwardTransNotification | The BGP established event is generated | 1.3.6.1.2.1.15.0.2 |

| | | | |
|---|---|---|---|
| | | when the BGP FSM enters the ESTABLISHED state.<br>**Binding objects:**<br>(1) bgpPeerRemoteAddr<br>(2) bgpPeerLastError<br>(3) bgpPeerState | |
| ***Stacking*** | swUnitInsert | Unit Hot Insert notification.<br>**Binding objects:**<br>(1) swUnitMgmtId.<br>(2) swUnitMgmtMacAddr. | 1.3.6.1.4.1.171.12.11.2.2.1.0.1 |
| | swUnitRemove | Unit Hot Remove notification.<br>**Binding objects:**<br>(1) swUnitMgmtId.<br>(2) swUnitMgmtMacAddr. | 1.3.6.1.4.1.171.12.11.2.2.1.0.2 |
| | swUnitFailure | Unit Failure notification.<br>**Binding objects:**<br>(1) swUnitMgmtId. | 1.3.6.1.4.1.171.12.11.2.2.1.0.3 |
| | swUnitTPChange | The stacking topology change notification.<br>**Binding objects:**<br>(1) swStackTopologyType<br>(2) swUnitMgmtId<br>(3) swUnitMgmtMacAddr | 1.3.6.1.4.1.171.12.11.2.2.1.0.4 |
| | swUnitRoleChange | The stacking unit role change notification.<br>**Binding objects:**<br>(1) swStackRoleType<br>(2) swUnitMgmtId | 1.3.6.1.4.1.171.12.11.2.2.1.0.5 |
| ***VRRP*** | vrrpTrapNewMaster | The newMaster trap indicates that the sending agent has transitioned to 'Master' state.<br>Binding objects:<br>(1) vrrpOperMasterIpAddr | 1.3.6.1.2.1.68.0.1 |
| | vrrpTrapAuthFailure | A vrrpAuthFailure trap signifies that a packet has been received from a router | 1.3.6.1.2.1.68.0.2 |

| | | | |
|---|---|---|---|
| | | whose authentication key or authentication type conflicts with this router's authentication key or authentication type. Implementation of this trap is optional.<br>Binding objects:<br>(1) vrrpTrapPacketSrc<br>(2) vrrpTrapAuthErrorType | |
| ***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.<br>**Binding objects：**<br>(1)swPortSecPortIndex<br>(2)swL2PortSecurityViolationMac | 1.3.6.1.4.1.171.11.118.X.2.100.1.2.0.2<br>(X: module ID) |
| ***Safe Guard*** | swSafeGuardChgToNormal | This trap indicates system change operation mode from axhausted to normal.<br>**Binding objects:**<br>(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.<br>**Binding objects:**<br>(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.<br>**Binding objects:**<br>(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.<br>**Binding objects:**<br>(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.<br>**Binding objects:**<br>(1) swLoopDetectPortIndex<br>(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.<br>**Binding objects:**<br>(1) swLoopDetectPortIndex<br>(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.<br>**Binding objects**：<br>(1) swIpMacBindingPortIndex<br>(2) swIpMacBindingViolationIP<br>(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.<br>**Binding objects**：<br>(1) swIpMacBindingPortIndex<br>(2) swIpMacBindingViolationIPv6Addr<br>(3) swIpMacBindingViolationMac | 1.3.6.1.4.1.171.12.23.5.0.4 |
| ***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.<br>**Binding objects:**<br>(1) swFilterDetectedIP<br>(2) swFilterDetectedport | 1.3.6.1.4.1.171.12.37.100.0.1 |
| ***Traffic Control*** | swPktStormOccurred | When packet storm is detected by packet storm mechanism and take shutdown as action.<br>**Binding objects**：<br>(1) swPktStormCtrlPortIndex | 1.3.6.1.4.1.171.12.25.5.0.1 |

| | | | |
|---|---|---|---|
| | swPktStormCleared | When the packet storm is clear.<br>**Binding objects：**<br>(1) swPktStormCtrlPortIndex | 1.3.6.1.4.1.171.12.25.5.0.2 |
| | swPktStormDisablePort | When the port is disabled by the packet storm mechanism.<br>**Binding objects：**<br>(1) swPktStormCtrlPortIndex | 1.3.6.1.4.1.171.12.25.5.0.3 |
| ***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.<br>**Binding objects：**<br>(1) dot1agCfmMdIndex<br>(2) dot1agCfmMaIndex<br>(3) dot1agCfmMepIdentifier | 1.3.111.2.802.1.1.8.0.1 |
| ***CFM Extension*** | swCFMExtAISOccurred | A notification is generated when local MEP enters AIS status.<br>**Binding objects：**<br>(1) dot1agCfmMdIndex<br>(2) dot1agCfmMaIndex<br>(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. | 1.3.6.1.4.1.171.12.86.100.0.2 |

| | | | |
|---|---|---|---|
| | | **Binding objects：**<br>(1) dot1agCfmMdIndex<br>(2) dot1agCfmMaIndex<br>(3) dot1agCfmMepIdentifier | |
| | swCFMExtLockOccurred | A notification is generated when local MEP enters lock status.<br>**Binding objects：**<br>(1) dot1agCfmMdIndex<br>(2) dot1agCfmMaIndex<br>(3) dot1agCfmMepIdentifier | 1.3.6.1.4.1.171.12.86.100.0.3 |
| | swCFMExtLockCleared | A notification is generated when local MEP exits lock status.<br>**Binding objects：**<br>(1) dot1agCfmMdIndex<br>(2) dot1agCfmMaIndex<br>(3) dot1agCfmMepIdentifier | 1.3.6.1.4.1.171.12.86.<br>100.0.4 |
| ***Port Trap*** | linkUp | A notification is generated when port linkup.<br>**Binding objects：**<br>(1) ifIndex,<br>(2) if AdminStatus<br>(3) ifOperStatu | 1.3.6.1.6.3.1.1.5.4 |
| | linkDown | A notification is generated when port linkdown.<br>**Binding objects：**<br>(1) ifIndex,<br>(2) if AdminStatus<br>(3) ifOperStatu | 1.3.6.1.6.3.1.1.5.3 |
| ***External Alarm*** | swExternalAlarm | When external alarm Occurred.<br>**Binding objects：**<br>(1) swExternalAlarmChannel<br>(2) swExternalAlarmMessage | 1.3.6.1.4.1.171.12.11.2.2.5.0.1 |
| | swExternalAlarmStacking | When external alarm Occurred. | 1.3.6.1.4.1.171.12.11.2.2.5.0.2 |

| | | | |
|---|---|---|---|
| | | **Binding objects：**<br>(1) swExternalAlarmStackingUnit<br>(2) swExternalAlarmStackingChannel<br>(3) swExternalAlarmStackingMessage | |
| ***SIM*** | swSingleIPMSColdStart | The commander switch will send this notification when its member generates a cold start notification.<br>**Binding objects:**<br>(1) swSingleIPMSID<br>(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.<br>**Binding objects:**<br>(1) swSingleIPMSID<br>(2) swSingleIPMSMacAddr | 1.3.6.1.4.1.171.12.8.6.0.12 |
| | swSingleIPMSLinkDown | The commander switch will send this notification when its member generates a link down notification.<br>**Binding objects:**<br>(1) swSingleIPMSID<br>(2) swSingleIPMSMacAddr<br>(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.<br>**Binding objects:**<br>(1) swSingleIPMSID<br>(2) swSingleIPMSMacAddr<br>(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.<br>**Binding objects:**<br>(1) swSingleIPMSID<br>(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.<br>**Binding objects:**<br>(1) swSingleIPMSID<br>(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. | 1.3.6.1.4.1.171.12.8.6.0.17 |

| | | | |
|---|---|---|---|
| | | **Binding objects:**<br>(1) swSingleIPMSID<br>(2) swSingleIPMSMacAddr | |
| | swSingleIPMSrisingAlarm | The commander switch will send this notification when its member generates a rising alarm notification.<br>**Binding objects:**<br>(1) swSingleIPMSID<br>(2) swSingleIPMSMacAddr | 1.3.6.1.4.1.171.12.8.6.0.18 |
| | swSingleIPMSfallingAlarm | The commander switch will send this notification when its member generates a falling alarm notification.<br>**Binding objects:**<br>(1) swSingleIPMSID<br>(2) swSingleIPMSMacAddr | 1.3.6.1.4.1.171.12.8.6.0.19 |
| | swSingleIPMSmacNotification | The commander switch will send this notification when its member generates a MAC address variation notification.<br>**Binding objects:**<br>(1) swSingleIPMSID<br>(2) swSingleIPMSMacAddr<br>(3) swSingleIPMSTrapMessage | 1.3.6.1.4.1.171.12.8.6.0.20 |
| | swSingleIPMSPortTypeChange | The commander switch will send this notification when its member generates a port type change notification.<br>**Binding objects:**<br>(1) swSingleIPMSID<br>(2) swSingleIPMSMacAddr<br>(3) ifIndex<br>(4) swSingleIPMSTrapMessage | 1.3.6.1.4.1.171.12.8.6.0.21 |
| | swSingleIPMSPowerStatusChg | The commander switch will send this notification when its member generates a power status change notification.<br>**Binding objects:**<br>(1) swSingleIPMSID<br>(2) swSingleIPMSMacAddr<br>(3) swSingleIPMSTrapMessage | 1.3.6.1.4.1.171.12.8.6.0.22 |
| | swSingleIPMSPowerFailure | The commander switch will send this notification when its member generates a power failure notification.<br>**Binding objects:**<br>(1) swSingleIPMSID<br>(2) swSingleIPMSMacAddr<br>(3) swSingleIPMSTrapMessage | 1.3.6.1.4.1.171.12.8.6.0.23 |
| | swSingleIPMSPowerRecover | The commander switch will send this notification when its member generates | 1.3.6.1.4.1.171.12.8.6.0.24 |

| | | | |
|---|---|---|---|
| | | a power recover notification.<br>**Binding objects:**<br>(1) swSingleIPMSID<br>(2) swSingleIPMSMacAddr<br>(3) swSingleIPMSTrapMessage | |
| ***DLMS*** | swDlmsIllegalAc | This Notification indicates the user inputs an illegal activation code.<br>Binding objects:<br>*swDlmsInstallAc | 1.3.6.1.4.1.171.12.101.0.1<br>This trap is used for both stackable and non-stackable device. |
| | swDlmsLicenseExpired | The notification is sent when a license of non-stackable device is expired.<br>Binding object:<br>*swDlmsLicenseModelName<br>*swDlmsLicenseAc | 1.3.6.1.4.1.171.12.101.0.2<br>This trap is used for non-stackable device. |
| | swDlmsLicenseInstallationSuccess | The notification is sent when a license of non-stackable device was installed successfully.<br>Binding object:<br>*swDlmsLicenseModelName<br>*swDlmsInstallAc | 1.3.6.1.4.1.171.12.101.0.3<br>This trap is used for non-stackable device. |
| | swDlmsLicenseExpiresIn30Days | When a license of non-stackable device is going to expire, the notification is sent before 30 days.<br>Binding object:<br>*swDlmsLicenseModelName<br>*swDlmsInstallAc | 1.3.6.1.4.1.171.12.101.0.4<br>This trap is used for non-stackable device. |
| | swDlmsStackLicenseExpired | The notification is sent when a license of devices stacked is expired.<br>Binding object:<br>*swDlmsStackLicenseModelUnitId<br>*swDlmsStackLicenseModelName<br>*swDlmsStackLicenseAc | 1.3.6.1.4.1.171.12.101.0.21<br>For stackable device |
| | swDlmsStackLicenseInstallationSuccess | The notification is sent when a license of devices stacked was installed successfully.<br>Binding object:<br>*swDlmsStackLicenseModelUnitId<br>*swDlmsStackLicenseModelName<br>*swDlmsInstallAc | 1.3.6.1.4.1.171.12.101.0.22<br>For stackable device |

| | | | |
|---|---|---|---|
| | swDlmsStackLicenseExpiresIn30Days | When a license of devices stacked is going to expire, the notification is sent before 30 days.<br>Binding object:<br>*swDlmsStackLicenseModelUnitId<br>*swDlmsStackLicenseModelName<br>*swDlmsInstallAc | 1.3.6.1.4.1.171.12.101.0.23<br>For stackable device |

# 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), Japanese Web-based Access Control, Web-based Access Control, 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)<br>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 |
|---|---|---|

| | | |
|---|---|---|
| 0x01 | VLAN name (ASCII) | A tag field of greater than 0x1F is interpreted as the first octet of the following field. |
| 0x02 | VLAN ID (ASCII) | |
| Others<br>(0x00, 0x03 ~ 0x1F, >0x1F) | 1. When the switch receives the VLAN setting string, it will think it is the VLAN ID first. In other words, the switch will check all existed VLAN ID and check if there is one matched.<br>2. If the switch can find one matched, it will move to that VLAN.<br>3. If the switch can not find the matched VLAN ID, it will think the VLAN setting string as a “VLAN Name”.<br>4. Then it will check that it can find out a matched VLAN Name. | |

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, or WAC/JWAC authentication is successful, the port will be assigned to VLAN 3. However if the user does not configure the VLAN attributes, when the port is not guest VLAN member, it will be kept in its current authentication VLAN, and when the port is guest VLAN member, it will be assigned to its original 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)<br>13 (for ACL rule) | Required |
| Attribute-Specific Field | Used to assign the ACL profile or rule. | ACL Command<br>For example:<br>ACL profile: *create access_profile ethernet vlan 0xFFF profile_id 100*;<br>ACL rule: *config access_profile profile_id 100 add access_id auto_assign ethernet vlan_id default port all deny*; | Required |

If the user has configured the ACL attribute of the RADIUS server (for example, ACL profile: **create access_profile ethernet vlan 0xFFF profile_id 100**; ACL rule: **config access_profile profile_id 100 add access_id auto_assign ethernet**), and the 802.1X or MAC-based Access

Control, WAC or JWAC authentication is successful, the device will assign the ACL profiles and rules according to the RADIUS server. For more information about the ACL module, please refer to the ‘Access Control List (ACL) Commands’ section.